AI BASED CYBERSECURITY FOR THE 5G-ENABLED INDUSTRY

Asterios (Stelios) Mpatziakas, Anastasios Drosou
Information Technologies Institute
Centre for Research and Technology Hellas (ITI-CERTH)

CENTRE FOR RESEARCH & TECHNOLOGY - HELLAS
Information Technologies Institute

CERTH
CENTRE FOR
RESEARCH & TECHNOLOGY
HELLAS

15/12/2013

ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ (*ΙΠΤΗΛ*)

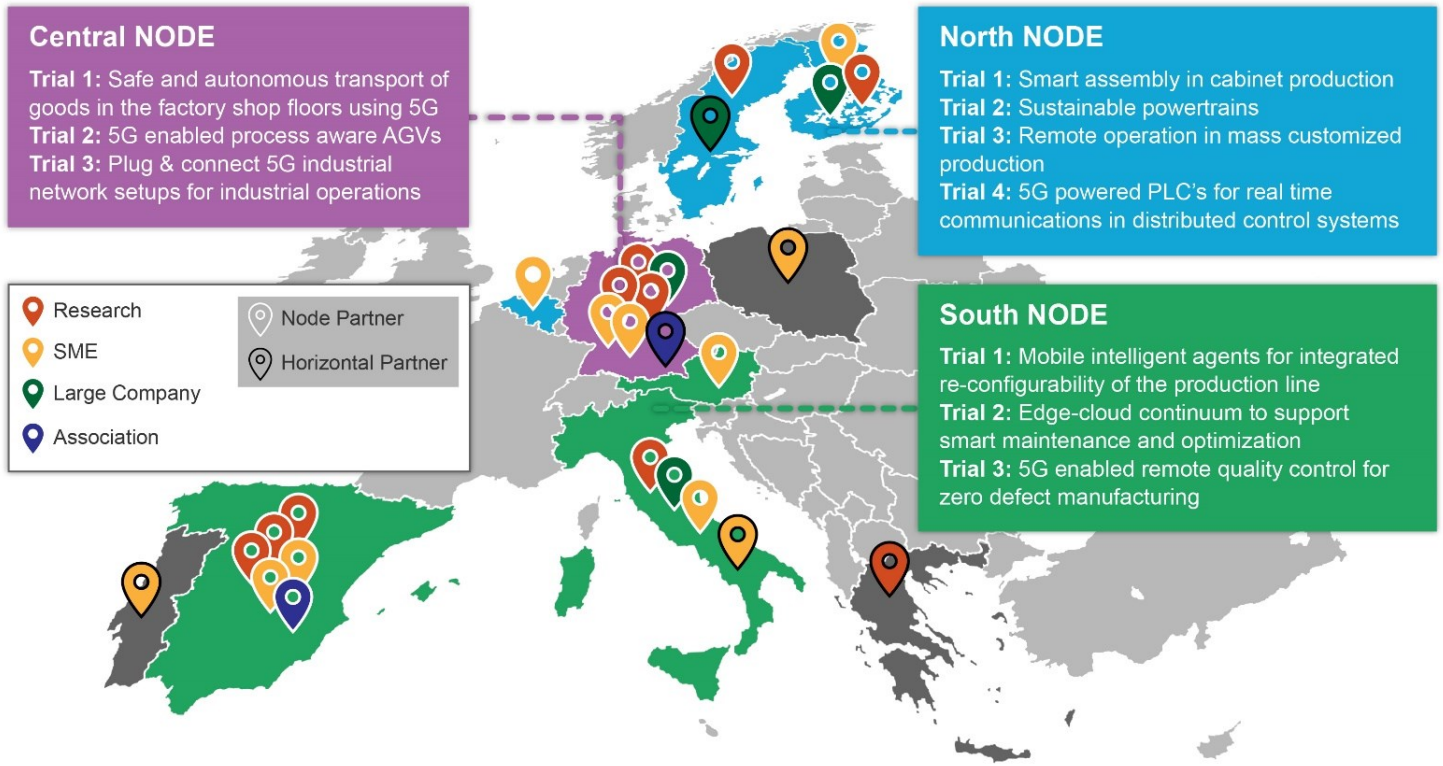
- Ένα από τα κορυφαία ερευνητικά ιδρύματα Πληροφορικής, Τηλεματικής και Τηλεπικοινωνιών, κομμάτι του Εθνικού Κέντρου Έρευνας και Τεχνολογικής ανάπτυξης (ΕΚΕΤΑ).
- Προσωπικό (700> εργαζομένους):
  - **18 Senior Researchers, 72 Post docs, 100 MSc, >400 Assoc. Researchers**
- Το ΙΠΤΗΛ συμμετείχε σε
  - **> 70 Horizon Europe** EC co-funded Research Projects
  - **>220 Horizon2020** EC co-funded Research Projects
  - **>80 Research/Innovate** National R&D Project

1st RI **στην Ελλάδα** τα τελευταία **7 συνεχόμενα έτη όσον αφορά την συμμετοχή σε ερευνητικά έργα με ανταγωνιστική χρηματοδότηση** (FP7, H2020)

- **Δημοσιεύσεις (τελευταία 5 έτη):**
  - **>300 περιοδικά, 650 συνέδρια, 100 βιβλία και κεφάλαια, <6.500 αναφορές**

ZERO-SWARM PROJECT

- **Το Zero-SWARM**, είναι ένα Horizon Europe IA πρόγραμμα, με σκοπό την επιτάχυνση της υιοθέτησης των 5G τεχνολογιών από τον ευρωπαϊκό κατασκευαστικό τομέα.
- Στόχος είναι να πετύχει παραγωγή κλιματικά ουδέτερη και υποβοηθούμενη ψηφιακά από τεχνολογίες όπως τα ιδιωτικά 5G δίκτυα, ένα ενεργό πληροφοριακό συνεχές (**active information continuum), τεχνολογίες digital twin technologies και χρήση AI**.
- 27 εταίροι από όλη την Ευρώπη.



ZEROSWARM

ΠΕΡΙΓΡΑΜΜΑ

- Κυβερνο-ασφάλεια στην 5G enabled I4.0
- AI enabled κυβερνο-ασφάλεια σε βιομηχανικά συστήματα :
  - AI για αυτοματοποιημένη αναγνώριση και αντιμετώπιση δικτυακών ανωμαλιών

ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑ ΣΤΗΝ 5G ENABLED I4.0

ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΠΟΧΗ ΤΗΣ I4.0

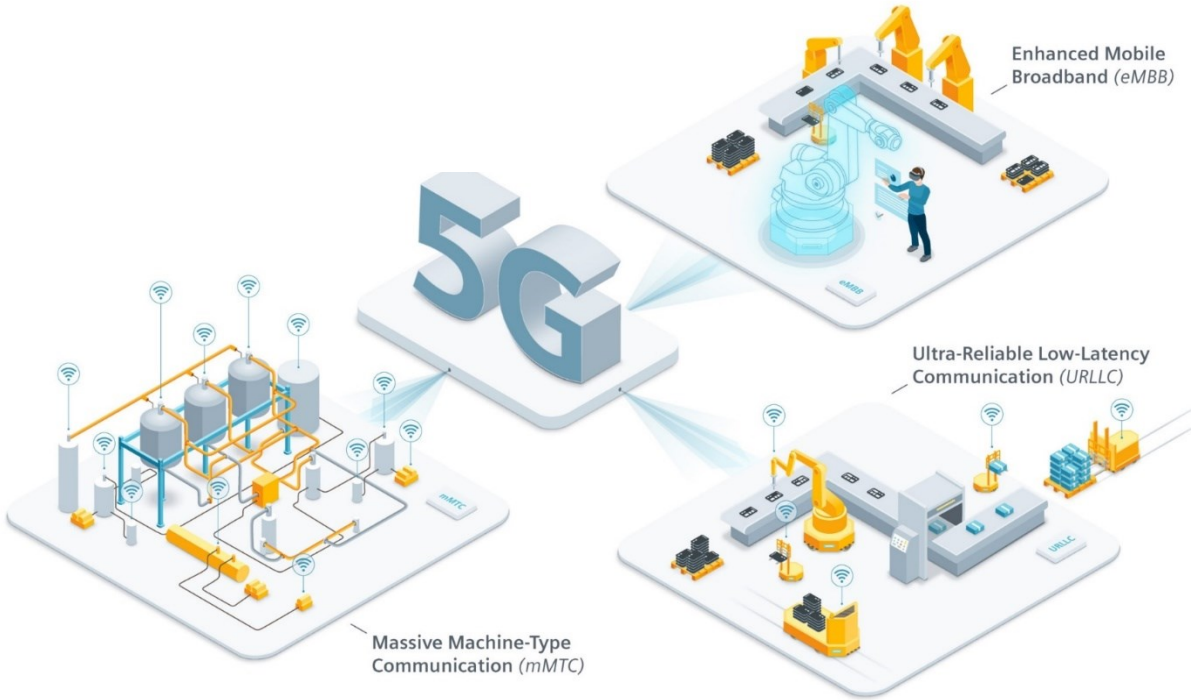
- Ο όρος Industry 4.0 μπορεί να οριστεί ως 'η τρέχουσα τάση για αυτοματοποίηση και ανταλλαγή πληροφορίας στις κατασκευαστικές τεχνολογίες συμπεριλαμβανομένων των **κυβερνό-φυσικών (CPS) συστημάτων, το IIOT, το cloud και cognitive computing για την δημιουργία του έξυπνου εργοστασίου**'.
- Οι βιομηχανίες εξελίσσονται, **συνδέοντας τις υποδομές τους σε πληροφοριακές (IT) τεχνολογίες** με σκοπό την αύξηση των δυνατοτήτων τους και την δημιουργία νέων εισροών.
- Βλέπουμε την επιταχυμένη διασύνδεση στοιχείων της κατασκευαστικής αλυσίδας που **σχεδιάστηκαν χωρίς στιβαρή ασφάλεια** και συχνά την έκθεση τους στο διαδίκτυο.
- Αυτό οδηγεί στην έκθεση του βιομηχανικού τομέα σε πολλές απειλές και ρίσκα.

ΠΡΟΣΦΑΤΑ ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΠΟΤΥΧΙΩΝ ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΒΙΟΜΗΧΑΝΙΑ

- **Maersk (2017):** Μια κυβερνο-επίθεση με το malware "NotPetya" οδήγησε σε διακοπές σε όλη την διακομιστική αλυσίδα της εταιρίας, οδηγώντας στην ακινησία χιλιάδων κοντέινερ ανά την υφήλιο για εβδομάδες.
- **Solar Winds (2020):** Η εισαγωγή κακόβουλου κώδικα σε ένα εργαλείο διαχείρισης δικτύου και μια ψεύτικη ανακοίνωση για αναβάθμιση λογισμικού χρησιμοποιήθηκαν για να δημιουργήσουν backdoors στα συστήματα των θυμάτων. Εταιρίες όπως η Intel, η Cisco και η Deloitte ήταν ανάμεσα στα θύματα.
- **Εγκαταστάσεις επεξεργασίας νερού Oldsmar (2021):** Μια ομάδα επιτιθέμενων κατάφερε να αποκτήσει πρόσβαση στα συστήματα SCADA που χρησιμοποιούνται για τον έλεγχο της χημικής επεξεργασίας του νερού της Φλόριντα και τροποποιήσουν τα επίπεδα υδροξείδιου του νατρίου στο πόσιμο νερό.
- **JBS (2021):** Μια επίθεση Remote access hijack με στόχο την τοποθέτηση ransomware διέκοψε την παραγωγή, κρέατος και τη διανομή του σε ολόκληρες τις Ηνωμένες Πολιτείες.
- Μια έκθεση της IBM για το 2023 ανέφερε ότι ο κατασκευαστικός τομέας ήταν ο **πιο συχνός στόχος** επιθέσεων ransomware τα τελευταία δύο χρόνια. Περισσότερο από το ένα τρίτο των κατασκευαστών που δέχτηκαν επιθέσεις κατέβαλε λύτρα **για να ανακτήσει τα δεδομένα του**.

5G ΓΙΑ ΤΑ INDUSTRY VERTICALS

- Ως industry vertical, ορίζουμε τις εταιρίες που επικεντρώνονται σε μια εξειδικευμένη αγορά ή τεχνολογικό τομέα που εκτείνεται σε πολλούς κλάδους.
- Το 5G μπορεί είτε να αντικαταστήσει είτε να συμπληρώσει τις υπάρχεις υποδομές είτε ασύρματες είτε ενσύρματες :
  - Προσφέρει **πολύ χαμηλή ταχύτητα απόκρισης** (latency), **υψηλή αξιοπιστία** (reliability), και εξειδικευμένες λειτουργίες όπως τον ακριβή συγχρονισμό και γεω-εντοπισμό, time sensitive networking κτλ.
  - **Προσφέρει ομοιόμορφα, ευέλικτα, επεκτάσιμα και διαμορφώσιμα** ασύρματα δίκτυα που μπορούν να στηθούν τοπικά ή απομακρυσμένα (εκτός εγκαταστάσεων) μέσω διαφόρων επιλογών ανάπτυξης (deployment).

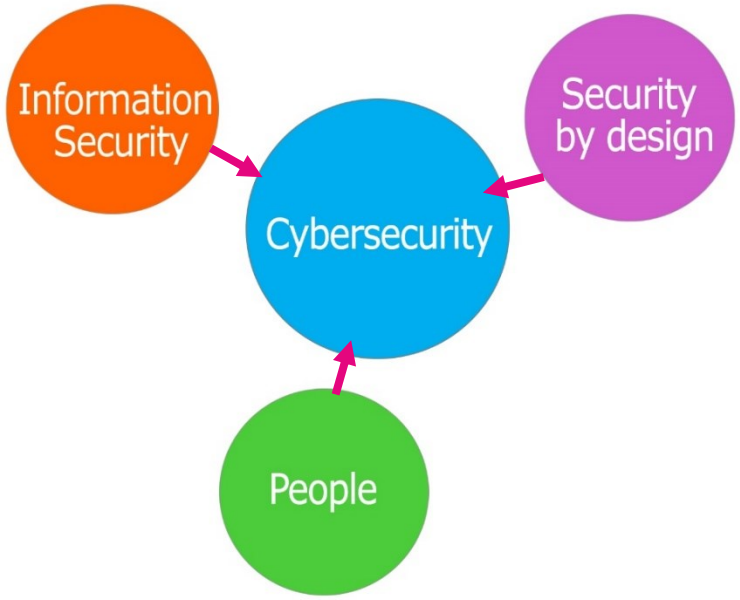


AI ENABLED CYBERSECURITY IN 5G/B5G NETWORKS (1/2)

- Το AI είναι ζωτικής σημασίας για την επίτευξη ιδιοτήτων των 5G/b5G όπως:
  - **Zero-touch Automation** (ελάχιστη χειροκίνητη παρέμβαση),
  - **Δίκτυα Self-X** (self-serving, self-fulfilling, self-assuring)
  - **Δίκτυα αυτοοργάνωσης** (SON) επόμενης γενιάς (δυναμική βελτιστοποίηση και αντιμετώπιση προβλημάτων κατά τη λειτουργία τους).
- Το AI μπορεί να αποτελέσει την βάση για μηχανισμούς κυβερνο-ασφάλειας και να υποστηρίξει την λεγόμενη Zero-Trust approach:
  - Τα δίκτυα 5G /b5G θα πρέπει να διαχειρίζονται **μεγάλο όγκο κίνησης, τεράστιο αριθμό συνδεδεμένων συσκευών** ενώ θα γεφυρώνουν **ετερογενείς τεχνολογίες και υπηρεσίες**.
  - Το περιβάλλον που υπόσχονται τα πλήρως υλοποιημένα δίκτυα 5G/b5G θα οδηγήσει σε ένα **τοπίο περίπλοκων και δυναμικών απειλών στον κυβερνοχώρο**.
  - Η τεχνητή νοημοσύνη μπορεί να παρέχει λύσεις που είναι προσαρμοστικές, έξυπνες και μπορούν να συμβαδίζουν με την **πυκνότητα της κίνησης** (traffic density) και την ρυθμαπόδοση (throughput) που απαιτείται από τα δίκτυα 5G / b5G.

ASPECTS OF CYBERSECURITY

- Για να επιτευχθεί ένα σύστημα ασφάλειας στον κυβερνοχώρο, πρέπει να ληφθούν υπόψη πολλαπλές πτυχές!
- **Ασφάλεια μέσω σχεδίασης** σημαίνει ένα σχεδιασμό που «προστατεύει **σε εύλογα πλαίσια** από κακόβουλους φορείς του κυβερνοχώρου, δηλαδή εμποδίζοντάς τους να αποκτήσουν πρόσβαση σε συσκευές, δεδομένα και τις διασυνδεδεμένες υποδομές».
  - Αυτό περιλαμβάνει τη χρήση συγκεκριμένων αρχών, πολιτικών και διαδικασιών αρχιτεκτονικής και σχεδιασμού.
- **Οι άνθρωποι** πρέπει να έχουν επίγνωση, να λαμβάνουν εκπαίδευση και να είναι υπεύθυνοι για τη φυσική ασφάλεια.
- **Η ασφάλεια της πληροφορίας** (information security) περιλαμβάνει IT, OT, διαφύλαξη λειτουργικών και προσωπικών δεδομένων.
- **Το AI μπορεί να βοηθήσει και στα τρία.**



AI ENABLED CYBERSECURITY IN 5G/B5G NETWORKS (2/2)

- Τι εννοούμε AI enabled Κυβερνοασφάλεια;
  - Την χρήση **μηχανισμών που βασίζονται στο AI** για την εκτέλεση/επιβολή διεργασιών για τη διαχείριση της ασφάλειας, της εμπιστοσύνης και του απορρήτου σε ένα σύστημα.

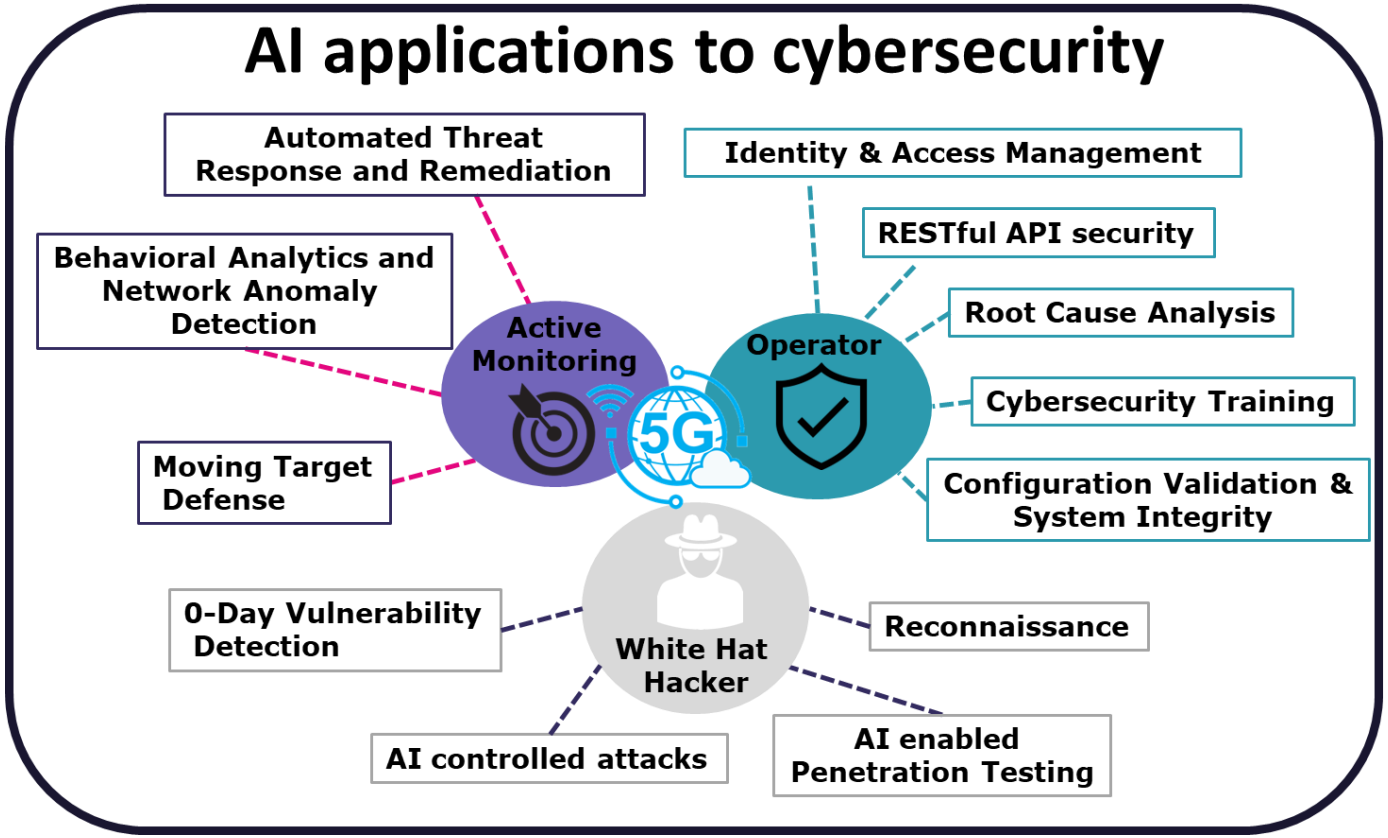
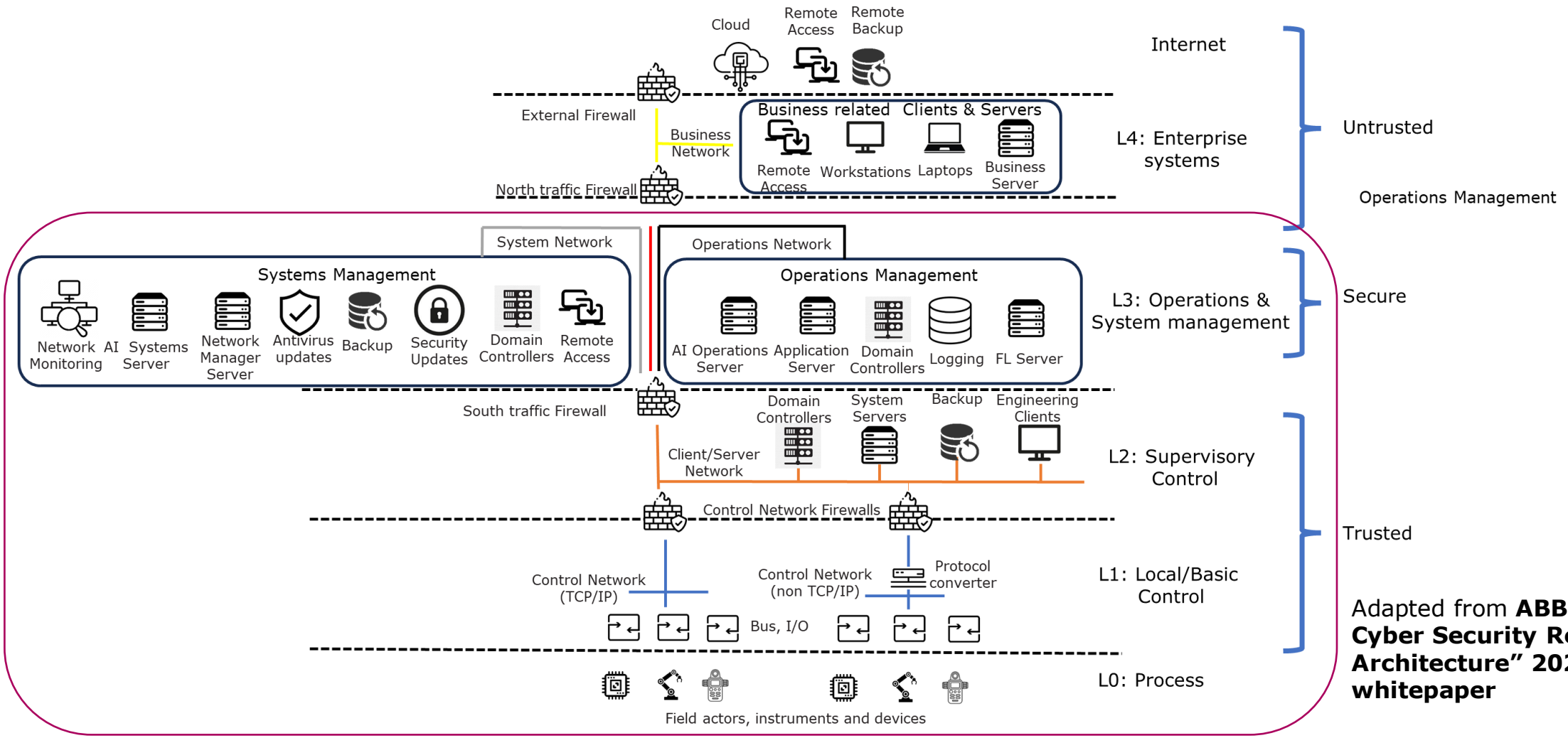


Figure adapted from [1] C. Benzaïd and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?," in *IEEE Network*, vol. 34, no. 6, pp. 140-147, November/December 2020,.

AI FOR NETWORK ANOMALY DETECTION AND MITIGATION

15/12/2023

REFERENCE CYBERSECURITY ARCHITECTURE

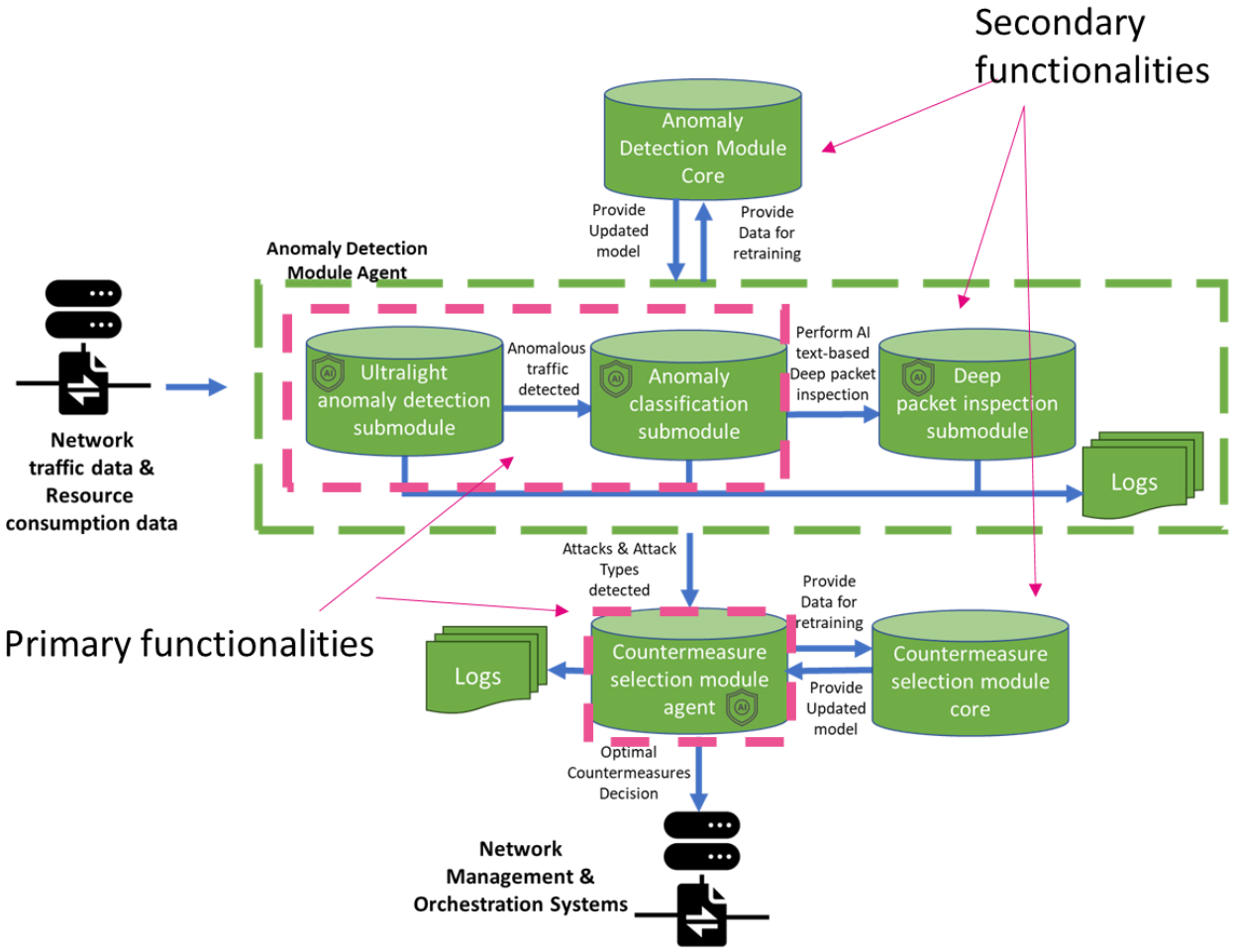


Adapted from **ABB "ICS Cyber Security Reference Architecture" 2021 whitepaper**

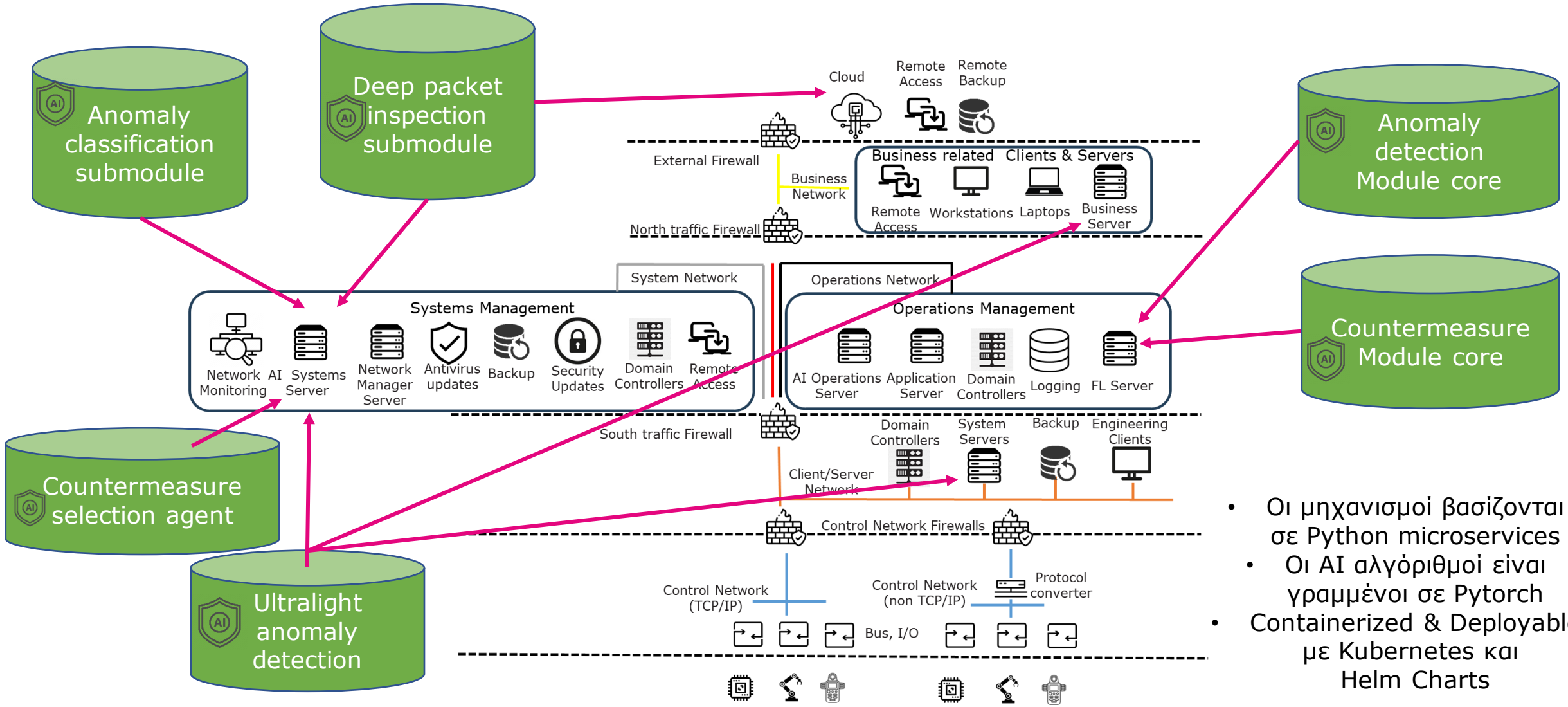
Βασισμένο στην αρχιτεκτονική των 5 επιπέδων του **IEC 62443 reference model**

ANOMALY DETECTION AND COUNTERMEASURE SELECTION MODULE

- Η ανίχνευση ανωμαλιών μπορεί να εντοπίσει αποκλίσεις από την κανονική συμπεριφορά του συστήματος, οι οποίες μπορεί να είναι **ενδεικτικές** μιας **κυβερνοεπίθεσης** ή μιας **δυσλειτουργίας του συστήματος**.
- Η ανίχνευση και η αναγνώριση των ανωμαλιών στα **αρχικά τους στάδια** επιτρέπει την **ταχεία απόκριση**, ελαχιστοποιώντας την **πιθανή ζημιά** ή το **χρόνο διακοπής λειτουργίας**.
- Οι κυβερνοεπιθέσεις μπορούν να αντιμετωπιστούν με **διαφορετικές δράσεις μετριασμού** (mitigation actions), δημιουργώντας την ανάγκη για μηχανισμούς που βοηθούν την **αυτοματοποιημένη επιλογή των βέλτιστων αντίμετρων** (countermeasures).



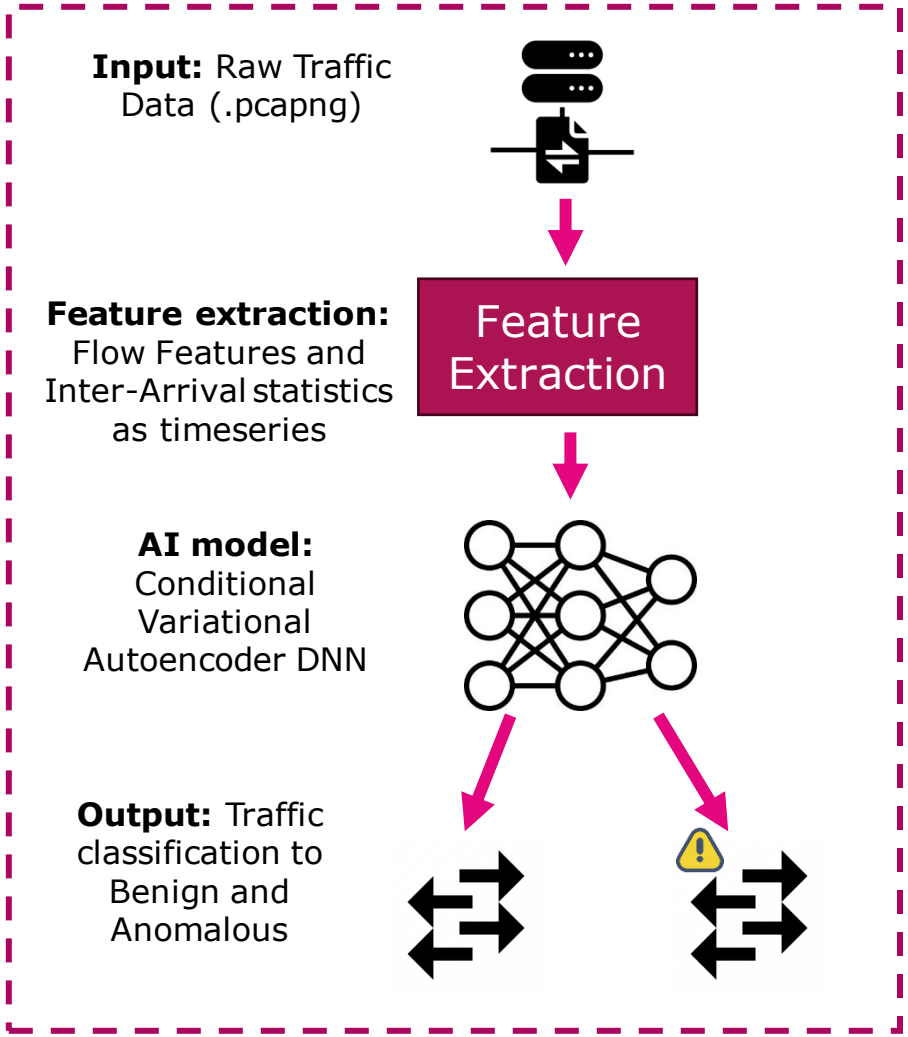
POSITION IN ARCHITECTURE



- Οι μηχανισμοί βασίζονται σε Python microservices
- Οι AI αλγόριθμοι είναι γραμμένοι σε Pytorch
- Containerized & Deployable με Kubernetes και Helm Charts

ULTRALIGHT ANOMALY DETECTION: OVERVIEW

- Η ταχεία ανίχνευση των ανωμαλιών στο δίκτυο αποτελεί **βάση για την ασφάλειά του**.
- Η τεχνητή νοημοσύνη, σε σύγκριση με τις «παραδοσιακές» μεθόδους ML, επεκτείνεται καλύτερα σε δεδομένα ανωμαλιών μεγάλης κλίμακας/υψηλότερης διάστασης.
- Η ανώμαλη κίνηση δεν υποδηλώνει πάντα επίθεση, αλλά θα μπορούσε επίσης να υποδεικνύει δυσλειτουργίες, σφάλματα υλικού κ.λπ.
- Ο σκοπός αυτού του εργαλείου είναι να ανιχνεύει ανωμαλίες και όχι την υποκείμενη αιτία τους.
- Προτείνουμε την χρήση μιας παραλλαγής των **Conditional Variational Autoencoder** (CVAE) variant, το "**Log-Cosh CVAE**" [1] μαζί με ένα Συνελικτικό Δίκτυο (CNN).

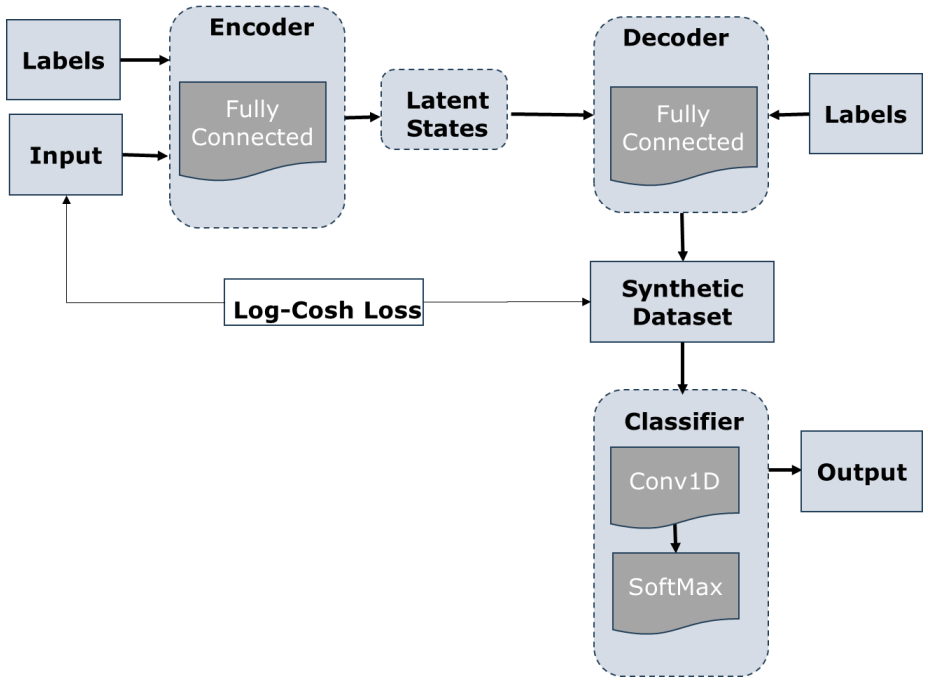


[1] X. Xu, J. Li, Y. Yang and F. Shen, "Toward Effective Intrusion Detection Using Log-Cosh Conditional Variational Autoencoder," in *IEEE Internet of Things Journal*, vol. 8, no. 8, 2021

ULTRALIGHT ANOMALY DETECTION: PROBLEM SOLUTION & RESULTS

- Το CVAE αντιμετωπίζει αποτελεσματικά την ανισοκατανομή μεταξύ των κλάσεων και δεδομένα μεγάλων διαστάσεων.
- Το CVAE μοντελοποιεί την κατανομή των πραγματικών δεδομένων με λανθάνουσες μεταβλητών (latent variables) και λειτουργεί ως γεννήτρια τεχνητών δεδομένων που χρησιμοποιούμε για να εκπαιδεύσουμε τον αλγόριθμο.
- Αξιολογήσαμε τον αλγόριθμο σε ένα ανοιχτό dataset το 5G-NIDD (8 attacks DoS/DDoS and Port Scan types)[1].
- Τα αποτελέσματα έδειξαν ότι η προτεινόμενη προσέγγιση :

CVAE Architecture



A) αποδίδει **εξίσου καλά** με τη λύση ML με την καλύτερη απόδοση(Decision Tree ~99.9% accuracy)

B) Είναι σημαντικά **γρηγορότερο** (avg. 1 ms) συγκριτικά με την αμέσως καλύτερη λύση(Decision Tree avg. 28 ms)

[1] Sehan Samarakoon et al., December 2, 2022, "5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network", IEEE Dataport

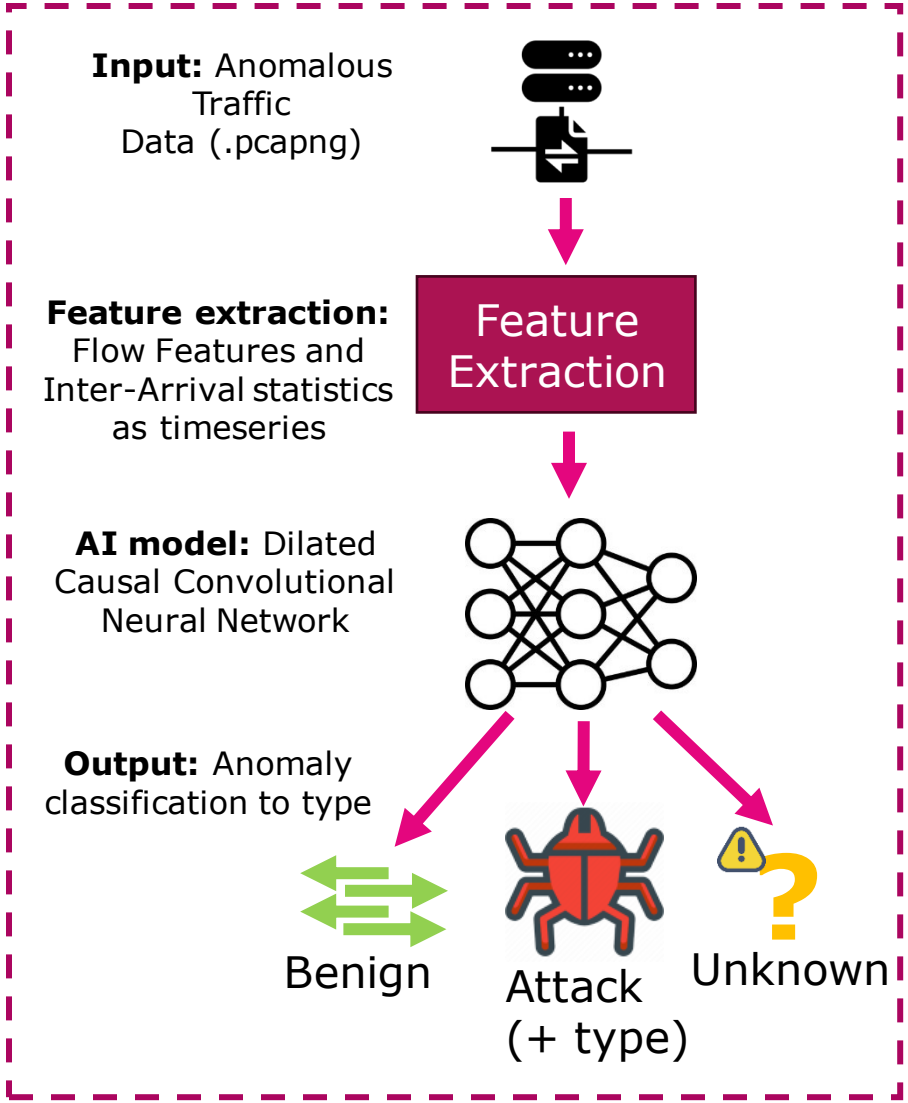
ANOMALY CLASSIFICATION

- Το επόμενο βήμα μετά τον εντοπισμό μιας ανωμαλίας είναι η προσπάθεια να διακρίνουμε:

A. το είδος της ανωμαλίας

B. Σε περίπτωση κυβερνο-επίθεσης/κυβερνοαπειλής, τον τύπο της

- Πρέπει να γνωρίζουμε τα είδη των επιθέσεων για να επιλέξουμε **τα κατάλληλα αντίμετρα**
- Πρέπει να παρακολουθούμε περιπτώσεις ψευδώς θετικών αποτελεσμάτων: Η καλοήθης κυκλοφορία που προσδιορίζεται ως ανώμαλη μπορεί να υποδεικνύει ότι το εργαλείο ανίχνευσης των ανωμαλιών **χρειάζεται επανεκπαίδευση**.
- Προτείνουμε την χρήση των **Dilated Causal Convolutional NN (DCNN) [1]** για αυτή την εργασία.



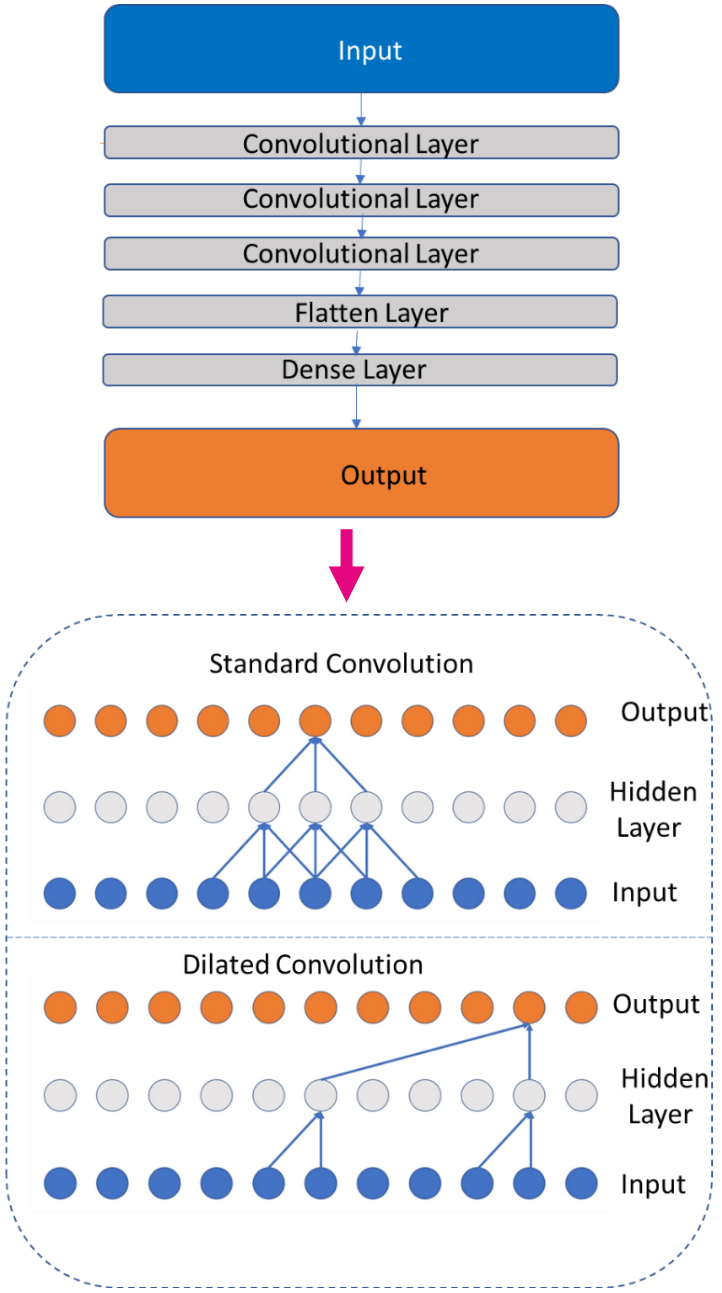
[1] X. Zhang and J. You, "A Gated Dilated Causal Convolution Based Encoder-Decoder for Network Traffic Forecasting," in *IEEE Access*, vol. 8, pp. 6087-6097, 2020, doi: 10.1109/ACCESS.2019.2963449.

ANOMALY CLASSIFICATION: PROBLEM SOLUTION AND RESULTS

- Στα DCNN, εφαρμόζονται φίλτρα παρακάμπτοντας δεδομένα κατά την είσοδο τους στο δίκτυο, επιτρέποντας στο δεκτικό (perceptive) πεδίο του δικτύου να αναπτυχθεί εκθετικά.
- Αυτή η ιδιότητα τους επιτρέπει να μοντελοποιούν ακόμη και sparse δεδομένα μαζί με μακροπρόθεσμες/βραχυπρόθεσμες σχέσεις ακολουθίας.
- Αξιολογήσαμε τον αλγόριθμο στο dataset 5G-NIDD.
- Τα αποτελέσματα έδειξαν ότι η προτεινόμενη προσέγγιση :

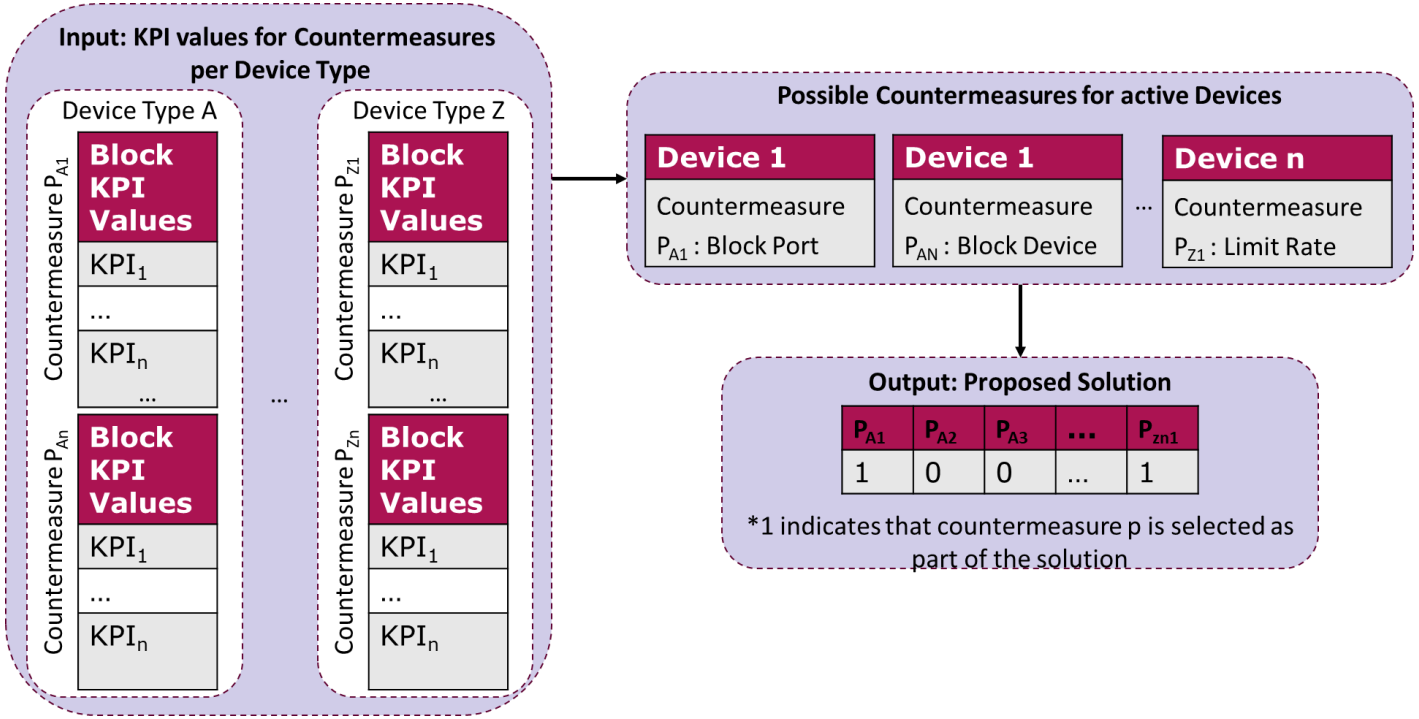
A) **αποδίδει εξίσου καλά και λίγο γρηγορότερα (0.03s)** σε σχέση με την καλύτερη ML λύση (Random Forest (RF) ~99.4% accuracy, 0.037s)

B) Είναι **σημαντικά πιο αργή** σε σύγκριση με τη δεύτερη καλύτερη λύση (Decision Tree, ~99.1% accuracy, 30ms)



AUTOMATED COUNTERMEASURE SELECTION: OVERVIEW

- Αφού εντοπιστούν μία ή περισσότερες επιθέσεις, πρέπει να τις αντιμετωπίσουμε.
- Μοντελοποιήσαμε την διαδικασία επιλογή των αντίμετρων ως ένα **multi-objective 0-1 Knapsack πρόβλημα**
- Για **κάθε επίθεση** που ανιχνεύεται, μπορούν να εφαρμοστούν **περισσότερες από μία ενέργειες αντιμέτρων**, π.χ. αποκλεισμός μιας θύρας, περιορισμός του ρυθμού της κακόβουλης συσκευής, αποκλεισμός της συσκευής κ.λπ.
- Χρησιμοποιούμε μια νέα προσέγγιση [1] που συνδυάζει τα Pointer DNNs με την μέθοδο normalized normal constrained method για να επιλύσει το πρόβλημα.

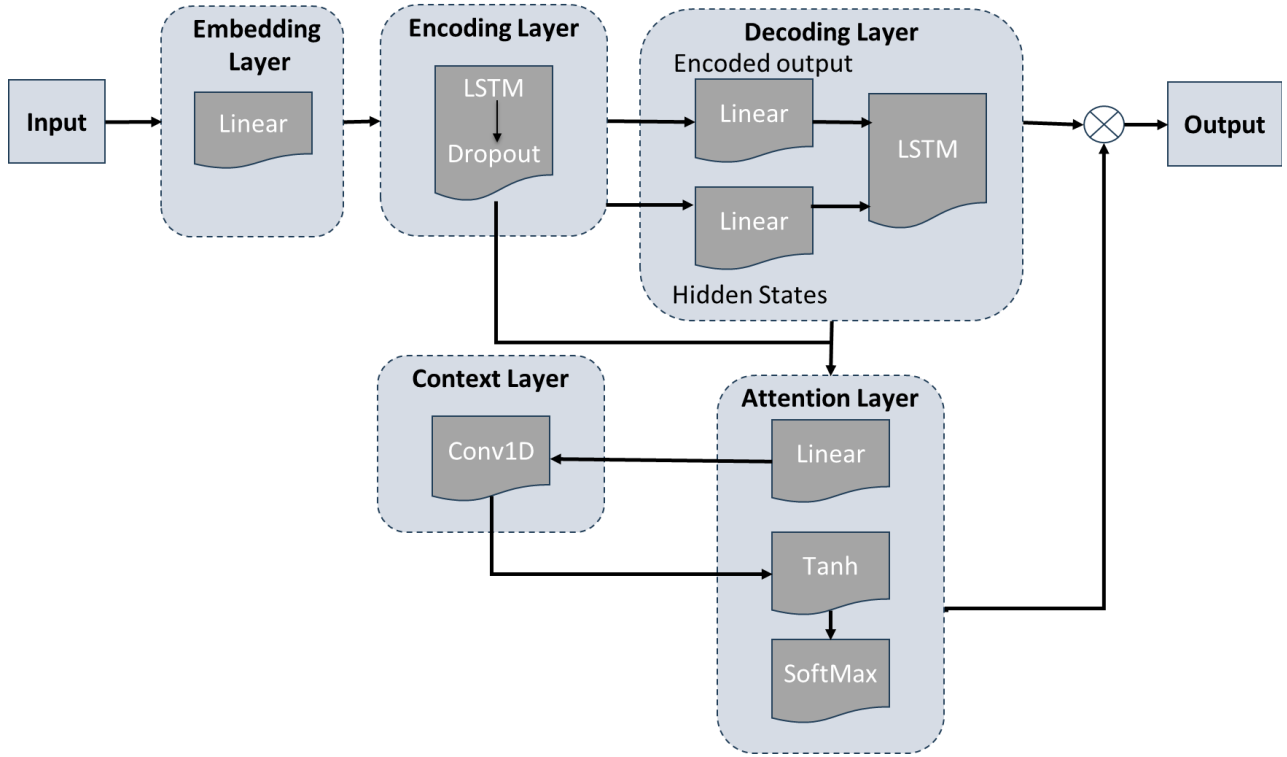


[1] Asterios Mpatziakas, Anastasios Drosou, Stavros Papadopoulos, Dimitiris Tzovaras, IoT threat mitigation engine empowered by artificial intelligence multi-objective optimization, Journal of Network and Computer Applications, Volume 203, 2022

AUTOMATED COUNTERMEASURE SELECTION: PROBLEM SOLUTION

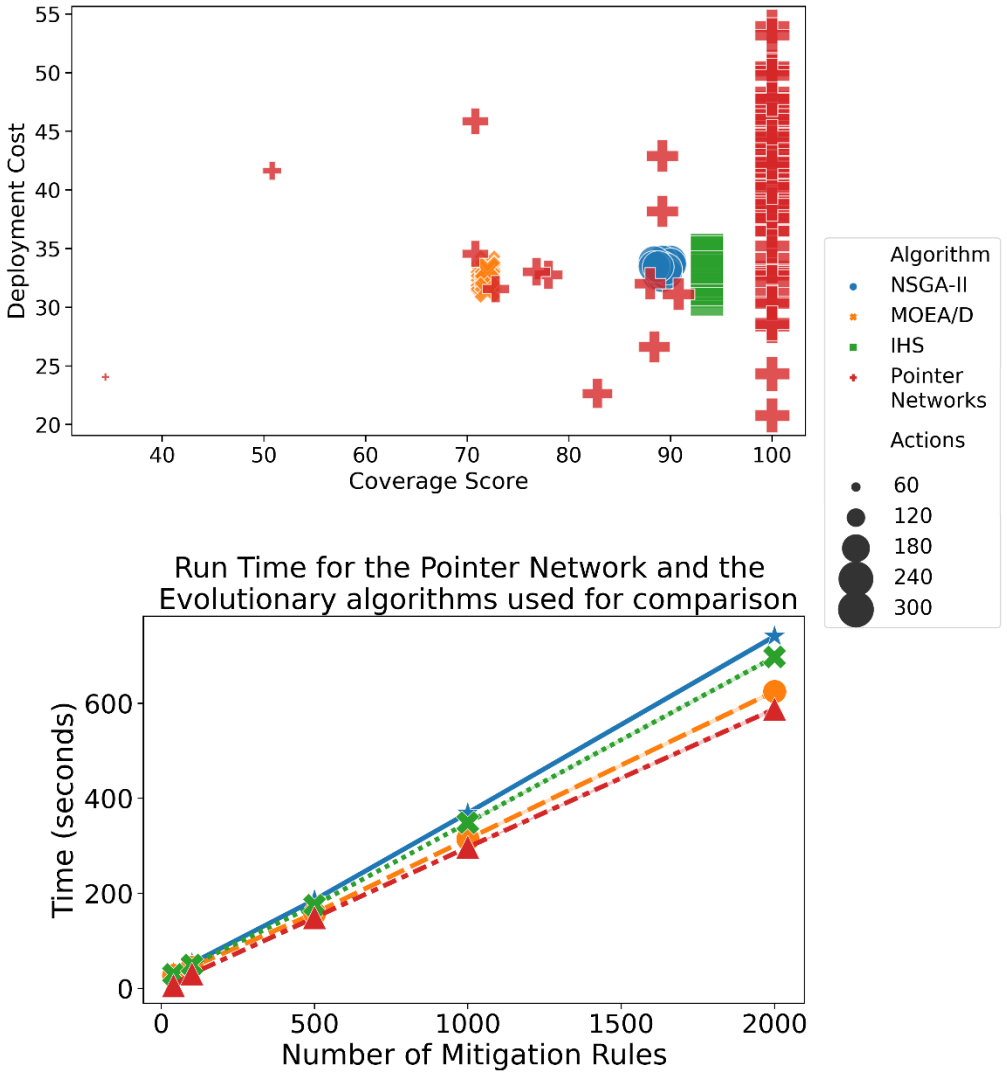
- Ο στόχος είναι να βρεθεί το σύνολο των αντίμετρων που βελτιστοποιεί **τέσσερα KPI που σχετίζονται με κυβερνο-ασφάλεια** (CVSS, Deployment Cost, Coverage, RORI index)
- Στα MO προβλήματα, η βελτιστοποίηση της τιμής ενός μεμονωμένου KPI μπορεί να οδηγήσει σε **ανεπιθύμητα αποτελέσματα** σε σχέση με τις τιμές των άλλων KPI.
- Το αποτέλεσμα είναι ένα **σύνολο βέλτιστων λύσεων που αντισταθμίζονται για τα KPI**, που συχνά αναφέρεται ως Μέτωπο Pareto
- Τέλος, επιλέγεται μια λύση από το σύνολο χρησιμοποιώντας μια μέθοδο όπως π.χ το **Weighted Sum**, Weighted Product or TOPSIS.

Pointer network Architecture



AUTOMATED COUNTERMEASURE SELECTION: RESULTS

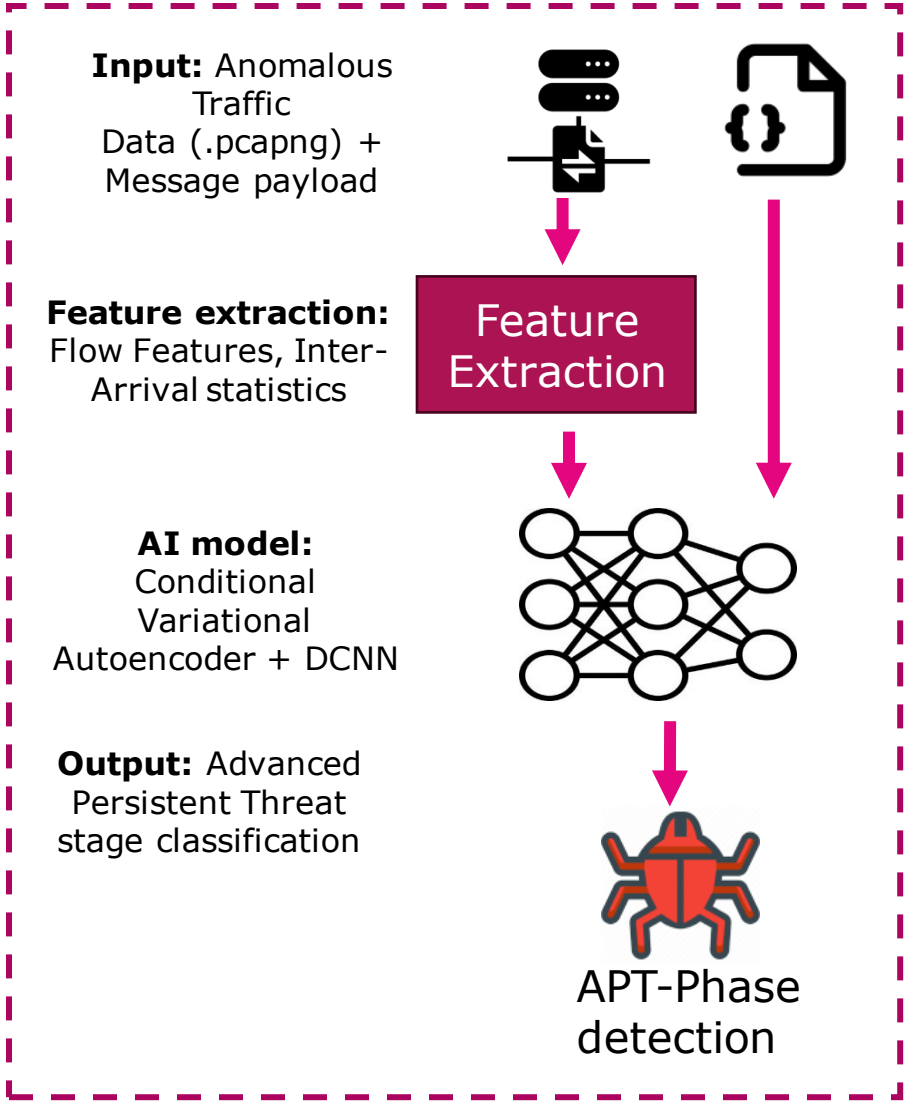
- Για λόγους αξιολόγηση εξάγαμε τα αποτελέσματα και για τρεις εξελικτικούς αλγόριθμους, (NSGA-II, MOEA/D, IHS).
- Στο πιο περίπλοκο σενάριο που εξετάστηκε στις προσομοιώσεις μας [1], τα αποτελέσματα από το Pointer Network είναι καλύτερα για τα περισσότερα KPI, εκτός από τη βαθμολογία CVSS όπου υπολείπεται με μικρή διαφορά(μ.ο. ~1%).
- Το Pointer Network είναι **τουλάχιστον 4% ταχύτερο σε σύγκριση με τις υπόλοιπες μεθόδους**.



[1] Asterios Mpatziakas, Anastasios Drosou, Stavros Papadopoulos, Dimitiris Tzovaras, IoT threat mitigation engine empowered by artificial intelligence multi-objective optimization, Journal of Network and Computer Applications, Volume 203, 2022

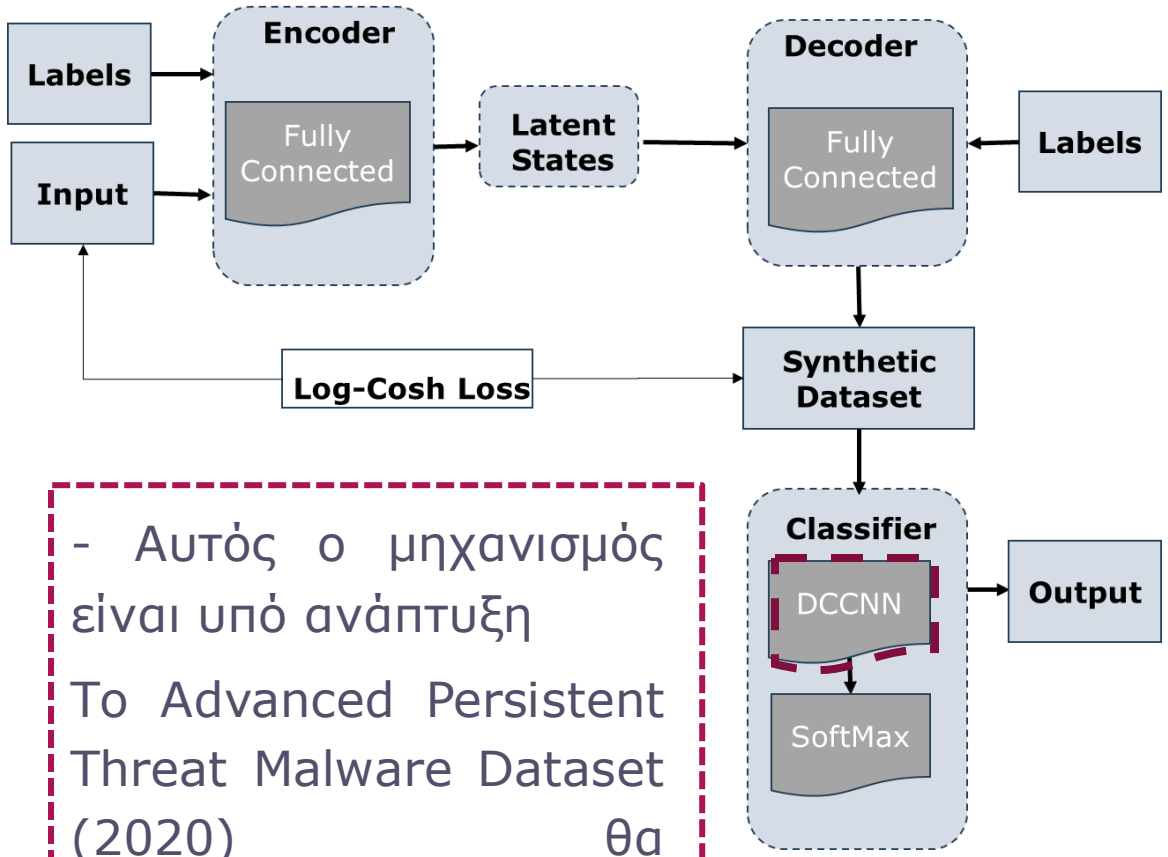
DEEP PACKET INSPECTION TOOL FOR UNKNOWN ANOMALY ANALYSIS (1/2)

- Το εργαλείο επιθεώρησης Deep Packet επιτρέπει στον χειριστή του συστήματος να αποκτήσει περαιτέρω γνώσεις σχετικά με **πρωτόγνωρα μοτίβα ανώμαλης κίνηση**ς στο δίκτυο.
- Μαζί με τα δεδομένα κίνησης, χρησιμοποιείται και το περιεχόμενο του μηνύματος ως πληροφορία.
- Έχει αποδειχθεί ότι το AI μπορεί να αναγνωρίσει σωστά, κομμάτια των λεγόμενων Προηγμένων Επίμονων Απειλών (Advanced Peristant Threats - APT).
- Οι APT είναι **πολύπλοκες, εξελιγμένες επιθέσεις** με στόχο να αποκτήσουν τον έλεγχο ενός δικτύου και λαμβάνουν χώρα σε εκτεταμένες χρονικές περιόδους.



DEEP PACKET INSPECTION FOR UNKNOWN ANOMALY ANALYSIS

- Προτείνουμε την χρύση του Log-Cosh CVAE και του DCCNN για την προέκταση που προτείνεται στο [1].
- Εκ των υστέρων έλεγχος εάν κίνηση με ανώμαλο μοτίβο επισκεψιμότητας ανήκει σε ένα από τα ακόλουθα βήματα ενός APT:
- **Reconnaissance:** χαρτογράφηση τοπολογίας δικτύου, διαθέσιμες υπηρεσίες και χρησιμοποιημένες εκδόσεις λογισμικού για τον εντοπισμό πιθανών σημείων εισόδου.
- **Foothold establishment:** τα σημεία εισόδου αξιοποιούνται για τη δημιουργία ενός καναλιού εντολών και ελέγχου
- **Lateral movement:** τα ήδη παραβιασμένα κομμάτια του συστήματος χρησιμοποιούνται για να την είσοδο βαθύτερα στο σύστημα και την απόκτηση πρόσβασης σε υποσυστήματα που δεν είναι άμεσα συνδεδεμένα με ένα δημόσιο δίκτυο.
- **Data exfiltration:** κλοπή μη δημοσίων δεδομένων πιθανά υψηλής αξίας



- Αυτός ο μηχανισμός είναι υπό ανάπτυξη

Το Advanced Persistent Threat Malware Dataset (2020) θα χρησιμοποιηθεί για αξιολόγηση.

[1] A. Dijk, "Detection of Advanced Persistent Threats using Artificial Intelligence for Deep Packet Inspection," *2021 IEEE International Conference on Big Data (Big Data)*, Orlando, FL, USA, 2021, pp. 2092-2097.

INFORMATION TECHNOLOGIES INSTITUTE, CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS

https://www.iti.gr |contact: drosou@iti.gr ampatziakas@iti.gr