ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αρχιτεκτονική Προσαρμοστικής Ομοσπονδιακής Αυτόματης Μετά-Μηχανικής Μάθησης με Χρήση Τεχνολογίας Κατανεμημένων Μπλοκ Εγγραφής για Ψηφιακή Ασφάλεια και Ιδιωτικότητα στη Βιομηχανία 4.0

Κωνσταντίνος Δεμερτζής

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

Επιβλέπων

Επίκουρη Καθηγήτρια Δρ Κοζύρη Μαρία

Λαμία, Ιούλιος 2020

UNIVERCITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Blockchained Adaptive Federated Auto MetaLearning Architecture for CyberSecurity and Privacy in Industry 4.0

Konstantinos Demertzis

MASTER THESIS

Supervisor

Assistant Professor Dr Koziri Maria

Lamia, July 2020

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «**Αρχιτεκτονική Προσαρμοστικής Ομοσπονδιακής Αυτόματης Μετά-Μηχανικής Μάθησης με Χρήση Τεχνολογίας Κατανεμημένων Μπλοκ Εγγραφής για Ψηφιακή Ασφάλεια και Ιδιωτικότητα στη Βιομηχανία 4.0 (Blockchained Adaptive Federated Auto MetaLearning Architecture for CyberSecurity and Privacy in Industry 4.0)**» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία

Υπογραφή

Αρχιτεκτονική Προσαρμοστικής Ομοσπονδιακής Αυτόματης Μετά-Μηχανικής Μάθησης με Χρήση Τεχνολογίας Κατανεμημένων Μπλόκ Εγγραφής για Ψηφιακή Ασφάλεια και Ιδιωτικότητα στη Βιομηχανία 4.0

Κωνσταντίνος Δεμερτζής

Τριμελής Επιτροπή:

Ονοματεπώνυμο, Επίκουρη Καθηγήτρια Δρ Κοζύρη Μαρία (επιβλέπων)

Ονοματεπώνυμο, ……

Ονοματεπώνυμο, …….

Επιστημονικός Σύμβουλος:

Ονοματεπώνυμο…..

Στα λατρεμένα μου παιδιά Βίκυ και Σταύρο
και την πολυαγαπημένη μου σύζυγο Έφη

Αντί Προλόγου

Η σύγχρονη εποχή χαρακτηρίζεται από ραγδαίες τεχνολογικές εξελίξεις, με αποτέλεσμα να αναπτύσσεται μία νέα οικονομία σε παγκόσμιο επίπεδο, όπου το σημαντικότερο περιουσιακό στοιχείο να είναι τα δεδομένα. Η εποχή των «Μεγάλων Δεδομένων», γέννησε την διττή ανάγκη για την ανάλυση τους και την εξαγωγή της πολύτιμης κρυμμένη γνώσης που αυτά περιλαμβάνουν και παράλληλα την διασφάλιση τους από αθέμιτες ενέργειες και την προστασία της ιδιωτικότητας των πληροφοριών που εμπεριέχουν. Ο επιτυχής συνδυασμός της ασφάλειας και της διαχείριση μεγάλου όγκου δεδομένων, τα οποία συνθέτουν τον αντικειμενικό σκοπό της κατεύθυνσης «Πληροφορική με Εφαρμογές στην Ασφάλεια, Διαχείριση Μεγάλου Όγκου Δεδομένων και Προσομοίωση», του Προγράμματος Μεταπτυχιακών Σπουδών του Τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική και του Τμήματος Πληροφορικής του Πανεπιστημίου Θεσσαλίας με τίτλο: «Πληροφορική και Υπολογιστική Βιοϊατρική», αποτελούν αναπόφευκτα, μια τεράστια πρόκληση και συνάμα μια μοναδική ευκαιρία, με εξαιρετικές προοπτικές.

Θέλοντας λοιπόν να εξοικειωθώ με τις τρέχουσες τάσεις στο χώρο της διαχείρισης δεδομένων μεγάλης κλίμακας, να εντρυφήσω στις προηγμένες τεχνικές ανάλυσης, οπτικοποίησης και προσομοίωσης τους και να αποκτήσω δεξιότητες στη σχεδίαση και υλοποίηση κλιμακούμενων λύσεων οι οποίες σχετίζονται με την ασφάλεια πληροφοριακών συστημάτων, επέλεξα την συμμετοχή μου στο συγκεκριμένο Προγράμματος Μεταπτυχιακών Σπουδών.

Η προσπάθεια μου ανταμείφθηκε με υποτροφία και απαλλαγή διδάκτρων, γεγονός που με πείσμωσε να προσπαθήσω ακόμα περισσότερο. Ο χρόνος κυλούσε πλέον πολύ γρήγορα και η χαρά της γνώσης με τις καθημερινές μικρές επιτυχίες συνοδευόταν από πολλές δύσκολες στιγμές. Απογοήτευση, κούραση, πίεση χρόνου. Υπήρχαν στιγμές που καθετί φάνταζε ακατόρθωτο και στιγμές που αισθανόμουν κενό κάτω από τα πόδια μου. Ευτυχώς υπήρχε πάντα εκεί το διπλό δίχτυ ασφαλείας μου. Από την μια οι Καθηγητές του Τμήματος, να με ενθαρρύνουν, να με καθοδηγούν, να με βγάζουν από τα αδιέξοδα, αλλά και πολλές φορές να με επαναφέρουν στην πραγματικότητα και να μου υπενθυμίζουν τον στόχο μου και από την άλλη η σύζυγος και τα παιδιά μου, πάντα με αγάπη, ευχάριστη διάθεση, υπομονή και καλοσύνη, να μου δίνουν χαρά, έμπνευση και κουράγιο να συνεχίσω.

Κλείνω τον Μεταπτυχιακό κύκλο σπουδών μου, μετά από 2 ½ έτη αδιάκοπης και επίπονης δουλειάς, έχοντας αισίως **3 δημοσιεύσεις σε διεθνή επιστημονικά περιοδικά και 2 συμμετοχές σε διεθνές συνέδρια**. Η αναλυτική λίστα των δημοσιεύσεων παρουσιάζεται στη σελίδα XX.

Οι συγκεκριμένες δημοσιεύσεις, προκάλεσαν το ενδιαφέρον επαγγελματιών του χώρου της ασφάλειας, οι οποίοι ενδιαφέρθηκαν για την υλοποίηση τους και την μεταφορά της τεχνογνωσίας, από τον ακαδημαϊκό χώρο της έρευνας, στον πραγματικό κόσμο των επιχειρήσεων.

Το συγκεκριμένο γεγονός, πέρα από τεράστια ηθική ικανοποίηση, δημιουργεί προοπτικές για την περεταίρω εξέλιξη των προτύπων και των ερευνητικών μεθόδων που διερευνήθηκαν στο Πρόγραμμα Μεταπτυχιακών Σπουδών, αναδεικνύει τους τρόπους και τις μεθόδους διδασκαλίας που ακολουθεί και καταξιώνει την ακαδημαϊκή και ερευνητική εμπεριστατωμένη γνώση που παρέχεται τόσο στο συγκεκριμένο πρόγραμμα, όσο και γενικότερα στο Τμήμα και κατ' επέκταση στο Πανεπιστήμιο Θεσσαλίας.

Επιχειρώντας μια ανασκόπηση αυτών των 2 ½ ετών, είμαι πλέον σίγουρος ότι δεν υπάρχει κάτι που δεν γίνεται. Είμαι πεπεισμένος ότι η μεγαλύτερη ψυχική δύναμη είναι η αφοσίωση και επιμονή στον στόχο. Παράλληλα πιστεύω ότι οι μεγάλοι στόχοι και τα μεγαλεπήβολα όνειρα, απαιτούν μικρά αλλά σταθερά βήματα και παράλληλα υπομονή και μεθοδικότητα.

Η αλήθεια είναι όμως ότι ο υπέρλαμπρος και εθιστικός κόσμος της έρευνας μου δημιούργησε μια ακόρεστη επιθυμία για ακόμα περισσότερα. Αισιοδοξώ και ελπίζω, ότι ο κύκλος που μόλις τελείωσε, αποτελεί απλά την έναρξη μιας ακόμα πιο ενδιαφέρουσας ακαδημαϊκής και ερευνητικής αναζήτησης, γεμάτη νέες προκλήσεις.

Ευχαριστίες

Κλείνοντας έναν πολύ σημαντικό και σπουδαίο κύκλο της ζωής μου, νιώθω την ανάγκη να ευχαριστήσω ένα σύνολο μοναδικών ανθρώπων, που έμπρακτα συνέβαλαν στην προσπάθεια μου να ολοκληρώσω τη Μεταπτυχιακή μου διατριβή.

Κατ' αρχάς θα ήθελα να εκφράσω τις ειλικρινές μου ευχαριστίες, στην επιβλέποντα της παρούσας Μεταπτυχιακής διατριβής, Επίκουρο Καθηγητή Δρ Μαρία Κοζίρη. Η Επίκουρη Καθηγήτρια Δρ Μαρία Κοζίρη, μου έδειξε απεριόριστη εμπιστοσύνη και κατανόηση, γεγονός που με πείσμωσε πραγματικά στο να υπερβάλω εαυτόν. Η καθοδήγηση και συμπαράσταση της, η αντικειμενική και αμερόληπτη της κρίση, η ξεκάθαρη και παράλληλα αυστηρή άποψη της για την ποιότητα της ακαδημαϊκής έρευνας, αποτέλεσαν καταλυτικό παράγοντα στην επιτυχή κατάληξη της προσπάθειας μου. Το ήθος, σε συνδυασμό με το επιστημονικό της κύρος, συνθέτουν μια ολοκληρωμένη προσωπικότητα, η οποίος αποτελεί πρότυπο για μένα.

Επίσης θα ήθελα να ευχαριστήσω τον Επίκουρο Καθηγητή Δρ Τζιρίτα Νικόλαο και τον Δρ Κίκιρα Παναγιώτη, οι οποίοι με καθοδήγησαν, μου συμπαραστάθηκαν, με διόρθωσαν και κατάφεραν με τις ικανότητες και τις εμπειρίες τους, να με οδηγήσουν στο επιτυχές αποτέλεσμα.

Οι συνάδελφοι, συμφοιτητές του ΜΠΣ, κατέχουν και θα κατέχουν ξεχωριστή θέση στην καρδιά μου. Τους ευχαριστώ όλους και κάθε έναν ξεχωριστά.

Επίσης ιδιαίτερες ευχαριστίες θα πρέπει να αποδώσω στο σύνολο του διδακτικού προσωπικού του Τμήματος, οι οποίοι με περιβάλανε με ιδιαίτερη αγάπη και εμπιστοσύνη.

Τέλος ευχαριστώ το προσωπικό της γραμματείας που πέραν της προθυμίας και διάθεσης τους για οποιαδήποτε βοήθεια, είχαν πάντα έναν καλό λόγο να μου πουν.

Η κόρη μου Βίκυ, τριτοετής φοιτήτρια σε τμήμα Πληροφορικής της Σχολής Θετικών Επιστημών του ΔΙΠΑΕ και ο γιος μου Σταύρος, δευτεροετής φοιτητής του τμήματος Μηχανικών Χωροταξίας της Πολυτεχνικής Σχολής του ΑΠΘ, αποτελούν το πρότυπο και τον φωτεινό φάρο της ζωής μου. Η αγάπη τους, η στοργή τους και τα χαμόγελα τους, μου δίνουν απίστευτο κουράγιο και δύναμη κάθε μέρα. Η λέξη λατρεία είναι μικρή να περιγράψει το τι νιώθω γι' αυτά. Τους εύχομαι ολόψυχα να πετύχουν τα όνειρα τους.

Τέλος, τίποτα δεν θα είχα καταφέρει εάν δεν είχα αμέριστη και διαρκή συμπαράσταση από την σύζυγο και γυναίκα της ζωής μου, Έφη. Από την πρώτη στιγμή, ήταν στο πλευρό μου, να με στηρίζει, να με ενθαρρύνει και να με εμψυχώνει. Ανέχτηκε υπομονετικά τις γκρίνιες και τα προβλήματα μου, την απόσταση, τις ταλαιπωρίες, τις οικονομικές δυσχέρειες. Στάθηκε δίπλα μου με υπομονή, αναλαμβάνοντας όλες τις υποχρεώσεις της οικογένειας, προκειμένου να έχω τον χρόνο να ασχοληθώ με τις σπουδές μου. Ειδικότερα τώρα, στην κρισιμότερη φάση της ζωής μου, το χαμόγελο της με πλημυρίζει δύναμη και αισιοδοξία.

Της αφιερώνω λοιπόν την Μεταπτυχιακή μου διατριβή με όλη μου την αγάπη και την αφοσίωση.

Περίληψη

Η μεγιστοποίηση της παραγωγικής διαδικασίας στη σύγχρονη βιομηχανία, όπως αυτή προτάσσεται και πριμοδοτείτε από το πρότυπο Industry 4.0, προϋποθέτει ευρεία χρήση κυβερνο-φυσικών συστημάτων τα οποία με βάση τεχνολογίες τεχνητής νοημοσύνης, παρακολουθούν και εποπτεύουν τις φυσικές διαδικασίες, λαμβάνοντας αυτόνομα και αποκεντρωμένα, βέλτιστες αποφάσεις. Επιτρέπεται με αυτό τον τρόπο στον παραγωγικό και μεταποιητικό τομέα να κάνει τεράστια καινοτομικά άλματα, να αποκτήσει σημαντική εξωστρέφεια και να αναπτύξει δραστηριότητες που μέχρι πρότινος ήταν αδύνατες.

Για την επίτευξη των παραπάνω, η υλοποίηση κάθε είδους έξυπνων λύσεων παραγωγής και οργανωτικών ή λειτουργικών υπηρεσιών, ολοκληρώνεται μέσω του επιχειρησιακού δικτύου Industrial Internet of Thing (IIoT), όπου τα αποκεντρωμένα συστήματα επικοινωνούν και συνεργάζονται σε πραγματικό χρόνο. Επίσης, ο επικείμενος μετασχηματισμός της βιομηχανίας σε μια πλήρως αυτοματοποιημένη διαδικασία, προϋποθέτει την συνεχή και αέναη συλλογή πληροφοριών από κάθε παραγωγικό στάδιο, προκειμένου να διερευνηθεί πολύπλευρα η ενεστώσα, αλλά και η ιστορική κατάσταση των παραγωγικών διαδικασιών.

Η συλλογή των υπόψη πληροφοριών οι οποίες βελτιστοποιούν την αποτελεσματικότητα των αποφάσεων, συνεπάγονται την ανάγκη διαχείρισης και ανάλυσης μεγάλης κλίμακας δεδομένων (big data), τα οποία προέρχονται από ετερογενείς πηγές, είναι ετερόκλητα και τις περισσότερες φορές μη διαλειτουργικά. Η διαχείριση των συγκεκριμένων μεγάλων δεδομένων, περιπλέκεται ακόμη περισσότερο, από την ανάγκη προστασίας της πληροφορίας ως σημαντικότατο περιουσιακό αγαθό, της εξασφάλισης του εμπορικού απορρήτου και της διασφάλισης της ιδιωτικότητας βάση του πρόσφατου Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation – GDPR).

Επιπρόσθετα, τα συστήματα ανάλυσης δεδομένων μεγάλης κλίμακας, λαμβάνουν μια συνεχής, απεριόριστη εισροή παρατηρήσεων όπου στην τυπική περίπτωση, τα νεότερα δεδομένα είναι και τα σημαντικότερα, καθώς υφίσταται η έννοια της παλαίωσης με βάση τον χρονικό τους προσδιορισμό. Οι ροές αυτές δεδομένων, χαρακτηρίζονται από υψηλή μεταβλητότητα, καθώς τα χαρακτηριστικά τους μπορούν να αλλάξουν δραστικά και με μη προβλέψιμο τρόπο κατά την πάροδο του χρόνου, αλλάζοντας την τυπική, φυσιολογική τους συμπεριφορά.

Με δεδομένη λοιπόν την αυξανόμενη πολυπλοκότητα και το διαρκώς μεταβαλλόμενο, κατανεμημένο βιομηχανικό περιβάλλον, σε συνδυασμό με την αδυναμία των παραδοσιακών συστημάτων, τα οποία αδυνατούν στις περισσότερες των περιπτώσεων να εναρμονιστούν με τις σύγχρονες προκλήσεις, επιβάλλεται η χρήση εναλλακτικών, δραστικότερων και ουσιαστικότερων μεθόδων ανάλυσης, ασφάλειας και προστασίας των βιομηχανικών δεδομένων και συνάμα υποδομών.

Ιδανική λύση προβάλει η υιοθέτηση ευφυών λύσεων τεχνητής νοημοσύνης, οι οποίες είναι ικανές να επιδεικνύουν λογική, εμπειρική μάθηση και ικανότητες λήψης βέλτιστων αποφάσεων, αφού εκπαιδευτούν κατάλληλα από ιστορικά δεδομένα, αντιπροσωπευτικά του προβλήματος που προσπαθούν να επιλύσουν.

Στις περισσότερες των περιπτώσεων, δεν είναι δυνατή ή δεν ενδείκνυται η κεντρική αποθήκευση όλων των ιστορικών δεδομένων, γεγονός που επιβάλει την εξόρυξη γνώσης σε πραγματικό χρόνο και πάνω σε ένα υποσύνολο μιας ροής δεδομένων, το οποίο περιέχει ένα

μικρό αλλά πρόσφατο ποσοστό παρατηρήσεων του συνόλου. Το γεγονός αυτό δημιουργεί σοβαρές ενστάσεις σχετικά με την ακρίβεια και την αξιοπιστία των χρησιμοποιούμενων ευφυών αλγορίθμων, οι οποίοι ευτελίζονται με την πάροδο του χρόνου και καταντούν ανίκανοι να ανιχνεύσουν σοβαρές απειλές.

Με βάση το κενό που εντοπίζεται στους τρόπους χειρισμού και διασφάλισης των βιομηχανικών δεδομένων, στην συγκεκριμένη μεταπτυχιακή διατριβή, προτείνεται η ανάπτυξη μιας ολιστικής αρχιτεκτονικής προσαρμοστικής ομοσπονδιακής αυτόματης μετά-μηχανικής μάθησης, με χρήση τεχνολογίας κατανεμημένων μπλοκ εγγραφής, για ψηφιακή ασφάλεια και ιδιωτικότητα στο πρότυπο Industry 4.0. Η υπόψη αρχιτεκτονική συνδυάζει κάτω από ένα βέλτιστο και αποδοτικό πλαίσιο, τις πλέον σύγχρονες τεχνολογίες ανάπτυξης σύγχρονου λογισμικού, με σκοπό την πρόβλεψη και την αξιολόγηση των συνθηκών που σχετίζονται με τις απειλές στο βιομηχανικό οικοσύστημα, διασφαλίζοντας παράλληλα την ιδιωτικότητα και το βιομηχανικό απόρρητο.

Λέξεις Κλειδιά

Κατανεμημένη Υπολογιστική Νοημοσύνη, Προσαρμοστική Ομοσπονδιακή Μάθηση, Αυτόματη Μηχανική Μάθηση, Μετά-Μάθηση, Κατανεμημένα Μπλοκ Εγγραφής, Ψηφιακή Ασφάλεια, Ανίχνευση Ανωμαλιών, Ιδιωτικότητα, Ροές Δεδομένων, Βιομηχανία 4.0.

Abstract

As proposed by Industry 4.0, the maximizing of the production requires the use of AI cyber-physical systems that supervise the industrial processes in order to make autonomous and decentralized decisions. To achieve the above, the implementation of any kind of intelligent production solutions or operational services is completed through the Industrial Internet of Thing (IIoT) network, where decentralized systems communicate and collaborate in real-time.

Also, the impending transformation of the industry into a fully automated process presupposes the endless storage of information from each stage in the production chain. The amount of stored data, which optimizes the effectiveness of decisions, implies the need to manage and analyze big data volumes, which come from heterogeneous and often non-interoperable sources. The management of these big volumes is further complicated by the need for high-security policies and privacy under the recent General Data Protection Regulation (GDPR).

The data analysis systems receive a continuous, unlimited inflow of observations where, in the typical case, the newer data is the most important, as the concept of aging is based on their timing. These data streams are characterized by high volatility, as their characteristics can change drastically and in an unpredictable way over time, altering their typical, normal behavior. Given the increasing complexity of threats, the changing environment and the weakness of traditional systems, which in most cases fail to adapt to modern challenges, the need for alternative more active and more effective security methods keeps increasing. Such approaches are the adoption of intelligent solutions to protect of industrial data and infrastructures.

Intelligent systems are capable, of displaying logical, empirical, and non-human decision-making, since they are trained appropriately by historical data representative of the problem they are trying to solve. In most cases, it is either not possible or it is inappropriate to centrally store all historical data. Thus, we should perform real-time knowledge mining and we should obtain a subset of a data flow containing a small but recent percentage of observations. This fact raises serious objections to the accuracy and reliability of the employed intelligent system algorithms, who have been tame over time and they become incapable of detecting serious threats.

Based on the gap in the ways of handling and securing industrial data, this dissertation proposes a Blockchained Adaptive Federated Auto MetaLearning Architecture for CyberSecurity and Privacy in Industry 4.0. The architecture combines, under an optimal and efficient framework, the most modern and efficient technologies in order to protect the industrial ecosystem, while ensuring privacy and industrial secrecy.

Keywords

Distributed Computational Intelligence, Adaptive Federated Learning, Auto-Machine Learning, Meta-Learning, Blockchain, Cyber Security, Anomaly Detection, Privacy, Data Streams, Industry 4.0.

Δομή

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή, παρουσιάζεται ο σκοπός και τίθενται οι επιμέρους στόχοι της διατριβής. Επίσης, αναλύεται η μεθοδολογία έρευνας που ακολουθήθηκε, γίνεται μια βιβλιογραφική ανασκόπηση και αξιολόγηση των δημοσιευμένων ερευνών στο γνωστικό αντικείμενο των θεμάτων που διαπραγματεύεται και τέλος παρουσιάζεται το ερευνητικό κενό που καλείται να καλύψει η προτεινόμενη αρχιτεκτονική.

Στο δεύτερο κεφάλαιο, παρουσιάζεται το πρότυπο Industry 4.0, ενώ παράλληλα αναλύονται διεξοδικά τα θέματα που σχετίζονται με τις τεχνολογίες συλλογής και ανάλυσης των δεδομένων μεγάλης κλίμακας που παράγουν οι υπόψη υποδομές. Επιπρόσθετα, παρουσιάζονται τα θέματα που αφορούν την ψηφιακή ασφάλεια των βιομηχανικών υποδομών και των κυβερνο-φυσικών συστημάτων και γίνεται μια ενδελεχή παρουσίαση σχετικά με την προστασία του βιομηχανικού κι εμπορικού απορρήτου στα σύγχρονα κατανεμημένα περιβάλλοντα μονάδων μαζικής παραγωγής.

Στο τρίτο κεφάλαιο, παρουσιάζεται η προτεινόμενη αρχιτεκτονική, γίνεται μια διεξοδική παράθεση των απαιτήσεων των σύγχρονων πληροφοριακών συστημάτων και με βάση τις υπόψη απαιτήσεις, παρουσιάζονται οι χρησιμοποιούμενες αρχιτεκτονικές και οι τεχνολογίες ανάπτυξης της.

Στο τέταρτο κεφάλαιο, τεκμηριώνεται η προτυποποίηση των διαδικασιών λειτουργίας και ο τρόπος εφαρμογής της προτεινόμενης αρχιτεκτονικής. Επίσης παρατίθεται και αναλύεται ένα λεπτομερές σενάριο χρήσης του τρόπου λειτουργίας της και των λειτουργικών απαιτήσεων που αυτή προϋποθέτει, με σκοπό να καθορισθεί μια σαφής και συνεπή περιγραφή του τρόπου υποστήριξης των επιχειρησιακών δυνατοτήτων της. Επιπρόσθετα, παρουσιάζονται πέντε ανεξάρτητες εφαρμογές που αναπτύχθηκαν και δημοσιεύτηκαν σε διεθνή επιστημονικά περιοδικά και πρακτικά συνεδρίων με βάση την ιδέα προτυποποίησης της συγκεκριμένης αρχιτεκτονικής, υλοποιώντας τμηματικά τα βασικά δομικά λειτουργικά πλαίσια που την απαρτίζουν.

Τέλος η διατριβή ολοκληρώνεται με το πέμπτο κεφάλαιο, στο οποίο προκειμένου να αναλυθεί, να τεκμηριωθεί και να επιβεβαιωθεί το νόημα των πρωτογενών και δευτερογενών στοιχείων της έρευνας που διεκπεραιώθηκε, πραγματοποιείται συζήτηση, παρουσίαση των καινοτομιών που αναπτύχθηκαν, κριτική ανάλυση και αξιολόγηση της προτεινόμενης αρχιτεκτονικής, συνοδευόμενη από πιθανές μελλοντικές κατευθύνσεις και εν γένει βελτιώσεις που μπορούν να την αναβαθμίσουν.

Πίνακας Περιεχομένων

Περίληψη ..... **XII**

Abstract ..... **XIV**

Δομή ..... **XV**

Κατάλογος Σχημάτων ..... **XVIII**

Κατάλογος Δημοσιεύσεων ..... **XIX**

1. Εισαγωγή **2**

1.1 Σκοπός και Στόχοι *3*

1.2 Μεθοδολογία έρευνας *4*

1.3 Βιβλιογραφική Ανασκόπηση *5*

1.4 Αξιολόγηση Βιβλιογραφίας και Ερευνητικό Κενό *7*

2. Ψηφιακή Ασφάλεια και Δεδομένα Μεγάλης Κλίμακας στο Πρότυπο Industry 4.0 ..... **12**

2.1 Το πρότυπο Industry 4.0 ..... *13*

2.1.1 Μοντέλα ανάπτυξης 14

2.1.2 Αρχές σχεδιασμού 15

2.1.3 Δομικά στοιχεία 18

2.2 Δεδομένα μεγάλης κλίμακας *21*

2.2.1 Υποδομές 22

2.2.2 Αναλυτική 23

2.2.3 Αρχιτεκτονικές 23

2.3 Ψηφιακή Ασφάλεια *26*

2.3.1 Ανάλυση δικτυακής κίνησης 28

2.3.2 Ανίχνευση ανωμαλιών 34

2.3.3 Προστασία ιδιωτικότητας και βιομηχανικού απορρήτου 37

3. Προσαρμοστική Ομοσπονδιακή Αυτόματη Μετά-Μάθηση Μέσω Κατανεμημένων Μπλοκ **47**

3.1 Η προτεινόμενη αρχιτεκτονική *48*

3.2 Απαιτήσεις Συστήματος *50*

3.2.1 Γενικές Απαιτήσεις 50

3.2.2 Ειδικές Απαιτήσεις 51

3.2.3 Απαιτήσεις Αρχιτεκτονικής Σχεδίασης 53

3.2.4 Απαιτήσεις Ασφαλείας 53

3.3 Χρησιμοποιούμενες Αρχιτεκτονικές *54*

3.3.1 Ομόσπονδη Μάθηση (Federated Learning) 54

3.3.2 Κατανεμημένη Αρχιτεκτονική (Distributed Architecture) 55

3.3.3 Αρχιτεκτονική Κοντέινερ (Containerized Architecture) 57

3.3.4 Υπολογιστική Άκρου (Edge Computing) 58

3.3.5 Αυτόματη Μηχανική Μάθηση (Meta and Auto-Machine Learning) 59

3.4 Τεχνολογίες *64*

3.4.1 Hyperledger Fabric 64

3.4.2 PySyft 65

3.4.3 Docker Compose 66

4. Προτυποποίηση και Εφαρμογή Προτεινόμενου Συστήματος **69**

4.1 Τεχνική Ανάλυση *70*

4.1.1 Συλλέκτης (Collector) 73

4.1.2 Αναλυτής (Analyzer) 74

4.1.3 Αυτοματοποίηση Νευρωνικών Δικτύων (Neural Search Module) 75

4.1.4 Αγγελιοφόρος (Messenger) 78

4.1.5 Διαχειριστής Ροής (Streamer) 80

4.1.6 Κρυπτογράφος (Crypto Module) 81

4.1.7 Σύστημα Ομοσπονδιακής Μάθησης (Federating Module) 82
4.1.8 Μηχανισμός Αλυσίδας Μπλοκ (Blockchain Module) 84
4.1.9 Σύστημα Οπτικοποίησης (Elastic Stack Module) 85
4.1.10 Σύστημα Διαφύλαξης Απορρήτου (Privacy Module) 86

4.2 Σενάριο Χρήσης 86
4.2.1 Βήμα 1ο – Συλλογή ροών δεδομένων (Collector) 92
4.2.2 Βήμα 2ο – Ανάλυση δικτυακής κίνησης (Analyzer) 92
4.2.3 Βήμα 3ο – Αυτόματη δημιουργία Νευρωνικού Δικτύου (Neural Search Module) 94
4.2.4 Βήμα 4ο – Δρομολόγηση πληροφορίας (Messenger) 95
4.2.5 Βήμα 5ο – Διαχείριση ροής (Streamer) 95
4.2.6 Βήμα 6ο – Κρυπτογράφηση ροής (Crypto Module) 96
4.2.7 Βήμα 7ο – Μηχανισμός ομοσπονδιακής μάθησης (Federating Module) 97
4.2.8 Βήμα 8ο – Αλυσίδα μπλοκ εγγραφών (Blockchain Module) 98
4.2.9 Βήμα 9ο – Οπτικοποίηση κατάστασης (Elastic Stack Module) 102
4.2.10 Βήμα 10ο – Προστασία Ιδιωτικότητας (Privacy Module) 103

4.3 Εφαρμογές που αναπτύχθηκαν 104
4.3.1 Network Flow Forensics Using Cybersecurity Intelligence 104
4.3.2 Cyber-Typhon: An Online Multi-Task Anomaly Detection Framework 106
4.3.3 Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks 108
4.3.4 The Next Generation of Cognitive Security Operation Centers for AI enabled Cyber Defence 109
4.3.5 Anomaly Detection via Blockchained Deep Learning Smart Contracts in Industry 4.0 110

5. Συζήτηση – Συμπεράσματα – Μελλοντικές Κατευθύνσεις 115

5.1 Συζήτηση 116

5.2 Καινοτομίες Μεταπτυχιακής Διατριβής 118

5.3 Κριτική 122

5.4 Αξιολόγηση 124
5.4.1 Πλεονεκτήματα 125
5.4.2 Περιορισμοί 126

5.5 Συμπεράσματα 127

5.6 Μελλοντικές Κατευθύνσεις 129

5.7 Επίλογος 130

Βιβλιογραφία 133

Κατάλογος Σχημάτων

Σχήμα 1 - Γραφική αναπαράσταση της Lambda αρχιτεκτονικής (www.ericsson.com/en/blog) 24
Σχήμα 2 - Γραφική αναπαράσταση της Kappa αρχιτεκτονικής (www.ericsson.com/en/blog) 25
Σχήμα 3 - Τεχνικές μοντελοποίησης ομοσπονδιακής μάθησης (https://doi.org/10.1145/3298981) 55
Σχήμα 4 - Σύγκριση τεχνολογιών εικονοποίησης (https://docs.docker.com/) 58
Σχήμα 5 - Αρχιτεκτονική Edge Computing 59
Σχήμα 6 - Οι τρείς στρατηγικές του Neural Architecture Search 63
Σχήμα 7 - Η αρχιτεκτονική του Docker Compose 66
Σχήμα 8 - Η αρχιτεκτονική του Stream4Flow (https://stream4flow.ics.muni.cz/) 72
Σχήμα 9 - Η γραφική απεικόνιση της προτεινόμενης αρχιτεκτονικής 73
Σχήμα 10 - Συλλέκτης 74
Σχήμα 11 - Γραφική απεικόνιση της αρχιτεκτονικής του IPFIXcol (https://stream4flow.ics.muni.cz/) 74
Σχήμα 12 - Αναλυτής 75
Σχήμα 13 - Γραφική απεικόνιση της αρχιτεκτονικής του IPFIXcol με την προσθήκη του ICICFlowMeter 75
Σχήμα 14 - Ο μηχανισμός αυτοματοποίησης Νευρωνικών Δικτύων 76
Σχήμα 15 - Η αρχιτεκτονική του Auto-Keras Neural Architecture Search (https://autokeras.com/) 78
Σχήμα 16 - Αγγελιοφόρος 78
Σχήμα 17 - Σχηματική απεικόνιση των υπηρεσιών του Apache Kafka (https://kafka.apache.org/) 79
Σχήμα 18 - Διαχειριστής ροής 80
Σχήμα 19 - Σχηματική απεικόνιση των υπηρεσιών του Apache Spark (https://spark.apache.org/) 80
Σχήμα 20 - Σχηματική του Apache Spark Streaming (https://spark.apache.org/) 80
Σχήμα 21 - Κρυπτογράφος 81
Σχήμα 22 - Σύστημα ομοσπονδιακής μάθησης 82
Σχήμα 23 - Οριζόντια αρχιτεκτονική ομοσπονδιακής μάθησης (https://medium.com/disassembly/) 83
Σχήμα 24 - Μηχανισμός αλυσίδας μπλοκ 84
Σχήμα 25 - Σύστημα οπτικοποίησης 85
Σχήμα 26 - Σύστημα διαφύλαξης απορρήτου 86
Σχήμα 27 - Γραφική απεικόνιση του Industry 4.0 οικοσυστήματος (www.globalsuccess-club.net/) 87
Σχήμα 28 - Ιεραρχία διεργασιών σύμφωνα με το IEC62264 (www.plattform-i40.de/) 88
Σχήμα 29 - Διαστρωματωμένη επικοινωνία στο IEC62264 (arXiv:1910.00303 [cs.CR]) 89
Σχήμα 30 - Δομή IP επικοινωνίας σε κατανεμημένη βιομηχανία (www.cisco.com/) 89
Σχήμα 31 - Η αρχιτεκτονική του πρωτοκόλλου OPC UA (www.cisco.com/) 90
Σχήμα 32 - Χαρτογράφηση προτύπων στο Industry 4.0 (http://i40.semantic-interoperability.org/) 90
Σχήμα 33 - Πολυωνυμικοί δακτύλιοι (www.wikidata.org/) 96
Σχήμα 34 - Ο διαχειριστής ροής μετά την προσθήκη του PySEAL 97
Σχήμα 35 - Οπτικοποίηση συμβάντων με το Elastic Stack (www.elastic.co/elastic-stack) 102
Σχήμα 36 - Σχηματική απεικόνιση διαφορικής ιδιωτικότητα (www.winton.com/research) 103
Σχήμα 37 – Η αρχιτεκτονική του Network Flow Forensics Framework 105
Σχήμα 38 - Γραφική αναπαράσταση του Cyber-Typhon 107
Σχήμα 39 - Γραφική αναπαράσταση προτεινόμενης Lambda αρχιτεκτονικής 108
Σχήμα 40 - Αρχιτεκτονική ανίχνευσης ανωμαλιών με χρήση έξυπνων συμβολαίων 112

Κατάλογος Δημοσιεύσεων

Journals

1. **Demertzis K.,** Iliadis L., Tziritas N., Kikiras P., (2020), **Anomaly Detection via Blockchained Deep Learning Smart Contracts in Industry 4.0**, Neural Computing & Applications, Springer DOI : 10.1007/s00521-020-05189-8 (**Impact Factor 4.774**).

2. **Demertzis, K.;** Tziritas, N.; Kikiras, P.; Sanchez, S.L.; Iliadis, L., (2019), **The Next Generation Cognitive Security Operations Center: Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks.** Big Data and Cognitive Computing (ISSN 2504-2289) 2019, 3, 6, MDPI.

3. **Demertzis, K.;** Kikiras, P.; Tziritas, N.; Sanchez, S.L.; Iliadis, L., (2018), **The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence.** Big Data and Cognitive Computing (ISSN 2504-2289) 2018, 2, 35, MDPI.

Proceedings of the International Academic Conferences

4. **Demertzis K.,** Iliadis L., Kikiras P., Tziritas N. (2019) **Cyber-Typhon: An Online Multi-task Anomaly Detection Framework.** In: MacIntyre J., Maglogiannis I., Iliadis L., Pimenidis E. (eds) Artificial Intelligence Applications and Innovations. AIAI 2019. IFIP Advances in Information and Communication Technology, vol 559. Springer, Cham.

5. Kikiras P., **Demertzis K.,** Tziritas N., Sanchez S.L., Iliadis L., (2020) **The Next Generation of Cognitive Security Operation Centers for AI enabled Cyber Defence.** In: NATO Cooperative Cyber Defence Centre of Excellence, 13th International Conference on Cyber Conflict (CyCon 2021), 25-28 May 2021 in Tallinn, Estonia, (*in progress*)

Βιβλιογραφία

1. https://www.i-scoop.eu/industry-4-0/
2. Δημητρόπουλος, Ε., (2004). Εισαγωγή στη μεθοδολογία της επιστημονικής έρευνας: προς ένα συστηματικό δυναμικό μοντέλο μεθοδολογίας επιστημονικής έρευνας. Αθήνα: Έλλην.
3. W. Wang, X. Zhang, W. Shi, S. Lian and D. Feng, "Network traffic monitoring, analysis and anomaly detection [Guest Editorial]," in IEEE Network, vol. 25, no. 3, pp. 6-7, May-June 2011, doi: 10.1109/MNET.2011.5772054
4. C. Xu, S. Chen, J. Su, S. M. Yiu and L. C. K. Hui, "A Survey on Regular Expression Matching for Deep Packet Inspection: Applications, Algorithms, and Hardware Platforms," in IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2991-3029, Fourthquarter 2016, doi: 10.1109/COMST.2016.2566669
5. H. Zhang, C. Papadopoulos and D. Massey, "Detecting encrypted botnet traffic," 2013 Proceedings IEEE INFOCOM, Turin, 2013, pp. 3453-1358, doi: 10.1109/INFCOM.2013.6567180
6. R. Scandariato and J. Walden, "Predicting vulnerable classes in an android application," in Proceedings of the 4th international workshop on Security measurements and metrics, 2012
7. Chin E., Felt A., Greenwood K., Wagner D.: Analyzing inter-application communication in android, 9th conf. on Mobile systems, applications, and services. ACM, pp. 239–252 (2011)
8. Burguera I., Zurutuza U., Nadjm-Tehrani S.: Crowdroid: behavior-based malware detection system for android, 1st ACM workshop on on SPSM. ACM, pp. 15–26 (2011)
9. Glodek W., Harang R. R.: Permissions-based Detection and Analysis of Mobile Malware Using Random Decision Forests, IEEE Military Communications Conference, (2013)
10. Zhang, Jun, et al. "An effective network traffic classification method with unknown flow detection." Network and Service Management, IEEE Transactions on 10.2 (2013): 133-147
11. Gardiner, Joseph, and Shishir Nagaraja. "On the reliability of network measurement techniques used for malware traffic analysis." Security Protocols XXII, 2014. 321-333
12. Wang, Horng-Tzer, et al. "Real-time fast-flux identification via localized spatial geolocation detection." Computer Software and Applications Conference (COMPSAC), 2012 IEEE
13. Tu, Truong Dinh, Cheng Guang, and Liang Yi Xin. "Detecting bot-infected machines based on analyzing the similar periodic DNS queries." 2015 International Conference on Communications, Management and Telecommunications (ComManTel). IEEE, 2015
14. Hsu C.-H. , C.-Y. Huang, Chen K.-T.: Fast-flux bot detection in real time, (2010), in 13th international conference on Recent advances in intrusion detection, ser. RAID'10
15. Haffner P., Sen S., Spatscheck O., Wang D.: ACAS: Auto-mated Construction of Application Signatures, (2005), Proceedings of the ACM SIGCOMM, pp.197-202
16. Alshammari R., Zincir-Heywood N. A.: A flow based approach for SSH traffic detection, (2007), Cy-bernetics, ISIC. IEEE International Conference on, pp.296-301
17. M. Kiran, P. Murphy, I. Monga, J. Dugan and S. S. Baveja, "Lambda architecture for cost-effective batch and speed big data processing," 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, 2015, pp. 2785-2792, doi: 10.1109/BigData.2015.7364082
18. M. HoseinyFarahabady, J. Taheri, Z. Tari and A. Y. Zomaya, "A Dynamic Resource Controller for a Lambda Architecture," 2017 46th International Conference on Parallel Processing (ICPP), Bristol, 2017, pp. 332-341, doi: 10.1109/ICPP.2017.42
19. U. Suthakar, L. Magnoni, D. R. Smith and A. Khan, "Optimised lambda architecture for monitoring WLCG using spark and spark streaming," 2016 IEEE Nuclear Science Symposium, Medical Imaging Conference and Room-Temperature Semiconductor Detector Workshop (NSS/MIC/RTSD), Strasbourg, 2016, pp. 1-2, doi: 10.1109/NSSMIC.2016.8069637
20. Y. Yamato, H. Kumazaki and Y. Fukumoto, "Proposal of Lambda Architecture Adoption for Real Time Predictive Maintenance," 2016 Fourth International Symposium on Computing and Networking (CANDAR), Hiroshima, 2016, pp. 713-715, doi: 10.1109/CANDAR.2016.0130

21. M. S. Chong, M. Wakaiki and J. P. Hespanha, "Observability of linear systems under adversarial attacks," 2015 American Control Conference (ACC), Chicago, IL, 2015, pp. 2439-2444, doi: 10.1109/ACC.2015.7171098
22. L. Chen, Y. Ye and T. Bourlai, "Adversarial Machine Learning in Malware Detection: Arms Race between Evasion Attack and Defense," 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Greece, 2017, pp. 99-106, doi: 10.1109/EISIC.2017.21
23. Bifet, A., Holmes, G., & Pfahringer, B. (2010). Leveraging bagging for evolving data streams. In PKDD (pp. 135–150)
24. Baena-Garcia, M., del Campo-Avila, J., Fidalgo, R., Bifet, A., Gavalda, R., & Morales-Bueno, R. (2006). Early drift detection method. In ECML PKDD 2006 workshop on knowledge discovery from data streams
25. Qian Chen and Sherif Abdelwahed (2013), A model-based approach to self-protection in computing system, Proceeding CAC '13 Proc of the ACM Cloud and Autonomic Computing Conference, Article No 16
26. Yannis Soupionis, Stavros Ntalampiras and Georgios Giannopoulos, (2016), DOI: 10.1007/978-3-319-31664-2_29 Vol 8985 of the book series Lecture Notes in Computer Science
27. N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," 2017 21st Conference of Open Innovations Association (FRUCT), Helsinki, 2017, pp. 321-329. doi: 10.23919/FRUCT.2017.8250199
28. Arshdeep Bahga, Vijay K. Madisetti, Blockchain Platform for Industrial Internet of Things, Journal of Software Engineering and Applications 09(10):533-546, DOI: 10.4236/jsea.2016.910036
29. J. Gao et al., "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," in IEEE Access, vol. 6, pp. 9917-9925, 2018. doi: 10.1109/ACCESS.2018.2806303
30. Llopis, S. et al. "A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military", DOI: 10.1109/ICMCIS.2018.8398693, IEEE International Conference on Military Communications and Information Systems (ICMCIS), 2018
31. https://el.wikipedia.org
32. D. Xu, W. He and S. Li, "Internet of Things in Industries: A Survey," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243, Nov. 2014. doi: 10.1109/TII.2014.2300753
33. Weyer S, Schmitt M, Ohmer M, Gorecky D. Towards Industry 4.0 - Standardization as the crucial challenge for highly modular, multi-vendor production systems. IFAC-PapersOnLine. 2015 Jan 1;48(3):579–84.
34. Pereira AC, Romero F. A review of the meanings and the implications of the Industry 4.0 concept. Procedia Manufacturing. 2017 Jan 1;13:1206–14.
35. F.-Z. Benjelloun, A. A. Lahcen, and S. Belfkih, "An overview of big data opportunities, applications and tools," in 2015 Intelligent Systems and Computer Vision (ISCV), Mar. 2015, pp. 1–6, doi: 10.1109/ISACV.2015.7105553.
36. Rolf H.Weber, (2015), Internet of things: Privacy issues revisited, Computer Law & Security Review, Volume 31, Issue 5, October 2015, Pages 618-627, Elsevier
37. A. R. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial Internet of Things," 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2015, pp. 1-6. doi: 10.1145/2744769.2747942.
38. R. Boussada, M. E. Elhdhili and L. A. Saidane, "A survey on privacy: Terminology, mechanisms and attacks," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, 2016, pp. 1-7. doi: 10.1109/AICCSA.2016.7945804
39. D. Wang, "An Enterprise Data Pathway to Industry 4.0," IEEE Engineering Management Review, vol. 46, no. 3, pp. 46–48, thirdquarter 2018, doi: 10.1109/EMR.2018.2866157.
40. J. Chen, Q. Jiang, Y. Wang, and J. Tang, "Study of data analysis model based on big data technology," in 2016 IEEE International Conference on Big Data Analysis (ICBDA), Mar. 2016, pp. 1–6, doi: 10.1109/ICBDA.2016.7509810.
41. A. Sanla and T. Numnonda, "A Comparative Performance of Real-time Big Data Analytic Architectures," in 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Jul. 2019, pp. 1–5, doi: 10.1109/ICEIEC.2019.8784580.

42. W. Xi and L. Ling, "Research on IoT Privacy Security Risks," 2016 International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII), Wuhan, 2016, pp. 259-262. doi: 10.1109/ICIICII.2016.0069
43. M. N. Lakhoua, "Cyber Security of SCADA Network in Thermal Power Plants," in 2018 International Conference on Smart Communications and Networking (SmartNets), Nov. 2018, pp. 1–4, doi: 10.1109/SMARTNETS.2018.8707398.
44. J. Vávra and M. Hromada, "An evaluation of cyber threats to industrial control systems," International Conference on Military Technologies (ICMT) 2015, Brno, 2015, pp. 1-5. doi: 10.1109/MILTECHS.2015.7153700
45. A. A. Ghorbani, Wei Lu, Mahbod Tavallaee, "Network Intrusion Detection and Prevention - Concepts and Techniques". Advances in Information Security, Vol.47 Springer 2010.
46. Cheilas, K., Vakaloudis, A., Politis, A. 2015. TCP/IP Packet Analysis. [Book Chapter]. In Cheilas, K., Vakaloudis, A., Politis, A. 2015. Computer Networks - Laboratory Exercises. [ebook] Athens:Hellenic Academic Libraries Link. chapter 4. Available Online at: http://hdl.handle.net/11419/1767
47. Hugo Gonzalez, M.-A. Gosselin-Lavigne, Natalia Stakhanova, and Ali A. Ghorbani. "The impact of application layer denial of service attacks". In B. Issac and N. Israr, editors, Case Studies in Secure Computing - Achievements and Trends. ISBN# 978-1-4822-0706-4. CRC Press, Taylor and Francis, 2014
48. Z. Trabelsi, S. Zeidan, and M. M. Masud, "Network Packet Filtering and Deep Packet Inspection Hybrid Mechanism for IDS Early Packet Matching," in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Mar. 2016, pp. 808–815, doi: 10.1109/AINA.2016.178.
49. Wei Lu, Mahbod Tavallaee and Ali A. Ghorbani, Hybrid Traffic Classification Approach Based on Decision Tree, Proceedings of the 2009 IEEE Global Telecommunications Conference (GLOBECOM'09), pp. 1-6, December 2009.
50. Gerard Drapper Gil, Arash Habibi Lashkari, Mohammad Mamun, Ali A. Ghorbani, Characterization of Encrypted and VPN Traffic Using Time-Related Features", In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), pages 407-414, Italy, 2016
51. Nari, S.; Ghorbani, A.A., Automated malware classification based on network behaviour, 2013 International Conference on Computing, Networking and Communications (ICNC), vol., no., pp.642,647, 28-31 Jan. 2013.
52. Mahbod Tavallaee, Natalia Stakhanova and Ali A. Ghorbani, Toward Credible Evaluation of Anomaly-based Intrusion Detection Methods, IEEE Transactions on Systems, Man, and Cybernetics--Part C: Applications and Reviews, Vol. 40, No.5, pp.516 - 524, IEEE, 2010.
53. Y. Sani, A. Mohamedou, K. Ali, A. Farjamfar, M. Azman, and S. Shamsuddin, "An overview of neural networks use in anomaly Intrusion Detection Systems," in 2009 IEEE Student Conference on Research and Development (SCOReD), Nov. 2009, pp. 89–92, doi: 10.1109/SCORED.2009.5443289.
54. Georgouli, A. 2015. Μηχανική Μάθηση. [Book Chapter]. In Georgouli, A. 2015. Τεχνητή νοημοσύνη. [ebook] Athens:Hellenic Academic Libraries Link. chapter 4. Available Online at: http://hdl.handle.net/11419/3382
55. Manogaran G., Thota C., Lopez D., Sundarasekar R. (2017) Big Data Security Intelligence for Healthcare Industry 4.0. In: Thames L., Schaefer D. (eds) Cybersecurity for Industry 4.0. Springer Series in Advanced Manufacturing. Springer, Cham
56. http://www.hcg.gr
57. Μαυρίδης, Ι. 2015. Ιδιωτικότητα στο Διαδίκτυο και Κυβερνοέγκλημα. [Κεφάλαιο Συγγράμματος]. Στο Μαυρίδης, Ι. 2015. Ασφάλεια πληροφοριών στο διαδίκτυο. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. κεφ 13. Διαθέσιμο στο: http://hdl.handle.net/11419/1037
58. Tsavli M., Efraimidis , V. Katos, L. Mitrou, Reengineering the user: privacy concerns about personal data on smartphones, Information and Computer Security, Vol. 23, No. 4, pp. 394-405, 2015, Emerald
59. T. H. Szymanski, "Strengthening security and privacy in an ultra-dense green 5G Radio Access Network for the industrial and tactile Internet of Things," 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, 2017, pp. 415-422. doi: 10.1109/IWCMC.2017.7986322

60. C. Occhiuzzi, S. Amendola, S. Manzari and G. Marrocco, "Industrial RFID sensing networks for critical infrastructure security," 2016 46th European Microwave Conference (EuMC), London, 2016, pp. 1335-1338. doi: 10.1109/EuMC.2016.7824598
61. E. Borgia, "The Internet of Things vision : Key features , applications and open issues," Computer Communications, vol. 54, pp. 1–31, 2014.
62. M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang and X. Shen, "PaRQ: A Privacy-Preserving Range Query Scheme Over Encrypted Metering Data for Smart Grid," in IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, pp. 178-191, June 2013. doi: 10.1109/TETC.2013.2273889
63. Borgia, "The Internet of Things vision : Key features , applications and open issues," Computer Communications, vol. 54, pp. 1–31, 2014.
64. Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, Hannu Tenhunen, SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways, In Procedia Computer Science, Volume 52, 2015, Pages 452-459, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.05.013
65. Joshua Joy, Minh Le, Mario Gerla, (2017), LocationSafe: Granular Location Privacy for IoT Devices, Cryptography and Security, arXiv:1606.09605
66. M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.
67. H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.
68. S. E. Chang and Y. Chen, "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications," IEEE Access, vol. 8, pp. 62478–62494, 2020, doi: 10.1109/ACCESS.2020.2983601.
69. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.
70. J. Lu, A. Liu, F. Dong, F. Gu, J. Gama, and G. Zhang, "Learning under Concept Drift: A Review," IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 12, pp. 2346–2363, Dec. 2019, doi: 10.1109/TKDE.2018.2876857.
71. Golab L, Ozsu MT. Data Stream Management [Internet]. Morgan & Claypool; 2010 [cited 2020 Jul 22]. Available from: https://ieeexplore.ieee.org/document/6813254
72. "IEEE Draft Guide for Architectural Framework and Application of Federated Machine Learning," IEEE P3652.1/D6, April 2020, pp. 1–70, Jun. 2020.
73. https://gdpr-info.eu/
74. http://www.opengov.gr/minreform/?p=1627
75. M. Singh, "An Overview of Grid Computing," in 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Oct. 2019, pp. 194–198, doi: 10.1109/ICCCIS48478.2019.8974490.
76. A. Chandra, J. Weissman, and B. Heintz, "Decentralized Edge Clouds," IEEE Internet Computing, vol. 17, no. 5, pp. 70–73, Sep. 2013, doi: 10.1109/MIC.2013.93.
77. F. M. Benčić and I. Podnar Žarko, "Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph," in 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Jul. 2018, pp. 1569–1570, doi: 10.1109/ICDCS.2018.00171.
78. https://www.docker.com/
79. M. M. Rovnyagin, A. V. Guminskaia, A. A. Plyukhin, A. P. Orlov, F. N. Chernilin, and A. S. Hrapov, "Using the ML-based architecture for adaptive containerized system creation," in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Jan. 2018, pp. 358–360, doi: 10.1109/EIConRus.2018.8317106.

80. A. Ahmed and G. Pierre, “Docker Image Sharing in Distributed Fog Infrastructures,” in 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Dec. 2019, pp. 135–142, doi: 10.1109/CloudCom.2019.00030.
81. K. Cao, Y. Liu, G. Meng, and Q. Sun, “An Overview on Edge Computing Research,” IEEE Access, vol. 8, pp. 85714–85728, 2020, doi: 10.1109/ACCESS.2020.2991734.
82. A. Makmal, A. A. Melnikov, V. Dunjko, and H. J. Briegel, “Meta-learning within Projective Simulation,” IEEE Access, vol. 4, pp. 2110–2122, 2016, doi: 10.1109/ACCESS.2016.2556579.
83. Z. Xu, L. Cao, and X. Chen, “Learning to Learn: Hierarchical Meta-Critic Networks,” IEEE Access, vol. 7, pp. 57069–57077, 2019, doi: 10.1109/ACCESS.2019.2914469.
84. Elsken, Thomas; Metzen, Jan Hendrik; Hutter, Frank (August 8, 2019). "Neural Architecture Search: A Survey". Journal of Machine Learning Research. 20 (55): 1–21. arXiv:1808.05377
85. arXiv:1812.07995 [cs.LG]
86. https://www.hyperledger.org/
87. https://github.com/OpenMined/PySyft
88. arXiv:1811.04017 [cs.LG]
89. https://docs.docker.com/compose/
90. https://machinelearningmastery.com/
91. https://stream4flow.ics.muni.cz/
92. T. Jirsik, “Stream4Flow: Real-time IP flow host monitoring using Apache Spark,” in NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, Apr. 2018, pp. 1–2, doi: 10.1109/NOMS.2018.8406132.
93. https://github.com/CESNET/ipfixcol
94. https://kafka.apache.org/
95. https://spark.apache.org/
96. https://www.elastic.co/elastic-stack
97. https://blog.paperspace.com/neural-architecture-search-controllers/
98. https://autokeras.com/
99. arXiv:1806.10282 [cs.LG]
100. https://aws.amazon.com/kinesis/
101. C. Zhao et al., “Secure Multi-Party Computation: Theory, practice and applications,” Information Sciences, vol. 476, pp. 357–372, Feb. 2019, doi: 10.1016/j.ins.2018.10.024.
102. Armknecht, Frederik; Boyd, Colin; Gjøsteen, Kristian; Jäschke, Angela; Reuter, Christian; Strand, Martin (2015). "A Guide to Fully Homomorphic Encryption
103. http://i40.semantic-interoperability.org/
104. arXiv:1910.00303 [cs.CR]
105. https://www.rtautomation.com/technologies/modbus-tcpip/
106. https://www.unb.ca
107. https://www.microsoft.com/en-us/research/project/microsoft-seal/
108. https://www.microsoft.com/en-us/research/uploads/prod/2017/11/sealmanual-2-3-1.pdf
109. Dwork, Cynthia (2008-04-25). "Differential Privacy: A Survey of Results". In Agrawal, Manindra; Du, Dingzhu; Duan, Zhenhua; Li, Angsheng (eds.). Theory and Applications of Models of Computation. Lecture Notes in Computer Science. 4978. Springer Berlin Heidelberg. pp. 1–19. doi:10.1007/978-3-540-79228-4_1. ISBN 9783540792277.
110. S. Cronholm and G. Goldkuhl, “Strategies for information systems evaluation-six generic types,” Electronic Journal of Information Systems Evaluation, Vol. 6, No. 2, pp. 65–74, 2003.