ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Τεχνητά Ανοσοποιητικά Συστήματα για Ανίχνευση Χρηματοοικονομικής Απάτης: Ανασκόπηση Βιβλιογραφίας και Ανάπτυξη Εφαρμογής»

Του φοιτητή
Ποντικάκη Δημήτρη
Αρ. Μητρώου: 144240

Επιβλέπων
Αδαμίδης Παναγιώτης
Καθηγητής

Σεπτέμβριος 2023

Τεχνητά Ανοσοποιητικά Συστήματα για Ανίχνευση Χρηματοοικονομικής Απάτης: Ανασκόπηση Βιβλιογραφίας και Ανάπτυξη Εφαρμογής

Κωδικός Δ.Ε. 23164

Ποντικάκης Δημήτρης

Ονοματεπώνυμο εισηγητή: Αδαμίδης Παναγιώτης

Ημερομηνία ανάληψης Δ.Ε. 22-03-2023

Ημερομηνία περάτωσης Δ.Ε. 10-09-2023

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η οικονομική απάτη αποτελεί αυξανόμενη ανησυχία στη σημερινή ψηφιακή εποχή, προκαλώντας σημαντικές οικονομικές απώλειες και υπονομεύοντας την εμπιστοσύνη στα χρηματοπιστωτικά συστήματα. Οι παραδοσιακές μέθοδοι ανίχνευσης της απάτης είναι όλο και πιο ανεπαρκείς, καθώς συχνά αδυνατούν να προσαρμοστούν στις εξελιγμένες τεχνικές που χρησιμοποιούν οι σύγχρονοι απατεώνες. Τα Τεχνητά Ανοσοποιητικά Συστήματα (ΤΑΣ), εμπνευσμένα από τα βιολογικά ανοσοποιητικά συστήματα, προσφέρουν μια πολλά υποσχόμενη εναλλακτική λύση. Είναι εγγενώς προσαρμοστικά, ικανά να μαθαίνουν από νέους τύπους απειλών και μπορούν να εφαρμοστούν σε πληθώρα σεναρίων, καθιστώντας τα κατάλληλα για την ανίχνευση της χρηματοπιστωτικής απάτης. Ο συνδυασμός της επιστήμης των οικονομικών με την επιστήμη των υπολογιστών είναι δύο κλάδοι που μου προκαλούν ενδιαφέρον και ευελπιστώ να ασχοληθώ είτε επαγγελματικά είτε ακαδημαϊκά και είναι ο κυριότερος λόγος που επέλεξα αυτό το θέμα για την πτυχιακή μου εργασία.

Περίληψη

Το θέμα της πτυχιακής εργασίας “Τεχνητά Ανοσοποιητικά Συστήματα για Ανίχνευση Χρηματοοικονομικής Απάτης: Ανασκόπηση Βιβλιογραφίας και Ανάπτυξη Εφαρμογής” έχει να κάνει με την χρήση των τεχνικών και μεθοδολογιών Μηχανικής Μάθησης (ΜΜ), Τεχνητής Νοημοσύνης (ΤΝ) και Τεχνητών Ανοσοποιητικών Συστημάτων (ΤΑΣ) για την εύρεση απάτης σε χρηματοοικονομικά δεδομένα. Αρχικά γίνεται μια συνοπτική περιγραφή του ανοσολογικού συστήματος των θηλαστικών και μια επεξήγηση των μηχανισμών άμυνας που ενεργοποιούνται για την αντιμετώπιση των επιβλαβών παθογόνων μικροοργανισμών. Έπειτα, συστήνονται τα ΤΑΣ που βασίζονται στο βιολογικό ανοσοποιητικό σύστημα και παρουσιάζονται οι πιο γνωστοί αλγόριθμοι που εμπνέονται από αυτό αλλά και διάφορες παραλλαγές τους και εφαρμογές τους σε προβλήματα μηχανικής. Ύστερα, δίνεται ένας ορισμός της χρηματοοικονομικής απάτης, των κυριότερων τύπων απάτης που συναντάμε στην βιβλιογραφία και παρουσιάζονται σχετικές μελέτες και εργασίες που χρησιμοποιούν είτε τεχνικές ΤΑΣ, είτε ΤΝ είτε ΜΜ για να εντοπίσουν και να καταπολεμήσουν τις απάτες. Στο τέλος, γίνεται η περιγραφή του μοντέλου ΤΑΣ που δημιουργήσαμε για την εύρεση απάτης σε οικονομικά δεδομένα και παρουσιάζονται τα αποτελέσματα αυτού του μοντέλου σε σύγκριση με ήδη υπάρχοντα μοντέλα ΜΜ.

Artificial Immune Systems for Financial Fraud Detection: Literature Review and Application Development

Dimitris Pontikakis

Abstract

The digital revolution in the financial sector, while presenting numerous benefits, has simultaneously introduced a new era of sophisticated financial fraudulent activities. Conventional fraud detection methods often struggle to identify these evolving threats in a timely and effective manner. Taking inspiration from the biological immune system, which has evolved over millennia to detect and neutralize threats, this final year thesis explores the potential of Artificial Immune Systems (AIS) in detecting financial fraud.

By understanding the principles of the biological immune system and essential approaches and methodologies of AIS, an intelligent system referred to as NSFDA (Negative Selection Fraud Detection Algorithm) has been developed. The NSFDA, inspired by the Negative Selection Theory, was applied to financial data to detect anomalies that indicate fraud. Comparative analysis revealed that NSFDA outperformed several well-known machine learning algorithms in terms of fraud detection.

The outcomes of this study emphasize the potential of AIS-based models in addressing the challenges of financial fraud. Furthermore, they highlight the necessity for adaptive, evolutionary systems within the constantly changing landscape of the financial sector.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

ΤΑΣ	Τεχνητά Ανοσοποιητικά Συστήματα
AIS	Artificial Immune Systems
ΤΝ	Τεχνητή Νοημοσύνη
ΜΜ	Μηχανική Μάθηση
NSFDA	Negative Selection Fraud Detection Algorithm
IC	Immunological Computation
CST	Clonal Selection Theory
CLONALG	Clonal Selection Algorithms
NSA	Negative Selection Algorithms
AINE	Artificial Immune Networks
DCA	Dendritic Cell Algorithms
DT	Danger Theory
ΘΚ	Θεωρία Κινδύνου
DCA	Dendritic Cells Algorithm
APC	Antigen-Presenting Cells
ACFE	Association of Certified Fraud Examiners
AIRS	Artificial Immune Recognition System
BLAST	Basic Local Alignment Search Tool
SSAHA	Sequence Search and Alignment by Hashing Algorithm
UNSA	Unmodified Negative Selection Algorithm
MNSA	Modified Negative Selection Algorithm
SVM	Support Vector Machines
AFDM	AIS-based Fraud Detection Model
MLFF	Multilayer Feed Forward Neural Network
GMDH	Group Method of Data Handling
PNN	Probabilistic Neural Network
MLP	Multilayer Perceptron

ACHP	Analytic Contribution Hierarchy Process
PST	Pharmacopoeia Spectrum Tree
CART	Classification and Regression Trees
CSPRA	Conserved Self Pattern Recognition Algorithm
RMP	Risk Management Pipeline
AML	Anti-Money Laundering
IAMLS	Intelligent Agent-based AML System
AUPRC	Area Under Precision/Recall Curve

Κεφάλαιο 1ο: Εισαγωγή

Η άνοδος των τεχνολογικών εξελίξεων έχει επιφέρει πολυάριθμα οφέλη στον χρηματοπιστωτικό τομέα, εξορθολογίζοντας τις λειτουργίες και βελτιώνοντας τη συνολική αποτελεσματικότητα των οικονομικών συναλλαγών. Ωστόσο, έχει επίσης οδηγήσει σε αύξηση των εξελιγμένων χρηματοπιστωτικών απατών, οι οποίες αποτελούν σημαντική απειλή για την ακεραιότητα του χρηματοπιστωτικού συστήματος. Οι παραδοσιακές μέθοδοι ανίχνευσης της απάτης, αν και αποτελεσματικές ως ένα βαθμό, συχνά δυσκολεύονται να συμβαδίσουν με τις εξελισσόμενες τακτικές των απατεώνων. Ως εκ τούτου, υπάρχει επείγουσα ανάγκη για πιο έξυπνα και προσαρμοστικά συστήματα ικανά για έγκαιρη ανίχνευση της απάτης.

Με βάση τις αρχές του βιολογικού ανοσοποιητικού συστήματος, τα Τεχνητά Ανοσοποιητικά Συστήματα (ΤΑΣ) – Artificial Immune Systems (AIS) έχουν αναδειχθεί ως μια νέα υπολογιστική προσέγγιση στην επίλυση προβλημάτων. Τα ΤΑΣ, εμπνευσμένα από τους ποικίλους μηχανισμούς του βιολογικού ανοσοποιητικού συστήματος, έχουν εφαρμοστεί σε διάφορους τομείς, από την ανίχνευση ανωμαλιών έως τα προβλήματα βελτιστοποίησης, την αναγνώριση προτύπων, την εξόρυξη δεδομένων κ.α. Η ευελιξία και η προσαρμοστικότητα των ΤΑΣ τα καθιστούν ιδιαίτερα κατάλληλα για την αντιμετώπιση των προκλήσεων ανίχνευσης της χρηματοπιστωτικής απάτης.

Ο πρωταρχικός στόχος της παρούσας πτυχιακής εργασίας είναι να διερευνήσει τις δυνατότητες των τεχνητών ανοσοποιητικών συστημάτων στην ανίχνευση χρηματοοικονομικής απάτης. Επιπλέον, με την κατανόηση των αρχών του βιολογικού ανοσοποιητικού συστήματος και των μεθοδολογιών των ΤΑΣ, η παρούσα πτυχιακή εργασία αποσκοπεί στην ανάπτυξη ενός ευφυούς συστήματος - NSFDA (Negative Selection Fraud Detection Algorithm) - το οποίο αξιοποιεί τα πλεονεκτήματα των ΤΑΣ για την ενισχυμένη ανίχνευση χρηματοοικονομικής απάτης.

Η πτυχιακή εργασία είναι οργανωμένη σε επτά κεφάλαια. Στο τρέχον πρώτο κεφάλαιο παρουσιάζεται το ευρύτερο πλαίσιο της εργασίας, και περιγράφονται ο στόχος και ο σκοπός της. Στο δεύτερο κεφάλαιο παρουσιάζεται σύντομα το βιολογικό ανοσοποιητικό σύστημα και γίνεται αναφορά στους τύπους και τα επίπεδα ανοσίας. Στο τρίτο κεφάλαιο παρέχεται μια επισκόπηση των τεχνητών ανοσοποιητικών συστημάτων, παρακολουθώντας συνοπτικά την ιστορία τους, τις εφαρμογές τους στον πραγματικό κόσμο και παρουσιάζοντας τέσσερις βασικές θεωρίες στις οποίες βασίζονται οι αλγόριθμοι ΤΑΣ. Το τέταρτο κεφάλαιο επικεντρώνεται στον χρηματοπιστωτικό τομέα, επισημαίνοντας διάφορους τύπους χρηματοπιστωτικής απάτης και εξετάζοντας τις υπάρχουσες μεθοδολογίες ανίχνευσης απάτης με βάση τα ΤΑΣ αλλά και τις τεχνικές μηχανικής μάθησης, τεχνητης νοημοσύνης και εξόρυξης δεδομένων. Στο πέμπτο κεφάλαιο παρουσιάζεται το μοντέλο που δημιουργήσαμε (NSFDA), η δομή του αλγορίθμου και τα δεδομένα που χρησιμοποιήθηκαν, ενώ στην συνέχεια παραθέτονται συγκριτικά αποτελέσματα μεταξύ άλλων γνωστών αλγορίθμων μηχανικής μάθησης. Έπειτα, το έκτο κεφάλαιο εξετάζει πιθανές μελλοντικές εργασίες και βελτιώσεις του τρέχοντος μοντέλου και το τελευταίο, έβδομο κεφάλαιο, προσφέρει έναν επίλογο με τα συμπεράσματα.

Κεφάλαιο 2ο: Βιολογικό Ανοσοποιητικό Σύστημα

2.1 Εισαγωγή

Για να κατανοήσουμε ένα τεχνητό ανοσοποιητικό σύστημα πρέπει αρχικά να κατανοήσουμε την λειτουργία του Βιολογικού Ανοσοποιητικού Συστήματος των θηλαστικών. Τα θηλαστικά έχουν αναπτύξει ένα ισχυρό αμυντικό σύστημα που ονομάζεται ανοσοποιητικό σύστημα για την αντιμετώπιση ξένων και δυνητικά επικίνδυνων παθογόνων μικροοργανισμών. Το ανοσοποιητικό σύστημα αποτελείται από ένα σύνολο οργάνων, εξιδεικευμένων κυττάρων και εξωκυτταρικών μορίων που συνεργάζονται για την ανίχνευση και την εξάλειψη των παθογόνων μικροοργανισμών. Αυτή η συντονισμένη αντίδρασή τους όταν παρουσιάζεται ένα παθογόνο είναι γνωστή ως ανοσολογική ή ανοσοβιολογική απόκριση [1]. Η ξένη ουσία που προκαλεί την ανοσοβιολογική απόκριση ονομάζεται αντιγόνο. Ως αντιγόνο μπορεί να δράσει ένας ολόκληρος μικροοργανισμός (π.χ. ιός, βακτήριο κ.ά.), ένα τμήμα αυτού ή τοξικές ουσίες που παράγονται απ' αυτόν. Επίσης ως αντιγόνα μπορούν να δράσουν η γύρη, διάφορες φαρμακευτικές ουσίες, συστατικά τροφών, κύτταρα ή ορός από άλλα άτομα ή ζώα κ.ά. Η ανοσολογία είναι η μελέτη του ανοσοποιητικού συστήματος και των επιπτώσεών του στον οργανισμό. Στην ιατρική, ιστορικά, ο όρος “ανοσία” αναφέρεται στην κατάσταση κατά την οποία ένας οργανισμός μπορεί να αντισταθεί σε ασθένειες, πιο συγκεκριμένα σε μολυσματικές ασθένειες [2].

Με μια ευρύτερη έννοια, η φυσιολογική λειτουργία του ανοσοποιητικού συστήματος είναι να υπερασπίζεται έναν οργανισμό από κάθε είδους επιβλαβείς ουσίες, όπως μύκητες, βακτήρια, παράσιτα, ιούς και άλλα πρωτόζωα. Ωστόσο, μη μολυσματικές εξωτερικές ουσίες μπορούν επίσης να προκαλέσουν ανοσολογικές αντιδράσεις [1].

2.2 Τα επίπεδα του ανοσοποιητικού συστήματος

Το ανοσοποιητικό σύστημα μπορεί να θεωρηθεί ως ένα πολυστρωματικό σύστημα, κάθε στρώμα του οποίου αποτελείται από διαφορετικούς τύπους αμυντικών μηχανισμών [3],[4]. Τα τρία κύρια στρώματα περιλαμβάνουν τον ανατομικό φραγμό, την έμφυτη ανοσία και την προσαρμοστική ανοσία. Οι βιολογικοί αμυντικοί μηχανισμοί μπορούν να ταξινομηθούν σε δύο κατηγορίες: μη ειδικοί και ειδικοί αμυντικοί μηχανισμοί. Οι μη ειδικοί αμυντικοί μηχανισμοί παράγουν τον ίδιο τύπο απόκρισης ανεξάρτητα από το παθογόνο που εισέρχεται στον οργανισμό. Αντίθετα, οι ειδικοί αμυντικοί μηχανισμοί βασίζονται στην αναγνώριση συγκεκριμένων παθογόνων.

Το πρώτο στρώμα της βιολογικής άμυνας είναι οι ανατομικοί φραγμοί, που αποτελούνται από το δέρμα και την επιφάνεια των βλεννογόνων. Το άθικτο δέρμα εμποδίζει την έκρηξη των περισσότερων παθογόνων μικροοργανισμών και επίσης αναστέλλει την ανάπτυξη των περισσότερων βακτηρίων λόγω του χαμηλού pH του. Αντίθετα, πολλά παθογόνα εισέρχονται στον οργανισμό με τη δέσμευση ή τη διείσδυση μέσω των βλεννογόνων μεμβρανών. Ο ρόλος αυτών των μεμβρανών είναι να παρέχουν μια σειρά από μη ειδικούς μηχανισμούς που συμβάλλουν στην πρόληψη αυτών των εισβολών. Για παράδειγμα, το σάλιο, τα δάκρυα και ορισμένες βλεννώδεις εκκρίσεις, οι οποίες περιέχουν αντιβακτηριακές και αντιιικές ουσίες απομακρύνουν τους πιθανούς εισβολείς [4].

Η έμφυτη ανοσία είναι η δεύτερη γραμμή άμυνας κατά των παθογόνων μικροοργανισμών και άλλων επιβλαβών παραγόντων που εισέρχονται στον οργανισμό. Αποτελείται κυρίως από τους ακόλουθους μηχανισμούς [5] :

Φαγοκυτταρικά εμπόδια: Ορισμένα εξειδικευμένα κύτταρα (όπως τα μακροφάγα, τα ουδετερόφιλα και τα κύτταρα φυσικοί "φονείς") είναι ικανά να προσλαμβάνουν ξένες ουσίες, συμπεριλαμβανομένων ολόκληρων παθογόνων μικροοργανισμών. Αυτή η κατάποση έχει δύο σκοπούς: να σκοτώσει το αντιγόνο και να εκθέσει θραύσματα των πρωτεϊνών του εισβολέα σε άλλα κύτταρα και μόρια του ανοσοποιητικού συστήματος. Αυτό εξυπηρετεί, όπως θα δούμε στη συνέχεια, τη δράση των ειδικών μηχανισμών άμυνας.

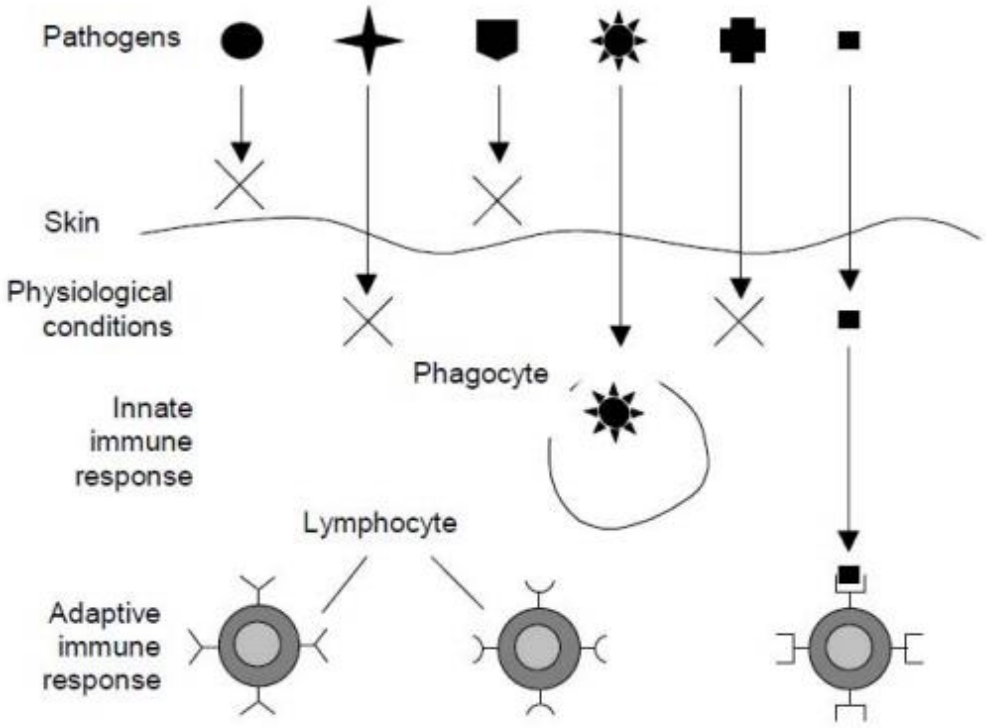
Φλεγμονώδης απόκριση: Τα ενεργοποιημένα μακροφάγα παράγουν κυτταροκίνες ή κυτοκίνες (μικρομοριακές πρωτεΐνες), οι οποίες προκαλούν τη φλεγμονώδη απόκριση που χαρακτηρίζεται από αγγειοδιαστολή και αύξηση της διαπερατότητας των τριχοειδών αγγείων. Οι αλλαγές αυτές επιτρέπουν την προσέλκυση μεγάλου αριθμού κυκλοφορούντων ανοσοκυττάρων στο σημείο όπου συμβαίνει η λοίμωξη.

Η έμφυτη ανοσία είναι σημαντική για τον έλεγχο των λοιμώξεων μέχρι να μπορέσει να ανταποκριθεί το προσαρμοστικό ανοσοποιητικό σύστημα, το οποίο χρειάζεται περισσότερο χρόνο για να αναπτυχθεί. Ενώ η έμφυτη ανοσία δεν είναι ειδική για συγκεκριμένα παθογόνα, εξακολουθεί να είναι αποτελεσματική στην αναγνώριση και την αντίδραση σε ένα ευρύ φάσμα πιθανών απειλών [5].

Η προσαρμοστική ανοσία που ονομάζεται επίσης επίκτητη ή ειδική ανοσία, αντιπροσωπεύει το τμήμα του ανοσοποιητικού μηχανισμού που είναι σε θέση να αναγνωρίζει και να εξαλείφει επιλεκτικά ξένους μικροοργανισμούς και μόρια. Είναι ένας τύπος ανοσίας που αναπτύσσεται μετά την έκθεση του οργανισμού σε ένα συγκεκριμένο αντιγόνο. Ωστόσο, χρειάζεται περισσότερος χρόνος για την ανάπτυξη μιας επίκτητης ανοσολογικής απόκρισης σε σύγκριση με την έμφυτη ανοσολογική απόκριση [3],[6]. Η προσαρμοστική ανοσία παράγει δύο τύπους αποκρίσεων παρουσία παθογόνων μικροοργανισμών: τη χυμική ανοσία και την κυτταρική ανοσία [6]. Η χυμική ανοσία βασίζεται στη σύνθεση αντισωμάτων από τα Β-λεμφοκύτταρα. Ωστόσο, στην κυτταρική ανοσία, τα Τ-λεμφοκύτταρα προκαλούν την καταστροφή των μικροοργανισμών που φέρουν εισβολικά αντιγόνα και εκείνων των αυτοκυττάρων που έχουν μολυνθεί. Πιο αναλυτικά [6] :

Χυμική ανοσία: Η χυμική ανοσία διαμεσολαβείται από αντισώματα που περιέχονται στα υγρά του σώματος (γνωστά ως χυμοί). Ο χυμικός κλάδος του ανοσοποιητικού συστήματος περιλαμβάνει την αλληλεπίδραση Β-λεμφοκυττάρων/αντιγόνου και τον επακόλουθο πολλαπλασιασμό και τη διαφοροποίηση των Β-λεμφοκυττάρων σε πλασματοκύτταρα που εκκρίνουν αντισώματα. Τα αντισώματα είναι πρωτεΐνες που λειτουργούν ως κύτταρα τελεστές της χυμικής απόκρισης δεσμεύοντας αντιγόνα και διευκολύνοντας την εξάλειψή τους.

Κυτταρική ανοσία: Παράλληλα με την ενεργοποίηση των Β-λεμφοκυττάρων, τα βοηθητικά Τ-λεμφοκύτταρα, στην περίπτωση κατά την οποία το αντιγόνο είναι ένα κύτταρο (καρκινικό κύτταρο, κύτταρο μεταμοσχευμένου ιστού ή κύτταρο μολυσμένο από ιό), βοηθούν τον πολλαπλασιασμό και την ενεργοποίηση μιας άλλης ειδικής κατηγορίας Τ-λεμφοκυττάρων, των κυτταροτοξικών Τ-λεμφοκυττάρων, τα οποία θα καταστρέψουν τα κύτταρα - στόχους. Η δράση των βοηθητικών αλλά και των κυτταροτοξικών Τ-λεμφοκυττάρων αποτελεί την κυτταρική ανοσία. Και στις δύο κατηγορίες Τ-λεμφοκυττάρων σχηματίζονται Τ-λεμφοκύτταρα μνήμης, που θα ενεργοποιηθούν σε πιθανή επόμενη επαφή του οργανισμού με το ίδιο αντιγόνο η οποία επιτρέπει στο ανοσοποιητικό σύστημα να ανταποκρίνεται ταχύτερα και αποτελεσματικότερα σε μεταγενέστερη έκθεση στο ίδιο αντιγόνο.



Εικόνα 2.1: Πολυεπίπεδη δομή του ανοσοποιητικού συστήματος [5].

Ανακεφαλαιώνοντας, το ανοσοποιητικό σύστημα είναι ένα εξαιρετικά πολύπλοκο και συντονισμένο σύστημα που προσφέρει στους οργανισμούς μια ισχυρή αμυντική γραμμή εναντίον μιας πληθώρας παθογόνων και άλλων επιβλαβών παραγόντων. Είναι σημαντικό να καταλάβουμε τον τρόπο λειτουργίας και την αλληλεπίδραση των διαφόρων επιπέδων και μηχανισμών της ανοσίας, καθώς αυτό έχει σημαντικές εφαρμογές όχι μόνο στην ιατρική και τη φαρμακολογία αλλά και στην επιστήμη των υπολογιστικών συστημάτων, όπως θα δούμε στην συνέχεια.

Κεφάλαιο 3ο: Τεχνητά Ανοσοποιητικά Συστήματα

3.1 Εισαγωγή

Τα Τεχνητά Ανοσοποιητικά Συστήματα είναι υπολογιστικά μοντέλα που εμπνέονται από τη συμπεριφορά του βιολογικού ανοσοποιητικού συστήματος των θηλαστικών. Όπως το βιολογικό ανοσοποιητικό σύστημα είναι υπεύθυνο για την προστασία του οργανισμού από επιβλαβείς παθογόνους μικροοργανισμούς και ξένες ουσίες έτσι και τα ΤΑΣ έχουν σχεδιαστεί για να μιμούνται αυτή την συμπεριφορά χρησιμοποιώντας αλγόριθμους που αναγνωρίζουν και ανταποκρίνονται σε ένα εύρος εισόδων. Οι αλγόριθμοι που χρησιμοποιούνται στα ΤΑΣ έχουν σχεδιαστεί για να προσομοιώνουν την προσαρμοστική και αυτο-οργανωτική συμπεριφορά του ανοσοποιητικού συστήματος. Αυτοί οι αλγόριθμοι χρησιμοποιούν την αναγνώριση προτύπων, τη μάθηση και τη μνήμη για τον εντοπισμό και την αντίδραση σε δυνητικά επιβλαβή ερεθίσματα [5]. Υπάρχουν διάφοροι αλγόριθμοι που είναι εμπνευσμένοι από ανοσολογικές θεωρίες.

Ένας από τους πρωτοπόρους στην έρευνα πάνω στα ΤΑΣ ήταν ο John Henry Holland**,** ο οποίος το 1989 πρότεινε τον πρώτο αλγόριθμο ΤΑΣ, που ονομάστηκε Σύστημα Ταξινόμησης (Classifier System). Αυτός ο αλγόριθμος χρησιμοποιούσε ένα σύνολο κανόνων για την αναγνώριση μοτίβων στα δεδομένα και ήταν εμπνευσμένος από τον τρόπο με τον οποίο τα αντισώματα αναγνωρίζουν αντιγόνα [7]. Η ιδέα της χρήσης των αρχών του ανοσοποιητικού συστήματος για επίλυση προβλημάτων μηχανικής προτάθηκε για πρώτη φορά από την Stephanie Forrest το 1990 [8], η οποία πρότεινε ότι η ικανότητα του ανοσοποιητικού συστήματος να μαθαίνει και να αναγνωρίζει μοτίβα θα μπορούσε να χρησιμοποιηθεί για την ανάπτυξη αλγορίθμων που έχουν σκοπό την επίλυση πολύπλοκων προβλημάτων.

Γιατί όμως αποτελεί έμπνευση το ανοσοποιητικό σύστημα για τους μηχανικούς και τους επιστήμονες υπολογιστών; Το ανοσοποιητικό σύστημα παρουσιάζει αρκετές ιδιότητες που οι μηχανικοί επιθυμούν να έχουν στα συστήματά τους. Κάποιες βασικές ιδιότητες [9 -11] είναι οι εξής:

Διανομή και αυτοοργάνωση: Η συμπεριφορά του ανοσοποιητικού συστήματος αναπτύσσεται μέσω της δράσης δισεκατομμυρίων παραγόντων (κύτταρα και μόρια) που κατανέμονται σε όλο το σώμα. Τα συλλογικά αποτελέσματά τους μπορεί να είναι εξαιρετικά πολύπλοκα χωρίς να υπάρχει κάποιος κεντρικός έλεγχος. Μια οργανωμένη απόκριση αναδύεται ως μια ιδιότητα σε όλο το σύστημα που προκύπτει από τις συμπεριφορές των παραγόντων χαμηλού επιπέδου. Αυτοί οι ανοσοποιητικοί παράγοντες δρουν ταυτόχρονα καθιστώντας τις ανοσοποιητικές διαδικασίες να χαρακτηρίζονται φυσικά παράλληλες.

Μάθηση, προσαρμογή και μνήμη: Το ανοσοποιητικό σύστημα είναι ικανό να αναγνωρίζει προηγούμενους αθέατους παθογόνους μικροοργανισμούς, επομένως έχει την ικανότητα να μαθαίνει. Η μάθηση προϋποθέτει την ύπαρξη μνήμης, η οποία υπάρχει στο ανοσοποιητικό σύστημα και του επιτρέπει να "θυμάται" παθογόνα που έχει συναντήσει προηγουμένως. Αυτό καλύπτεται από το φαινόμενο των πρωτογενών και δευτερογενών αποκρίσεων. Την πρώτη φορά που συναντάται ένα παθογόνο προκαλείται μια ανοσολογική απόκριση (πρωτογενής απόκριση). Την επόμενη φορά που συναντάται το παθογόνο αυτό εκδηλώνεται μια ταχύτερη και συχνά πιο επιθετική απόκριση (δευτερογενής απόκριση).

Αναγνώριση προτύπων: Μέσω των διαφόρων υποδοχέων και μορίων του, το ανοσοποιητικό σύστημα είναι ικανό να αναγνωρίζει ένα ευρύ φάσμα προτύπων. Αυτό επιτυγχάνεται μέσω υποδοχέων που αντιλαμβάνονται αντιγονικά υλικά σε διαφορετικά πλαίσια (επεξεργασμένα μόρια, ολόκληρα μόρια, πρόσθετα σήματα κ.λπ.). Οι υποδοχείς του έμφυτου ανοσοποιητικού συστήματος διαφέρουν ελάχιστα μεταξύ τους, ενώ οι υποδοχείς του επίκτητου ανοσοποιητικού συστήματος, όπως τα αντισώματα και οι υποδοχείς των Τ-λεμφοκυττάρων, υπόκεινται σε τεράστια ποικιλομορφία.

Ταξινόμηση: Το ανοσοποιητικό σύστημα είναι πολύ αποτελεσματικό στο να διακρίνει τις επιβλαβείς ουσίες από τους ιστούς του ίδιου του σώματος και να κατευθύνει τις ενέργειές του αναλόγως. Από υπολογιστική άποψη, το κάνει αυτό με πρόσβαση σε μία μόνο κατηγορία δεδομένων. Η δημιουργία ενός συστήματος που ταξινομεί αποτελεσματικά τα δεδομένα σε δύο κλάσεις, έχοντας εκπαιδευτεί σε παραδείγματα από τη μία μόνο κλάση, είναι ένα δύσκολο έργο.

Οι έρευνες σχετικά με τα ΤΑΣ μπορούν να χωριστούν σε ανοσοποιητικά μοντέλα, θεωρητικά ΤΑΣ και εφαρμοσμένα ΤΑΣ. Οι ερευνητικές εργασίες σχετικά με τα εφαρμοσμένα ΤΑΣ κυμαίνονται από την ανάπτυξη αλγορίθμων και υπολογιστικών συστημάτων εμπνευσμένων από το ανοσοποιητικό σύστημα, έως την εφαρμογή των ΤΑΣ σε διάφορες εφαρμογές του πραγματικού κόσμου. Αντίθετα, η ανοσολογική μοντελοποίηση περιλαμβάνει ερευνητικές εργασίες που περιγράφουν λεπτομερώς μοντέλα και προσομοιώσεις φυσικών και τεχνητών ανοσολογικών συστημάτων, ενώ τα θεωρητικά ΤΑΣ αποσκοπούν στην περιγραφή των θεωρητικών πτυχών των ΤΑΣ, συμπεριλαμβανομένης της μαθηματικής μοντελοποίησης αλγορίθμων, της ανάλυσης σύγκλισης (convergence analysis) και της ανάλυσης απόδοσης και πολυπλοκότητας των εν λόγω αλγορίθμων [12].

Την τελευταία δεκαετία, η επιστήμη της ανοσολογίας έχει προσελκύσει σημαντική προσοχή ως πηγή έμπνευσης για νέες προσεγγίσεις στην επίλυση σύνθετων υπολογιστικών προβλημάτων. Η εξαιρετικά κατανεμημένη, προσαρμοστική και αυτοοργανωτική φύση του ανοσοποιητικού συστήματος, μαζί με άλλες ιδιότητες που το χαρακτηρίζουν, όπως η μάθηση, η μνήμη, η εξαγωγή χαρακτηριστικών και η αναγνώριση προτύπων προσφέρουν πλούσιες μεταφορές για ένα αντίστοιχο τεχνητό σύστημα. Σε αντίθεση με άλλα τεχνητά συστήματα, τα ΤΑΣ απαιτούν διεπιστημονική συνεργασία μεταξύ ανοσολογίας και μηχανικής [10]. Αρκετοί άλλοι τομείς της ανοσολογίας έχουν γίνει αντικείμενο μελέτης για να εμπνεύσουν την ανάπτυξη αλγορίθμων και υπολογιστικών εργαλείων, για παράδειγμα, η Χυμική Ανοσολογική Απόκριση (Humoral Immunity) [13], η Θεωρία Κινδύνου (Danger Theory) [14], οι λειτουργίες των δενδριτικών κυττάρων (Dendritic Cell functions) [15] και η αναγνώριση προτύπων μοντέλων υποδοχέων (pattern recognition receptor model) [16]. Ωστόσο, αυτοί οι νέοι τομείς είναι σε πρώιμο στάδιο και βρίσκονται υπό συνεχή έρευνα και ανάπτυξη. Επίσης, αν και αναμφισβήτητα έχουν υπάρξει πολλές επιτυχημένες εφαρμογές των ΤΑΣ, υπάρχουν ακόμη πολύ λίγα παραδείγματα που ξεχωρίζουν ως πραγματικά παραδείγματα σοβαρής χρήσης αυτών των συστημάτων στη βιομηχανία.

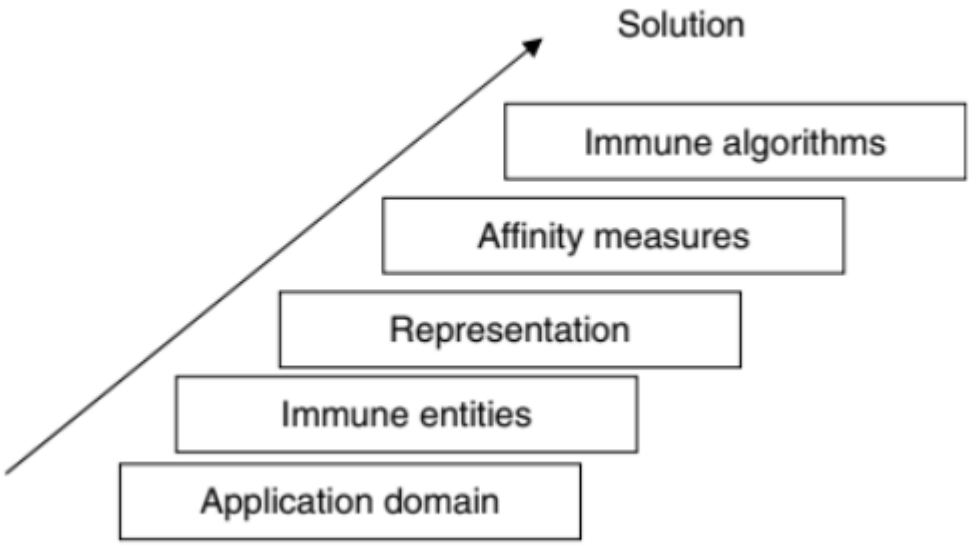
3.2 Προσέγγιση επίλυσης προβλημάτων με χρήση ΤΑΣ

Για την εφαρμογή ενός μοντέλου βασισμένου στο ανοσοποιητικό σύστημα για την επίλυση ενός συγκεκριμένου προβλήματος σε έναν ειδικό τομέα, θα πρέπει να επιλεγεί ο αλγόριθμος ανοσίας ανάλογα με τον τύπο του προβλήματος που πρέπει να επιλυθεί. Κατά συνέπεια, το πρώτο βήμα θα πρέπει να είναι ο προσδιορισμός των στοιχείων που εμπλέκονται στο πρόβλημα και ο προσδιορισμός του τρόπου με τον οποίο μπορούν να μοντελοποιηθούν ως οντότητες σε ένα συγκεκριμένο ΤΑΣ. Με

απλά λόγια μιλάμε για την δημιουργία του συνόλου δεδομένων [5]. Στα ΤΑΣ, η επιλογή της αναπαράστασης των δεδομένων είναι ζωτικής σημασίας και πρέπει να προσαρμόζεται στα δεδομένα του προβλήματος. Για παράδειγμα, η τροποποίηση των δεδομένων για να προσαρμοστούν σε μια συγκεκριμένη αναπαράσταση, όπως η απόρριψη κατηγορικών δεδομένων για να προσαρμοστούν σε μια αναπαράσταση συνεχών τιμών, θεωρείται κακή πρακτική. Τα ΤΑΣ συνήθως ακολουθούν την έννοια του "shape-space" για την αναπαράσταση δεδομένων [9].

Για την κωδικοποίηση αυτών των οντοτήτων, θα πρέπει να επιλεγεί ένα σχήμα αναπαράστασης για τα στοιχεία αυτά, όπως μια αναπαράσταση συμβολοσειράς (string representation), διάνυσμα πραγματικών τιμών ή ακόμα και υβριδική αναπαράσταση. Στη συνέχεια, θα πρέπει να οριστούν τα κατάλληλα μέτρα συγγένειας/απόστασης (affinity/distance). Τα μέτρα συγγένειας/απόστασης αξιολογούν πόσο καλά ταιριάζουν μεταξύ τους τα στοιχεία του συστήματος. Αυτά τα μέτρα μπορούν να συνδεθούν με μια επαγωγική μεροληψία (inductive bias), η οποία αναφέρεται στο σύνολο των υποθέσεων που κάνει ένας αλγόριθμος μάθησης για να προβλέψει τις εξόδους για νέα, αθέατα σημεία δεδομένων. Για παράδειγμα, οι συνεχείς μεταβλητές χρησιμοποιούν συνήθως το μέτρο της Ευκλείδειας απόστασης, ενώ οι αναπαραστάσεις bit-string μπορεί να χρησιμοποιούν την απόσταση Hamming. Πρέπει να δοθεί προσοχή ώστε να διασφαλιστεί ότι η επαγωγική μεροληψία είναι κατάλληλη για το συγκεκριμένο πρόβλημα [9].

Το επόμενο βήμα θα πρέπει να είναι η απόφαση για το ποιός αλγόριθμος ΤΑΣ θα είναι καλύτερος για τη δημιουργία ενός συνόλου κατάλληλων οντοτήτων που μπορούν να δώσουν μια καλή λύση στο συγκεκριμένο πρόβλημα. Υπάρχουν διάφοροι τύποι αλγορίθμων εμπνευσμένων από το ανοσοποιητικό σύστημα, οι οποίοι μπορούν να λειτουργούν ανεξάρτητα από την επιλογή της αναπαράστασης και του μέτρου συγγένειας. Αυτοί οι αλγόριθμοι προσθέτουν δυναμική στο σύστημα με βάση τις μετρήσεις που παρέχουν οι συναρτήσεις συγγένειας. Παρακάτω θα ανφερθούμε σε τέσσερις κύριους αλγόριθμους που εμπνέονται από το ανοσοποιητικό σύστημα και κυριαρχούν στη βιβλιογραφία [5].



Σχήμα 3.1: Η προσέγγιση του πολυεπίπεδου πλαισίου για την κατασκευή λύσεων ΤΑΣ [5].

3.3 Εφαρμογές ΤΑΣ στον πραγματικό κόσμο

Οι τεχνικές ανοσολογικού υπολογισμού - Immunological Computation (IC) (ή αλλιώς τεχνητά ανοσοποιητικά συστήματα) έχουν χρησιμοποιηθεί ως μέσο επίλυσης προβλημάτων σε ένα ευρύ φάσμα τομέων, όπως η βελτιστοποίηση (optimization), η ταξινόμηση (classification), η ομαδοποίηση/ συσταδοποίηση (clustering), η ανίχνευση ανωμαλιών (anomaly detection), η μηχανική μάθηση, ο προσαρμοστικός έλεγχος (adaptive control) και οι συνειρμικές μνήμες (associative memories). Έχουν επίσης χρησιμοποιηθεί σε συνδυασμό με άλλες μεθόδους (υβριδικές), όπως οι γενετικοί αλγόριθμοι (genetic algorithms), τα νευρωνικά δίκτυα, η ασαφής λογική (fuzzy logic) και η νοημοσύνη σμήνους (swarm intelligence). Ο κλάδος των ανοσοποιητικών υπολογιστικών συστημάτων περιλαμβάνει πραγματικές εφαρμογές της ασφάλειας υπολογιστών, της ανίχνευσης απάτης, της ρομποτικής, της ανίχνευσης σφαλμάτων, της εξόρυξης δεδομένων, της εξόρυξης κειμένου, της αναγνώρισης εικόνων και προτύπων, της βιοπληροφορικής, των παιχνιδιών, του χρονοπρογραμματισμού κ.α. [5]. Παρακάτω, περιγράφονται εν συντομία ορισμένες εφαρμογές των ΤΑΣ σε κάποιους μεγάλους τομείς του πραγματικού κόσμου :

Ασφάλεια υπολογιστών: Τα ΤΑΣ μπορούν να χρησιμοποιηθούν για την ανίχνευση και την πρόληψη επιθέσεων στον κυβερνοχώρο, όπως ιοί, σκουλήκια (worms) και άλλο κακόβουλο λογισμικό. Οι αλγόριθμοι ΤΑΣ μπορούν να αναλύουν την κυκλοφορία του δικτύου για τον εντοπισμό ανώμαλων μοτίβων και πιθανών απειλών. Αυτά τα συστήματα μπορούν επίσης να προσαρμόζονται και να μαθαίνουν από προηγούμενες επιθέσεις για να βελτιώσουν την ακρίβεια ανίχνευσης και να μειώσουν τα ψευδώς θετικά αποτελέσματα [17].

Ανίχνευση απάτης: Μια άλλη χρήση των ΤΑΣ μπορεί να γίνει στην δημιουργία και ανάπτυξη συστημάτων που εντοπίζουν απάτες. Τα συστήματα ανίχνευσης απάτης που βασίζονται σε ΤΑΣ χρησιμοποιούν διάφορες τεχνικές όπως η ανίχνευση ανωμαλιών, η ομαδοποίηση και η ταξινόμηση για τον εντοπισμό και την πρόληψη δόλιων δραστηριοτήτων. Για παράδειγμα οι τεχνικές ανίχνευσης ανωμαλιών εντοπίζουν δραστηριότητες που μπορεί να αποκλίνουν σημαντικά από μια κανονική συμπεριφορά στα δεδομένα, ενώ οι τεχνικές ομαδοποίησης ομαδοποιούν παρόμοιες δραστηριότητες για τον εντοπισμό προτύπων συμπεριφοράς. Τα συστήματα ανίχνευσης απάτης που βασίζονται σε ΤΑΣ έχουν χρησιμοποιηθεί σε κλάδους, όπως η τραπεζική, η ασφαλιστική και το ηλεκτρονικό εμπόριο [18].

Ρομποτική: Ο έλεγχος και ο συντονισμός συστημάτων πολλαπλών ρομπότ σε δυναμικά περιβάλλοντα είναι ένας τομέας που μπορούν να χρησιμοποιηθούν τεχνικές ΤΑΣ. Οι αλγόριθμοι ΤΑΣ μπορούν να προσομοιώσουν τη συμπεριφορά των ανοσοποιητικών κυττάρων, όπως τα αντισώματα και τα Τ-λεμφοκύτταρα, ώστε να μπορούν τα ρομπότ να ανιχνεύουν και να ανταποκρίνονται στις περιβαλλοντικές αλλαγές και απειλές. Τα συστήματα αυτά μπορούν επίσης να προσαρμόζονται στις μεταβαλλόμενες συνθήκες και να συνεργάζονται με άλλα ρομπότ για την επίτευξη κοινών στόχων. Ρομποτικά συστήματα βασισμένα σε ΤΑΣ έχουν χρησιμοποιηθεί σε διάφορες εφαρμογές που έχουν να κάνουν με αυτόνομη πλοήγηση, σχεδιασμό διαδρομής και αναγνώριση αντικειμένων [5],[19].

Ιατρική διάγνωση: Τα ΤΑΣ μπορούν να χρησιμοποιηθούν για τη διάγνωση ασθενειών και την πρόβλεψη της έκβασης των ασθενών με βάση τα κλινικά τους δεδομένα. Τα μοντέλα ΤΑΣ μπορούν να αναλύουν ιατρικές εικόνες, ηλεκτρονικά αρχεία υγείας και άλλες πληροφορίες ασθενών για τον εντοπισμό μοτίβων και τάσεων. Τα συστήματα αυτά μπορούν επίσης να μαθαίνουν από προηγούμενες περιπτώσεις για να βελτιώσουν την ακρίβειά τους ενω παρέχουν εξατομικευμένες συστάσεις [20].

Βελτιστοποίηση: Τα ΤΑΣ μπορούν να χρησιμοποιηθούν για την επίλυση σύνθετων προβλημάτων βελτιστοποίησης όπως η ομαδοποίηση, ο χρονοπρογραμματισμός (scheduling) και η δρομολόγηση (routing). Οι αλγόριθμοι ΤΑΣ μπορούν να εξερευνήσουν διαφορετικές λύσεις και να επιλέξουν τις καλύτερες με βάση την καταλληλότητα και την ποικιλομορφία τους. Τα συστήματα αυτά μπορούν επίσης να προσαρμόζονται σε μεταβαλλόμενες συνθήκες και περιορισμούς για να βελτιώσουν την αποδοτικότητα και την ευρωστία τους [21].

Συμπερασματικά, τα τεχνητά ανοσοποιητικά συστήματα έχουν ένα ευρύ φάσμα εφαρμογών στον πραγματικό κόσμο. Τα συστήματα αυτά μπορούν να μιμηθούν ορισμένες από τις πολύπλοκες και προσαρμοστικές συμπεριφορές του ανθρώπινου ανοσοποιητικού συστήματος για την επίλυση σύνθετων προβλημάτων και τη βελτίωση της απόδοσης. Ωστόσο η χρήση τέτοιων τεχνικών και αλγορίθμων δεν είναι τόσο διαδεδομένη καθώς βρίσκεται σε πρώιμο στάδιο.

3.4 Αλγόριθμοι και Τεχνικές ΤΑΣ

Ενώ πολλές άλλες περιοχές του ανοσοποιητικού συστήματος των σπονδυλωτών εμπνέουν τους επιστήμονες και μηχανικούς υπολογιστών για την ανάπτυξη νέων αλγορίθμων, τέσσερις σημαντικοί αλγόριθμοι ΤΑΣ αναπτύσσονται συνεχώς και αποκτούν δημοτικότητα:

1) Clonal Selection Algorithms (CLONALG).
2) Negative Selection Algorithms (NSA)
3) Artificial Immune Networks (AINE)
4) The Danger Theory - Dendritic Cell Algorithms (DCA).

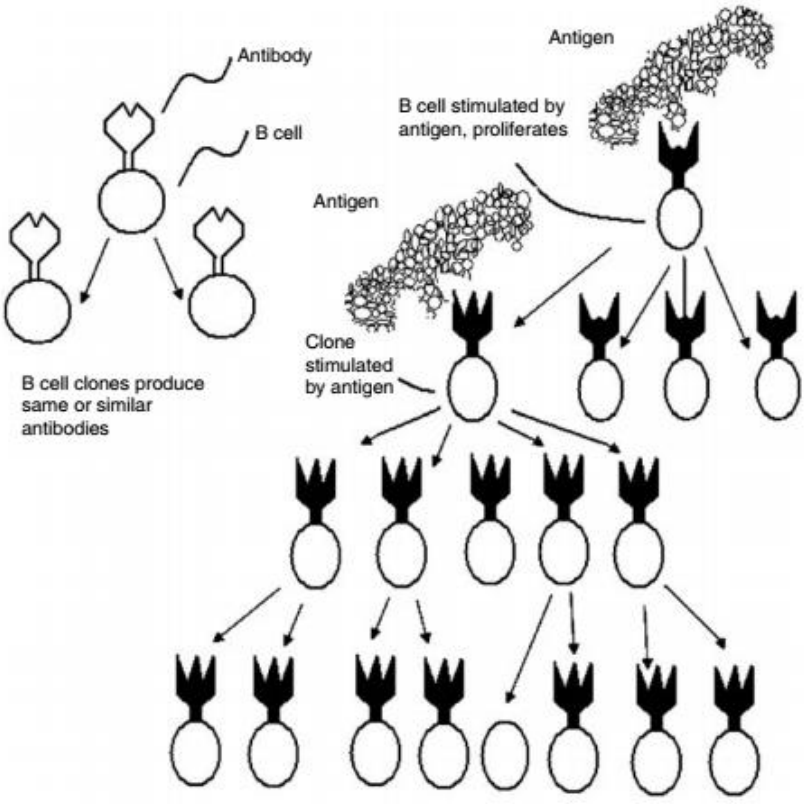
3.4.1 Clonal Selection Theory (CST)

Η θεωρία της κλωνικής επιλογής είναι μια βιολογική θεωρία που διατυπώθηκε από τον Αυστραλιανό ιολόγο Macfarlane Burnet το 1957 και χρησιμοποιήθηκε για να περιγράψει τη λειτουργία της επίκτητης ανοσίας, συγκεκριμένα την περιγραφή της ποικιλομορφίας των αντισωμάτων που χρησιμοποιούνται για την υπεράσπιση του οργανισμού από μια εισβολή [22].

Η θεωρία προτείνει ότι κάθε Β-λεμφοκύτταρο έχει έναν μοναδικό υποδοχέα στην επιφάνειά του, ο οποίος μπορεί να αναγνωρίζει και να συνδέεται με ένα συγκεκριμένο αντιγόνο. Η επανειλημμένη έκθεση σε ένα πρωτεϊνικό αντιγόνο έχει ως αποτέλεσμα την παραγωγή αντισωμάτων με αυξανόμενη συγγένεια (high affinity) για το αντιγόνο. Η διαδικασία αυτή ονομάζεται ωρίμανση συγγένειας (affinity maturation), και οδηγεί στην παραγωγή αντισωμάτων με βελτιωμένη ικανότητα να προσδένονται και να εξουδετερώνουν μικρόβια και τοξίνες [5]. Η ωρίμανση συγγένειας προκαλείται από μια σωματική υπερμετάλλαξη και έναν μηχανισμό επιλογής. Η σωματική υπερμετάλλαξη έχει ως αποτέλεσμα την ποικιλομορφία των αντισωμάτων με την εισαγωγή τυχαίων αλλαγών στα γονίδια που τα κωδικοποιούν. Ο μηχανισμός επιλογής εγγυάται ότι θα επιβιώσουν μόνο οι κλώνοι (αντισώματα) με μεγαλύτερη συγγένεια για το αντιγόνο που συναντάταιν [23].

Στην συνέχεια αυτή η σειρά γεγονότων οδηγεί στον πολλαπλασιασμό και τη διαφοροποίηση του ενεργοποιημένου λεμφοκυττάρου σε έναν κλώνο πανομοιότυπων κυττάρων, τα οποία φέρουν όλα τον ίδιο υποδοχέα αντιγόνου. Η κλωνική επέκταση του ενεργοποιημένου λεμφοκυττάρου εξασφαλίζει ότι δημιουργούνται αρκετά κύτταρα για την καταπολέμηση του παθογόνου. Μόλις εξουδετερωθεί το παθογόνο, η πλειονότητα των κλωνοποιημένων κυττάρων υφίσταται προγραμματισμένο κυτταρικό θάνατο, ενώ ένας μικρός αριθμός παραμένει ως κύτταρα μνήμης μακράς διάρκειας, ικανά να

αναπτύξουν ταχύτερη και ισχυρότερη απόκριση κατά την εκ νέου έκθεση στο ίδιο αντιγόνο. Σήμερα, η θεωρία της κλωνικής επιλογής θεωρείται γεγονός δεδομένης της συντριπτικής ποσότητας εμπειρικών στοιχείων [24].



Εικόνα 3.1: Κλωνική επέκταση (και επιλογή) των Β-λεμφοκυττάρων παρουσία ενός αντιγόνου [5].

Στα ΤΑΣ, το πρόβλημα αναπαρίσταται ως αντιγόνο και η λύση αναπαρίσταται ως ένα σύνολο λεμφοκυττάρων που μπορούν να αναγνωρίσουν το αντιγόνο [9]. Ένας αλγόριθμος ΤΑΣ ξεκινά έχοντας ως σύνολο δεδομένων έναν πληθυσμό λεμφοκυττάρων, καθένα από τα οποία έχει έναν μοναδικό υποδοχέα. Οι υποδοχείς αξιολογούνται με βάση την ικανότητά τους να αναγνωρίζουν το αντιγόνο και τα λεμφοκύτταρα με τους καλύτερους υποδοχείς επιλέγονται για περαιτέρω κλωνοποίηση. Η διαδικασία κλωνοποίησης δημιουργεί έναν νέο πληθυσμό λεμφοκυττάρων, το καθένα με έναν ελαφρώς τροποποιημένο υποδοχέα [23]. Η διαδικασία αυτή μιμείται τη φυσική επιλογή των λεμφοκυττάρων στο ανοσοποιητικό σύστημα. Τα νέα λεμφοκύτταρα αξιολογούνται με βάση την ικανότητά τους να αναγνωρίζουν το αντιγόνο και τα καλύτερα λεμφοκύτταρα επιλέγονται για περαιτέρω κλωνοποίηση. Οι αλγόριθμοι κλωνικής επιλογής αποτυπώνουν τις ιδιότητες της μάθησης, της μνήμης, της προσαρμογής, και της αναγνώρισης προτύπων [10].

Ο CLONALG (CLONal selection ALGorithm) είναι ένας αλγόριθμος κλωνικής επιλογής που εισήχθη από τους De Castro και Van Zuben το 2000 [25]. Στον αλγόριθμο CLONALG, ένας πληθυσμός υποψήφιων λύσεων σε ένα πρόβλημα μηχανικής αντιπροσωπεύεται από ένα σύνολο αντισωμάτων μνήμης. Ο αλγόριθμος CLONALG έχει εφαρμοστεί σε ένα ευρύ φάσμα προβλημάτων βελτιστοποίησης και ταξινόμησης, όπως το πρόβλημα του πλανόδιου πωλητή, η αναγνώριση προτύπων εικόνων και η ομαδοποίηση δεδομένων [26].

Τα βασικά βήματα ενός γενικού αλγόριθμου [5],[9] που βασίζεται στον CLONALG είναι τα εξής:

1. *Αρχικοποίηση*: Δημιουργούμε τυχαία έναν αρχικό πληθυσμό αντισωμάτων.
2. *Υπολογισμός συγγένειας αντισωμάτων (affinity calculation)*: Υπολογίζουμε και αξιολογούμε τη συγγένεια κάθε αντισώματος με το αντιγόνο.
3. *Κλωνοποίηση*: Επιλέγουμε τα αντισώματα του πληθυσμού για κλωνοποίηση, που έχουν την υψηλότερη συγγένειά (highest affinity) με το αντιγόνο. Η διαδικασία κλωνοποίησης αναπαράγει τις καλύτερες λύσεις πολλές φορές για να αυξήσει την αντιπροσώπευσή τους στο νέο πληθυσμό.
4. *Υπερμετάλλαξη*: Εισάγουμε τυχαίες αλλαγές (μεταλλάξεις) στις κλωνοποιημένες λύσεις για τη δημιουργία ποικιλομορφίας στον πληθυσμό. Αυτό το βήμα είναι απαραίτητο για την αποτροπή μιας πρόωρης σύγκλισης σε μια μη βέλτιστη λύση.
5. *Επιλογή αντισωμάτων*: Αξιολογούμε την καταλληλότητα κάθε κλωνοποιημένου αντισώματος στο νέο πληθυσμό και επιλέγουμε τα αντισώματα με την υψηλότερη συγγένεια για τη δημιουργία της επόμενης γενιάς.
6. *Ενημέρωση κυττάρων μνήμης*: Διατήρηση ενός μικρού πληθυσμού των καλύτερων αντισωμάτων από την προηγούμενη γενιά ως κύτταρα μνήμης για να διασφαλιστεί η ποικιλομορφία και να αποφευχθεί η απώλεια χρήσιμων πληροφοριών.
7. *Αντικατάσταση αντισωμάτων*: Αντικαθιστούμε αντισώματα με χαμηλή συγγένεια στον πληθυσμό με νέα τυχαία παραγόμενα αντισώματα για να εξασφαλιστεί η ποικιλομορφία και να αποφευχθεί η στασιμότητα.
8. *Τερματισμός*: Επαναλαμβάνουμε τα βήματα 3-7 για σταθερό αριθμό επαναλήψεων ή μέχρι να ικανοποιηθεί ένα κριτήριο διακοπής.
9. *Έξοδος*: Ένα σύνολο Β-λεμφοκυττάρων μνήμης ικανών να ταξινομούν ή να αναγνωρίζουν άγνωστα στοιχεία δεδομένων.

Η μελέτη των White και Garrett [27] παρέχει μια συνοπτική παρουσίαση των πλεονεκτημάτων και των κύριων τομέων της κλωνικής επιλογής που αξιοποιούνται στους αλγόριθμους τεχνητής κλωνικής επιλογής. Επιγραμματικά τα μεγαλύτερα πλεονεκτήματα είναι τα εξής:

Ποικιλομορφία: Διατήρηση μιας αραιά διαχωρισμένης πληθυσμιακής κατανομής σε ένα ευρύ πεδίο της αντιγονικού χώρου. Η ποικιλομορφία προστατεύει τα ανοσοποιητικά συστήματα από αντιγόνα που δεν έχουν ξανασυναντηθεί ούτε έχουν κάποια συσχέτιση με τα αντιγόνα που έχουν συναντηθεί στο παρελθόν .

Βελτιστοποίηση: Η επιλογή και ωρίμανση αντισωμάτων υψηλής συγγένειας έχει ως αποτέλεσμα ένα πληθυσμό που αποτελείται κυρίως από υψηλής ποιότητας λύσεις. Έτσι, έχουμε βελτίωση της ανοσολογικής απόκρισης σε δευτερογενείς συναντήσεις αποθηκεύοντας μερικά κύτταρα που παράγουν αντισώματα υψηλής συγγένειας από την πρώτη αλληλεπίδραση (κύτταρα μνήμης), απλά για να σχηματίσουν ένα μεγάλο αρχικό βελτιωμένο κλώνο για τις επόμενες συναντήσεις [25]**.**

Εξερεύνηση: Η μετάλλαξη και άλλες λειτουργίες παρέχουν ένα μέσο για την εξερεύνηση του τοπίου συγγένειας μεταξύ αντισωμάτων και αντιγόνων.

Αντικατάσταση: Εξασφάλιση του πολλαπλασιασμού των αντισωμάτων υψηλότερης συγγένειας και της απομάκρυνσης των στοιχείων χαμηλότερης συγγένειας επιτρέποντας μια ευρύτερη αναζήτηση του τοπίου συγγένειας.

Ενισχυτική μάθηση: Επαναλαμβανόμενη έκθεση σε αντιγονικό ερέθισμα και επιλογή, επιβράβευση των αντισωμάτων που ανταποκρίνονται περισσότερο επιτρέποντας στο σύστημα να γίνει πιο ακριβές με την πάροδο του χρόνου.

Φυσικά οι αλγόριθμοι κλωνικής επιλογής έχουν και ορισμένες ανεπάρκειες [23],[28] που συνοψίζονται παρακάτω :

Καθορισμός συναρτήσεων: Η τεχνική απαιτεί από τον χρήστη να επιλέγει συναρτήσεις για τον καθορισμό του αριθμού των κλώνων που θα παραχθούν και του βαθμού μετάλλαξης. Περαιτέρω, αυτό μπορεί να απαιτεί πρόσθετες παραμέτρους για την κλιμάκωση του αριθμού των κλώνων και του ποσού της μετάλλαξης.

Καθορισμός: Η επιλογή του αριθμού των αντισωμάτων υψηλής συγγένειας για κλωνοποίηση και ωρίμανση δεν είναι τετριμμένη και επηρεάζει σημαντικά την απόδοση του αλγορίθμου. Απαιτείται ακριβή εκτίμηση του μεγέθους του πληθυσμού. Ο μικρότερος πληθυσμός μπορεί να κατευθύνει τον αλγόριθμο προς μια γρήγορη σύγκλιση (rapid converge), ενώ ο μεγαλύτερος πληθυσμός απαιτεί εκτεταμένους υπολογιστικούς πόρους.

Επεκτασιμότητα (Scalability) και περιορισμένη προσαρμοστικότητα: Ο αριθμός των κλώνων που δημιουργούνται σε κάθε γενιά, και συνεπώς ο αριθμός των αξιολογήσεων συναρτήσεων είναι συνήθως μεγαλύτερος από τον αρχικό πληθυσμό αντισωμάτων. Κάτι τέτοιο αναμένεται να γίνει μη διαχειρίσιμο για μεγαλύτερα μεγέθη πληθυσμού.

Γενικά, οι αλγόριθμοι κλωνικής επιλογής είναι αργοί για προβλήματα βελτιστοποίησης μεγάλης κλίμακας, ειδικά όταν πρόκειται για μεγάλο αριθμό υποψήφιων λύσεων, ενώ η ικανότητά τους να προσαρμόζονται στις αλλαγές του τοπίου βελτιστοποίησης μπορεί να είναι περιορισμένη, καθώς μπορεί να δυσκολευτούν να χειριστούν δυναμικά προβλήματα βελτιστοποίησης όπου η βέλτιστη λύση αλλάζει με την πάροδο του χρόνου. Διάφορες παραλλαγές του αλγορίθμου κλωνικής επιλογής έχουν σχεδιαστεί για να επεκτείνουν ή να βελτιώσουν τον αρχικό αλγόριθμο με ποικίλους τρόπους [23]:

Elitist Immune Programming (EIP): Αυτή η παραλλαγή εισάγει την έννοια του “ελιτισμού”, διασφαλίζοντας ότι η καλύτερη λύση που έχει βρεθεί μέχρι στιγμής διατηρείται σε κάθε γενιά. Αυτό καθιστά τον αλγόριθμο πιο ανθεκτικό, διατηρώντας λύσεις υψηλής ποιότητας. Ένα από τα βασικά χαρακτηριστικά του ελιτιστικού ανοσοποιητικού προγραμματισμού είναι η διατήρηση της καλύτερης λύσης που έχει βρεθεί μέχρι στιγμής σε κάθε γενιά. Εφόσον η καλύτερη λύση διατηρείται, χρησιμεύει ως σημείο αναφοράς για τον υπόλοιπο πληθυσμό, καθοδηγώντας τον αλγόριθμο προς ολοένα και καλύτερες λύσεις. Αυτό είναι που την καθιστά "ελιτίστικη". Διατηρώντας την καλύτερη λύση, ο αλγόριθμος διασφαλίζει ότι η ποιότητα των λύσεων δεν υποβαθμίζεται με την πάροδο του χρόνου. Η έννοια του “ελιτισμού” καθιστά τον ελιτιστικό ανοσοποιητικό προγραμματισμό ιδιαίτερα χρήσιμο για προβλήματα στα οποία είναι ζωτικής σημασίας να μην χάνονται οι καλύτερες λύσεις, όπως σε πολύπλοκα προβλήματα βελτιστοποίησης με πολλαπλά τοπικά βέλτιστα.

Συμβίωση στον CLONALG: Αυτή η παραλλαγή χρησιμοποιεί μερικώς καθορισμένα αντισώματα που ενδέχεται να μην έχουν όλα τα απαιτούμενα δεδομένα για να αξιολογηθούν ως λύση. Ο αλγόριθμος κατασκευάζει ένα συγκρότημα με όλες τις απαιτούμενες ιδιότητες επιλέγοντας επανειλημμένα αντισώματα. Εάν ο αλγόριθμος αποτύχει να ολοκληρώσει μια τέτοια συναρμολόγηση, δημιουργεί νέα αντισώματα με τυχαίες τιμές για τις θέσεις που λείπουν. Αυτή η προσέγγιση επιτρέπει στον αλγόριθμο

να επιλύει προβλήματα σπάζοντάς τα σε μικρότερα υποπροβλήματα, βρίσκοντας ενδεχομένως λύσεις γρηγορότερα από τον αρχικό CLONALG.

Software Mutation Testing: Αυτός ο αλγόριθμος αναζητά επαναληπτικά αντισώματα που μπορούν να "σκοτώσουν" μεταλλαγμένα προγράμματα που δεν έχουν ήδη σκοτωθεί από τα υπάρχοντα τεστ μνήμης. Το "σκορ μετάλλαξης" χρησιμοποιείται για την αξιολόγηση της συγγένειας ενός αντισώματος. Αυτή η παραλλαγή είναι αποτελεσματική σε σενάρια δοκιμών λογισμικού όπου πρέπει να ελεγχθούν πολλαπλές συνθήκες ή μεταλλάξεις.

Protein Structure Prediction: Αυτή παραλλαγή αντιμετωπίζει το πρόβλημα πρόβλεψης της δομής πρωτεϊνών σε μοντέλα πλέγματος. Σε αυτόν τον αλγόριθμο, το αντιγόνο και τα Β-λεμφοκύτταρα αντιπροσωπεύουν μια αλληλουχία υδρόφοβων-πρότυπων της πρωτεΐνης. Αυτό είναι ιδιαίτερα χρήσιμο στη βιοπληροφορική για την πρόβλεψη της δομής των πρωτεϊνών.

Αυτές οι παραλλαγές του CLONALG αποδεικνύουν την ευελιξία και την προσαρμοστικότητα του αλγορίθμου. Με την εισαγωγή νέων εννοιών όπως ο ελιτισμός, η συμβίωση και οι εξειδικευμένες εφαρμογές, αυτές οι παραλλαγές επεκτείνουν τη χρησιμότητα του αρχικού αλγορίθμου σε νέους τομείς και προσφέρουν βελτιωμένη απόδοση σε συγκεκριμένες εργασίες.

Οι αλγόριθμοι κλωνικής επιλογής χρησιμοποιούνται συνήθως σε διάφορους τομείς εφαρμογών, όπως:

- Αναγνώριση προτύπων [27],[29],[30]
- Βελτιστοποίηση/πολυτροπική βελτιστοποίηση (Optimization/multimodal optimization) [31],[32]
- Αναγνώριση δυαδικών χαρακτήρων [28],[29]
- Ασφάλεια υπολογιστών [32]
- Επίλυση σύνθετων εργασιών μηχανικής μάθησης [32],[33]
- Μια ευέλικτη εναλλακτική λύση για τον γενετικό αλγόριθμο και τον εξελικτικό αλγόριθμο (evolutionary algorithm) [32]
- Μια ισχυρή μέθοδος για την αντιμετώπιση σύνθετων προβλημάτων συνδυαστικής βελτιστοποίησης, καθώς έχει τη δυνατότητα να διευρύνει το χώρο λύσεων [32]

3.4.2 Negative Selection Algorithm (NSA)

Οι αλγόριθμοι αρνητικής επιλογής λειτουργούν με την έννοια της διάκρισης "εαυτού/ξένου" (self/non-self discrimination). Η διάκριση εαυτού/ξένου είναι μια θεμελιώδης έννοια της ανοσολογίας και η βάση για τη λειτουργία του ανοσοποιητικού συστήματος. Αναφέρεται στην ικανότητα του ανοσοποιητικού συστήματος να διακρίνει μεταξύ του "εαυτού" του, δηλαδή των κυττάρων και των ιστών του ίδιου του σώματος, και των "ξένων", δηλαδή των ξένων ουσιών, όπως οι παθογόνοι μικροοργανισμοί ή τα καρκινικά κύτταρα. Αν δεν υπήρχε διάκριση μεταξύ εαυτού/ξένου, το ανοσοποιητικό σύστημα θα επιτίθετο στα κύτταρα και τους ιστούς του ίδιου του σώματος, οδηγώντας σε αυτοάνοσες ασθένειες [34].

Ο NSA ήταν μια λαμπρή ιδέα που προτάθηκε από την Stephanie Forrest (1994). Με την εφαρμογή τεχνικών εμπνευσμένων από το ανοσοποιητικό σύστημα για την ανίχνευση προτύπων συνέβαλε στην αντιμετώπιση των προβλημάτων στην ανίχνευση ιών σε συστήματα υπολογιστών και σε εισβολές σε δίκτυα [35]. Η ιδέα πίσω από τον αλγόριθμο είναι να δημιουργηθεί ένα σύνολο από (δυαδικούς) ανιχνευτές (detectors), δημιουργώντας πρώτα τυχαία υποψήφιους και απορρίπτοντας στη συνέχεια

εκείνους που αναγνωρίζουν τα δεδομένα εκπαίδευσης. Αυτοί οι ανιχνευτές μπορούν αργότερα να χρησιμοποιηθούν για την ανίχνευση ανωμαλιών. Έτσι, ο NSA αποτελείται από τρεις φάσεις: ορισμός του "εαυτού", δημιουργία ανιχνευτών και παρακολούθηση της εμφάνισης ανωμαλιών. Οι πρωταρχικές εφαρμογές του NSA ήταν στον τομέα της ανίχνευσης αλλαγών (ή ανωμαλιών), όπου οι ανιχνευτές δημιουργούνται στον συμπληρωματικό χώρο που μπορεί να ανιχνεύσει αλλαγές στα πρότυπα δεδομένων [36].

Ως εκ τούτου, ο NSA αναφέρεται επίσης ως αρνητική ανίχνευση με την ικανότητα να ανιχνεύει ξένα κύτταρα (αντιγόνα) χωρίς να διακόπτει τα αυτοκύτταρα. Η θεωρία της αρνητικής επιλογής έχει προταθεί από τους Timmis και Bentley (2002) υποδεικνύοντας την προστασία του οργανισμού από τα αυτοαντιδραστικά λεμφοκύτταρα. Στην ουσία, τα κοινά στοιχεία των αλγόριθμων αρνητικής επιλογής είναι η αναπαράσταση δεδομένων, η εκτίμηση της κάλυψης, τα μέτρα συγγένειας και οι κανόνες αντιστοίχισης που ταξινομούνται επίσης με διαφορετικά κριτήρια [37].

Όπως προτάθηκε από τον Percus (1999), ο NSA αντιγράφει τον τρόπο με τον οποίο γίνεται η θεωρητική ανάλυση των πιθανοτήτων αντιστοίχισης και δέσμευσης μέσα στα ανοσοποιητικά συστήματα. Για το σύστημα αρνητικής επιλογής, η πρώτη φάση είναι η διαδικασία ωρίμανσης που θα τεθεί σε χειμερία νάρκη για ένα χρονικό διάστημα. Στη συνέχεια, οι ανιχνευτές θα ενεργοποιηθούν όταν πραγματοποιηθεί επιτυχώς ένας αριθμός αντιστοιχίσεων με εισερχόμενα αντιγόνα [38]. Αργότερα, αυτοί οι ενεργοποιημένοι ανιχνευτές ή υποδοχείς θα εφαρμοστούν στη διαδικασία ψευδο-τυχαίας γενετικής αναδιάταξης κατά τη δημιουργία των Τ-λεμφοκυττάρων. Αυτή η επιλογή τυχαίας προσέγγισης οφείλεται στην απλότητα και την ομοιότητά της με το ανοσοποιητικό σύστημα [35].

Στη συνέχεια, η διαδικασία που λέγεται αρνητική επιλογή συνεχίζεται στον θύμο αδένα. Ο θύμος αδένας αποτελείται από δύο πανομοιότυπους λοβούς, και βρίσκεται ανατομικά στο πρόσθιο ανώτερο μεσοθωράκιο τμήμα, μπροστά από την καρδιά και πίσω από το στέρνο [5]. Εκεί, τα Τ-λεμφοκύτταρα που αντιδρούν προς τις πρωτεΐνες "εαυτού" θα εξαλειφθούν και τα υπόλοιπα θα επιτραπεί να εγκαταλείψουν τον θύμο αδένα (θα διατηρηθούν ως ανιχνευτές). Εάν ένα κύτταρο δεν ταιριάξει σε ορισμένο χρονικό διάστημα, θα γεράσει και τελικά θα πεθάνει [38]. Αυτό το σύνολο ανιχνευτών εφαρμόζεται στη συνέχεια για τον εντοπισμό και την ανίχνευση των εισερχόμενων δεδομένων (είτε "εαυτού" είτε "ξένων") [35].

Ανακεφαλαιώνοντας, ο NSA σχεδιάστηκε έχοντας ως μοντέλο την δημιουργία των Τ-λεμφοκυττάρων. Εάν ένα Τ-λεμφοκύτταρο αναγνωρίσει κάποιο κύτταρο εαυτού, το εξαλείφει πριν ωριμάσει και γίνει αντίσωμα ενώ τα υπόλοιπα κύτταρα αναπτύσσονται στο ανοσοποιητικό σύστημα για να αναγνωρίζουν και να επιτίθενται σε παθογόνα [39].

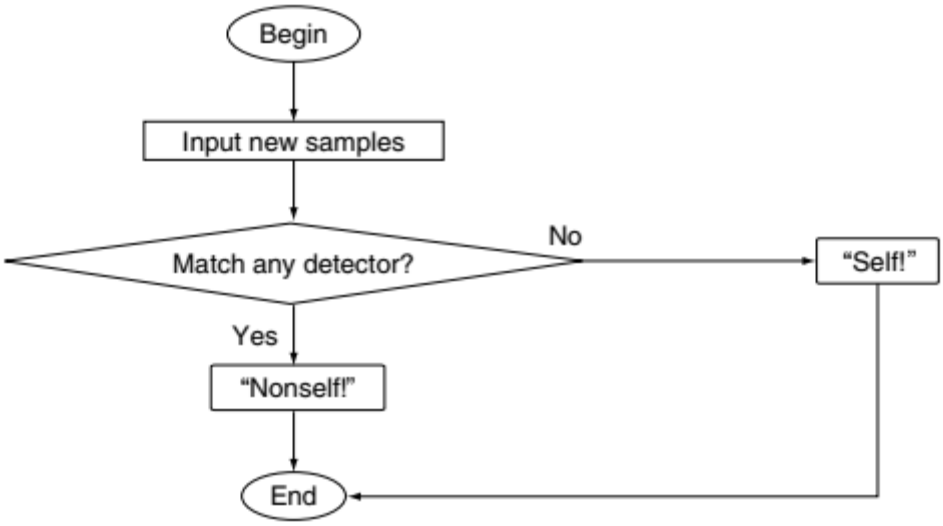
Το σύνολο ανιχνευτών που δημιουργείται έχει σχεδιαστεί για να αναγνωρίζει μοτίβα σε δεδομένα "εαυτού". Αυτοί οι ανιχνευτές παράγονται συνήθως με την διαδικασία της αρνητικής επιλογής, όπου ο αλγόριθμος παράγει τυχαίους ανιχνευτές και επιλέγει μόνο εκείνους που δεν ταιριάζουν με κανένα από τα δεδομένα "εαυτού". Αυτό έχει ως αποτέλεσμα να έχουμε ένα σύνολο ανιχνευτών που είναι πολύ συγκεκριμένοι για τα δεδομένα "εαυτού" και είναι ικανοί να ανιχνεύουν οποιαδήποτε σημεία ξένων δεδομένων που διαφέρουν σημαντικά από τα δεδομένα "εαυτού" [5],[40].

Ένας γενικός αλγόριθμος αρνητικής επιλογής [5],[9] αποτελείται συνήθως από τα ακόλουθα βήματα:

1. *Αρχικοποίηση:* Δημιουργούμε ένα σύνολο δεδομένων "ξένου" (non-self) που αντιπροσωπεύει τα χαρακτηριστικά του περιβάλλοντος από τα οποία υποτίθεται ότι το σύστημα πρέπει να προστατεύει και δημιουργούμε ένα σύνολο δεδομένων "εαυτού" (self) που αντιπροσωπεύει τα χαρακτηριστικά του συστήματος τα οποία δεν πρέπει να ανιχνεύονται ως "ξένα".

2. *Δημιουργία ανιχνευτών*: Δημιουργούμε ένα σύνολο ανιχνευτών που αντιπροσωπεύουν τα δεδομένα “εαυτού” (self data) ή την κανονική συμπεριφορά του συστήματος. Αυτό μπορεί να γίνει τυχαία ή χρησιμοποιώντας κάποιους προκαθορισμένους κανόνες.
3. *Εκπαίδευση*: Εκπαιδεύουμε τους ανιχνευτές πάνω στα δεδομένα “ξένου” και προσδιορίζουμε το επίπεδο συγγένειας ή ομοιότητάς τους με τα δεδομένα “εαυτού”. Χρησιμοποιούμε μια τιμή κατωφλίου (threshold value) για να καθορίσουμε ποια μοτίβα θεωρούνται “ξένα”.
4. *Ανίχνευση*: Εφαρμόζουμε τους ανιχνευτές στα δεδομένα εισόδου και εντοπίζουμε αυτά που πέφτουν κάτω από την τιμή κατωφλίου. Αυτά θεωρούνται ως ανωμαλίες ή δεδομένα “ξένου”.
5. *Επικαιροποίηση*: Ενσωματώνουμε τα ανιχνευθέντα “ξένα” μοτίβα στο σύνολο των ανιχνευτών για να βελτιώσουμε την ικανότητα του συστήματος να ανιχνεύει μελλοντικά “ξένα” μοτίβα.
6. *Τερματισμός*: Επαναλαμβάνουμε τα βήματα 2-5 έως ότου το σύστημα φτάσει σε ένα ικανοποιητικό επίπεδο ακρίβειας στον εντοπισμό μη αυτοσχέδιων μοτίβων.
7. *Έξοδος*: Η τελική έξοδος του αλγόριθμου είναι το σύνολο των ανιχνευτών που έχουν ταυτοποιηθεί ως πρότυπα “ξένου”

Να επισημάνουμε πως οι λεπτομέρειες κάθε βήματος, όπως η επιλογή των μέτρων συγγένειας, οι τιμές κατωφλίου και οι κανόνες επικαιροποίησης, μπορεί να διαφέρουν ανάλογα με τη συγκεκριμένη εφαρμογή και τον τομέα.



Εικόνα 3.2: Βήμα ανίχνευσης NSA [5]

Η δημιουργία των ανιχνευτών είναι το κρισιμότερο κομμάτι σε έναν αλγόριθμο αρνητικής επιλογής. Υπάρουν διάφοροι μέθοδοι παραγωγής ανιχνευτών, κάποιοι από τους κυριότερους συνοψίζονται εδώ πέρα [5]:

Εξαντλητική προσέγγιση: Αυτή η προσέγγιση παράγει ανιχνευτές με τυχαίο τρόπο και τους ελέγχει με βάση το σύνολο “εαυτού”. Εάν ένας ανιχνευτής ταιριάζει με οποιοδήποτε στοιχείο του αυτοσυνόλου, εξαλείφεται. Είναι μια απλή και ξεκάθαρη μέθοδος που μπορεί όμως να είναι υπολογιστικά δαπανηρή και όχι αποδοτική για μεγάλα σύνολα δεδομένων καθώς μπορεί να οδηγήσει στην δημιουργία

μεγάλου αριθμό ανιχνευτών. Η χρήση αυτή της προσέγγισης συνιστάται κυρίως για προβλήματα μικρής κλίμακας.

Προσέγγιση δυναμικού προγραμματισμού: Η δημιουργία των ανιχνευτών γίνεται μέσω ενός αλγόριθμου γραμμικού χρόνου. Αυτή η προσέγγιση είναι πιο αποδοτική από άποψη χρονικής πολυπλοκότητας καθιστώντας την πιο αποτελεσματική από την εξαντλητική μέθοδο και κατάλληλη για μεγαλύτερα σύνολα δεδομένων. Χρησιμοποιεί δυναμικό προγραμματισμό για την εύρεση ανιχνευτών που δεν ταιριάζουν με το σύνολο "εαυτού".

Απληστος αλγόριθμος (greedy algorithm) για τη δημιουργία ανιχνευτών: Ο "άπληστος αλγόριθμος" είναι μια άλλη αποτελεσματική μέθοδος για τη δημιουργία ανιχνευτών. Λειτουργεί επίσης σε γραμμικό χρόνο και είναι ιδιαίτερα χρήσιμος όταν το σύνολο δεδομένων είναι μεγάλο. Στοχεύει στην όσο το δυνατόν αποτελεσματικότερη κάλυψη του μη χώρου που βρίσκονται τα σύνολα "ξένου".

NSMutation Algorithm: Ο αλγόριθμος NSMutation είναι μια τροποποιημένη έκδοση του εξαντλητικού αλγορίθμου που εισάγει έναν μηχανισμό σωματικής υπερμετάλλαξης για τη βελτίωση της απόδοσης. Αυτός ο αλγόριθμος είναι μοναδικός στο ότι ελέγχει και επιλύει το πρόβλημα των περιττών ανιχνευτών, μειώνοντας έτσι τον συνολικό αριθμό των ανιχνευτών. Είναι ρυθμιζόμενος ώστε να ισορροπεί μεταξύ υψηλής κάλυψης και αποδοτικής δημιουργίας. Αντί να εξαλειφθεί ένας υποψήφιος ανιχνευτής που ταιριάζει με τα δεδομένα "εαυτού", πραγματοποιείται καθοδηγούμενη μετάλλαξη για να γίνεί έγκυρος ανιχνευτής.

Δυαδικό πρότυπο (Binary Template): Σε αυτή την προσέγγιση χρησιμοποιείται ένας ντετερμινιστικός αλγόριθμος για να δημιουργήσει ανιχνευτές πιο αποτελεσματικά όσον αφορά τον ελάχιστο αριθμό ανιχνευτών. Χρησιμοποιεί μια έννοια που ονομάζεται "πρότυπο", η οποία είναι μια συμβολοσειρά. Είναι ιδανική για προβλήματα που χρειαζόμαστε έναν σχετικά μικρό αριθμό ανιχνευτών.

DynamiCS: Η προσέγγιση DynamiCS αντιμετωπίζει προβλήματα ανίχνευσης του συνόλου "ξένου" σε ένα συνεχώς μεταβαλλόμενο περιβάλλον. Βασίζεται στην ιδέα του Hofmeyr για τη δυναμική τριών διαφορετικών πληθυσμών: ανώριμοι, ώριμοι και "ανιχνευτές μνήμης". Το μεγάλο πλεονέκτημα αυτής της προσέγγισης είναι η προσαρμοστικότητα σε μεταβαλλόμενα περιβάλλοντα. Το μειονέκτημα είναι η εξάρτηση από τον ανθρώπινο παράγοντα για να γίνει ένας ανιχνευτής ανιχνευτή μνήμης. Με απλούστερους όρους, ο ίδιος ο αλγόριθμος δεν αυτοματοποιεί πλήρως τη διαδικασία που καθιστά έναν ανιχνευτή ανιχνευτή μνήμης. Ένας άνθρωπος πρέπει να επιβεβαιώσει ή να επικυρώσει αυτή τη μετάβαση.

Κανόνες ανίχνευσης βάσει σχημάτων (Schemata-Based Detection Rules): Αυτή η προσέγγιση επιτρέπει μια πιο διαφοροποιημένη διαδικασία αντιστοίχισης με τη χρήση σχημάτων αντί για ακατέργαστα δεδομένα. Μετατρέπει το χώρο δεδομένων σε χώρο σχημάτων, συμπιέζοντας το χώρο δεδομένων. Οι ανιχνευτές κατασκευάζονται στη συνέχεια στον συμπληρωματικό χώρο των σχημάτων χρησιμοποιώντας την παραδοσιακή στρατηγική "δημιουργίας και δοκιμής". Ο υποψήφιος ανιχνευτής απορρίπτεται εάν περιέχει κοινά σχήματα. Ουσιαστικά, τα σχήματα χρησιμεύουν ως μια πιο συμπαγής αναπαράσταση των δεδομένων και οι ανιχνευτές δημιουργούνται με τρόπο που να μην ταιριάζουν με αυτά τα σχήματα.

Οι αλγόριθμοι αρνητικής επιλογής έχουν σημαντικά πλεονεκτήματα έναντι άλλων προσεγγίσεων σε προβλήματα ανίχνευσης ανωμαλιών και ταξινόμησης. Ο NSA μαθαίνει, ανακαλύπτει και ανιχνεύει αυτόματα οποιοδήποτε μη φυσιολογικό μοτίβο ή εμφάνιση (ξένα κύτταρα) [35],[38]. Επιπλέον διατηρεί μόνο τους ενεργούς ανιχνευτές με αποτέλεσμα να μειώνει τη χωρητικότητα της αποθήκευσης ανιχνευτών εντός ενός αποδεκτού εύρους [38]. Ένα άλλο πλεονέκτημα των αλγορίθμων αρνητικής

επιλογής είναι το χαμηλό υπολογιστικό τους κόστος. Αυτοί οι αλγόριθμοι έχουν σχεδιαστεί για να είναι υπολογιστικά αποδοτικοί, γεγονός που τους καθιστά κατάλληλους για εφαρμογές πραγματικού χρόνου όπου τα αποτελέσματα χρειάζονται γρήγορα. Έχουν προταθεί διάφορες παραλλαγές του NSA για τη δημιουργία ανιχνευτών. Αυτή η ευελιξία επιτρέπει την προσαρμογή του NSA για διάφορες εφαρμογές. Επίσης, οι αλγόριθμοι αρνητικής επιλογής μπορούν να προσαρμοστούν σε διαφορετικούς τύπους δεδομένων, συμπεριλαμβανομένων αριθμητικών, κατηγορικών και δεδομένων ακολουθίας, γεγονός που τους καθιστά ευέλικτους και εφαρμόσιμους σε ένα ευρύ φάσμα εργασιών [41].

Παρά τα πλεονεκτήματά τους, οι αλγόριθμοι αρνητικής επιλογής έχουν επίσης περιορισμούς [37] που πρέπει να λαμβάνονται υπόψη όταν χρησιμοποιούνται για εργασίες ανίχνευσης και ταξινόμησης ανωμαλιών. Αρχικά είναι ακατάλληλοι για γενική μέθοδο ταξινόμησης (με βάση μία κλάση). Η προσαρμογή των δεδομένων στον αλγόριθμο θα μειώσει άμεσα την αποτελεσματικότητα του αλγορίθμου και θα αγνοήσει κάθε σημαντική πληροφορία. Επιπλέον, οι συμβατικοί τρόποι παραγωγής ανιχνευτών οδηγούν πάντα σε εξαντλητική και χρονοβόρα διαδικασία. Τέλος, όσον αφορά την επεκτασιμότητα, πολλοί ερευνητές διαπίστωσαν ότι ο NSA παρήγαγε κακές επιδόσεις λόγω προβλημάτων κλιμάκωσης σε προβλήματα του πραγματικού κόσμου. Ταυτόχρονα, το κόστος για την εκπαίδευση των ανιχνευτών σχετίζεται εκθετικά με το μέγεθος του συνόλου “εαυτού” και έτσι το προφίλ του συστήματος αντιπροσωπεύεται μόνο από μέρος των στοιχείων του αυτοσυνόλου [42].

Για να αντιμετωπιστούν κάποια από τα μειονεκτήματα των κλασσικών αλγόριθμων αρνητικής επιλογής έχουν προταθεί διάφορες παραλλαγές που επικεντρώνονται κυρίως στην ανάπτυξη εναλλακτικών σχημάτων δημιουργίας ανιχνευτών για τη βελτίωση της απόδοσης του αλγορίθμου. Ορισμένες παραλλαγές του NSA αναφέρονται εδώ [23] :

NSA με βάση γενετικό αλγόριθμο (Genetic Algorithm-Based NSA): Οι Gao, Ovaska, Wang [43] πρότειναν έναν αλγόριθμο αρνητικής επιλογής που χρησιμοποιεί γενετικό αλγόριθμο που επικεντρώνεται στη βελτιστοποίηση των ανιχνευτών για μέγιστη κάλυψη του χώρου “ξένου” και ελάχιστη επικάλυψη μεταξύ τους. Η καταλληλότητα κάθε υποψήφιου ανιχνευτή υπολογίζεται με βάση την ακτίνα του, η οποία υπολογίζεται με βάση την απόστασή του από το πλησιέστερο δείγμα “εαυτού”. Όσοι έχουν μεγαλύτερες έγκυρες ακτίνες έχουν υψηλότερη καταλληλότητα για εξέλιξη στον γενετικό αλγόριθμο. Η εργασία καταλήγει στο συμπέρασμα ότι το σύστημα βελτιστοποίησης των ανιχνευτών NSA με βάση τον γενετικό αλγόριθμο είναι ανώτερο από τις συμβατικές μεθόδους ανίχνευσης ανωμαλιών.

Κλωνική βελτιστοποίηση NSA (Clonal Optimization NSA): Παρόμοια με τον NSA που βασίζεται σε γενετικό αλγόριθμο, η έμφαση δίνεται στη βελτιστοποίηση των ανιχνευτών. Ωστόσο, αυτή η παραλλαγή χρησιμοποιεί μεθόδους κλωνικής βελτιστοποίησης. Αυτή η παραλλαγή δοκιμάστηκε σε προσομοιωμένα προβλήματα ανίχνευσης σφαλμάτων, υποδεικνύοντας τη χρησιμότητά της στην ανίχνευση ανωμαλιών.

Αλγόριθμοι εξελικτικής αρνητικής επιλογής (Evolutionary Negative Selection Algorithms): Σε αυτή την προσέγγιση που ονομάζεται ENSA, υπάρχουν δύο τύποι. Ο απλός ENSA και ο βασικός ENSA. Στον απλό ENSA, εάν ο ανιχνευτής ταιριάζει με τα δεδομένα, εντοπίζεται μια μη φυσιολογική αλλαγή. Διαφορετικά, το αρχικό σύνολο ανιχνευτών εξελίσσεται στην επόμενη γενιά μέσω μετάλλαξης, επιλογής και αρνητικής επιλογής. Ο βασικός ENSA είναι παρόμοιος, αλλά περιλαμβάνει ένα πρόσθετο τυχαία παραγόμενο σύνολο ανιχνευτών στην επόμενη γενιά. Αυτή η αλλαγή επιτρέπει στον βασικό ENSA να κάνει αναζητήσεις στον παγκόσμιο χώρο και να αποτρέπει τη σύγκλιση σε τοπικά βέλτιστα.

Οι αλγόριθμοι αρνητικής επιλογής χρησιμοποιούνται συνήθως σε διάφορους τομείς εφαρμογών, όπως:

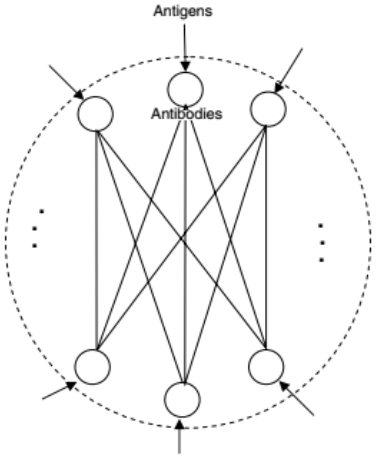
- Προστασία από ιούς [44],[29],[32]
- Εργαλεία παρακολούθησης [44],[29],[32]
- Ασφάλεια υπολογιστών [32]
- Ανίχνευση αλλαγών/ανωμαλιών [44],[29],[32]
- Συστήματα ανίχνευσης ταχείας αντίδρασης [44],[29],[32]

3.4.3 Immune Network Theory

Η θεωρία των ανοσολογικών δικτύων προτάθηκε για πρώτη φορά από τον βραβευμένο με Νόμπελ Niels Jerne ως ένας τρόπος εξήγησης των πολύπλοκων αλληλεπιδράσεων μεταξύ των διαφόρων συστατικών του ανοσοποιητικού συστήματος. Η θεωρία του Jerne βασίστηκε στην ιδέα ότι το ανοσοποιητικό σύστημα δεν είναι απλώς μια συλλογή ανεξάρτητων κυττάρων και μορίων, αλλά μάλλον ένα εξαιρετικά διασυνδεδεμένο και δυναμικό δίκτυο που μπορεί να προσαρμόζεται στις μεταβαλλόμενες συνθήκες. Αυτό το δίκτυο έχει την δυνατότητα να αυτοοργανώνεται και να δρα ακόμα και χωρίς την παρουσία αντιγόνων [45].

Η μέθοδος αυτή βασίζεται στη θεωρία του Jerne (1974) για τα ιδιοτυπικά δίκτυα (idiotypic networks) [45], η οποία υποδηλώνει ότι το ανοσοποιητικό σύστημα διατηρεί ένα δίκτυο διασυνδεδεμένων Β-λεμφοκυττάρων. Στα μοντέλα τεχνητού ανοσολογικού δικτύου - Artificial Immune Networks (AINE), ένας πληθυσμός Β-λεμφοκυττάρων αποτελείται από δύο υποπληθυσμούς: τον αρχικό πληθυσμό και τον κλωνοποιημένο πληθυσμό. Ο αρχικός πληθυσμός δημιουργείται από ένα υποσύνολο ακατέργαστων δεδομένων εκπαίδευσης για τη δημιουργία ενός δικτύου Β-λεμφοκυττάρων. Τα υπόλοιπα χρησιμοποιούνται ως στοιχεία εκπαίδευσης αντιγόνων. Στη συνέχεια, τα αντιγόνα επιλέγονται τυχαία από το σύνολο εκπαίδευσης και παρουσιάζονται στις περιοχές του δικτύου Β-λεμφοκυττάρων. Εάν η σύνδεση είναι επιτυχής, τότε το Β-λεμφοκύτταρο κλωνοποιείται και μεταλλάσσεται [46].

Από τη μετάλλαξη προκύπτει ένα ποικίλο σύνολο αντισωμάτων που μπορούν να χρησιμοποιηθούν στη διαδικασία ταξινόμησης. Μόλις δημιουργηθεί ένα νέο Β-λεμφοκύτταρο, γίνεται προσπάθεια ενσωμάτωσής του στο δίκτυο στα πλησιέστερα Β-λεμφοκύτταρα. Εάν το νέο Β-λεμφοκύτταρο δεν μπορεί να ενσωματωθεί, αφαιρείται από τον πληθυσμό. Εάν καμία σύνδεση δεν είναι επιτυχής, τότε δημιουργείται ένα Β-λεμφοκύτταρο που χρησιμοποιεί το αντιγόνο ως πρότυπο και στη συνέχεια ενσωματώνεται στο δίκτυο [36].



Εικόνα 3.3: Απεικόνιση ενός ανοσολογικού δικτύου. Οι κόμβοι, οι ακμές και τα βέλη αντιπροσωπεύουν αντισώματα, την αλληλεπίδραση μεταξύ τους και τη διέγερση του AINE από ξένα αντιγόνα, αντίστοιχα [5]

Από αυτή την πρωτοποριακή ανάπτυξη, εξελίσσονται συνεχώς νέα συστήματα βασισμένα σε δίκτυα, όπως το aiNet που είναι ένα παράδειγμα τεχνητού ανοσολογικού δικτύου που έχει σχεδιαστεί ειδικά για μη εποπτευόμενη ομαδοποίηση. Αν και γενικά θεωρείται ότι ανήκει στην οικογένεια των τεχνητών ανοσολογικών δικτύων, το aiNet εμπνέεται από τη θεωρία της κλωνικής επιλογής [23].

Ο αλγόριθμος aiNet είναι μια τροποποιημένη έκδοση του αλγορίθμου κλωνικής επιλογής (CLONALG) που ενσωματώνει έναν μηχανισμό καταστολής μεταξύ των Β-λεμφοκυττάρων. Σε αυτόν τον αλγόριθμο, τα στοιχεία δεδομένων αναπαρίστανται ως αντιγόνα, τα οποία αναγνωρίζονται από ανιχνευτές Β-λεμφοκυττάρων. Ο αλγόριθμος χρησιμοποιεί μια διαδικασία ωρίμανσης συγγένειας για τη δημιουργία Β-λεμφοκυττάρων με διαφορετικές ειδικότητες, παρόμοια με τον αλγόριθμο κλωνικής επιλογής. Κατά τη διάρκεια της διαδικασίας ωρίμανσης, τα Β-λεμφοκύτταρα υφίστανται μεταλλάξεις και διασταυρώσεις για την παραγωγή απογόνων κυττάρων με δυνητικά βελτιωμένες ικανότητες αναγνώρισης αντιγόνων. Μετά την ωρίμανση συγγένειας, ο αλγόριθμος aiNet χρησιμοποιεί έναν μηχανισμό ανταγωνισμού για την απομάκρυνση των Β-λεμφοκυττάρων με τις χειρότερες επιδόσεις από τον πληθυσμό. Αυτό το βήμα συμβάλλει στη διατήρηση ενός συνόλου Β-λεμφοκυττάρων υψηλής απόδοσης [9].

Τέλος, ο αλγόριθμος aiNet χρησιμοποιεί έναν κατασταλτικό μηχανισμό για την απομάκρυνση κυττάρων με παρόμοιες ιδιαιτερότητες από τον πληθυσμό. Αυτό το βήμα συμβάλλει στη διασφάλιση της ποικιλομορφίας εντός του δικτύου των Β-λεμφοκυττάρων και στην αποφυγή της υπερεξειδίκευσης [23]. Συνολικά, το δίκτυο των Β-λεμφοκυττάρων που προκύπτει αντιπροσωπεύει ομάδες μέσα στα δεδομένα και μπορεί να χρησιμοποιηθεί για εργασίες ταξινόμησης ή ομαδοποίησης. Οι λεπτομέρειες του αλγορίθμου aiNet μπορεί να διαφέρουν ανάλογα με το πρόβλημα που αντιμετωπίζεται και τις παραμέτρους που επιλέγονται.

Ένας γενικός αλγόριθμος ανοσολογικού δικτύου [5],[9] βασισμένος στο μοντέλο aiNet αποτελείται συνήθως από τα ακόλουθα βήματα :

1. *Αρχικοποίηση*: Δημιουργία ενός πληθυσμού τυχαίων αντισωμάτων, τα οποία αντιπροσωπεύουν υποψήφιες λύσεις στο πρόβλημα.

2. *Αντιγονική παρουσίαση*: Ο αλγόριθμος αξιολογεί τη συγγένεια (ομοιότητα) κάθε αντισώματος σε σχέση με το χώρο του προβλήματος. Τα αντισώματα με υψηλή συγγένεια επιλέγονται για περαιτέρω επεξεργασία.
3. *Κλωνική επιλογή*: Επιλογή ενός αριθμού αντισωμάτων με υψηλή συγγένεια και κλωνοποίηση αναλογικά με τη συγγένειά τους.
4. *Υπερμετάλλαξη*: Τα λεμφοκύτταρα στην συνέχεια επιδέχονται τυχαίες αλλαγές (μεταλλάξεις), κάτι που αλλάζει το γενότυπο του λεμφοκυττάρου και δημιουργεί ποικιλομορφία στον πληθυσμό.
5. *Ανταγωνισμός:* Τα νέα αντισώματα συγκρίνονται με τον υπάρχοντα πληθυσμό αντισωμάτων και επιλέγονται τα καταλληλότερα αντισώματα για να προχωρήσουν στην επόμενη γενιά. Αυτό το βήμα διασφαλίζει ότι μόνο τα πιο κατάλληλα αντισώματα διατηρούνται στον πληθυσμό.
6. *Τερματισμός*: Ο αλγόριθμος aiNet επαναλαμβάνει τα βήματα 2-5 μέχρι να ικανοποιηθεί ένα κριτήριο τερματισμού, όπως ένας μέγιστος αριθμός επαναλήψεων ή ένα ελάχιστο επίπεδο βελτίωσης της καταλληλότητας.
7. *Έξοδος*: Ένα δίκτυο ανιχνευτών Β-λεμφοκυττάρων ικανών να ανιχνεύουν “ξένα” πρότυπα.

Με βάση τον aiNET έχουν αναπτυχθεί τέσσερις αλγόριθμοι που συμβάλλουν στην επέκταση του πλαισίου εφαρμογής των ανοσολογικών δικτύων. Κάθε ένα από αυτά τα μοντέλα προσφέρει μοναδικές δυνατότητες και πλεονεκτήματα, καθιστώντας τα κατάλληλα για μια σειρά από εργασίες βελτιστοποίησης και ταξινόμησης [23] :

Opt-aiNet: Αναπτύχθηκε για την επίλυση προβλημάτων βελτιστοποίησης πολυτροπικών συναρτήσεων. Στόχος του είναι η εύρεση πολλαπλών βέλτιστων λύσεων. Ένα από τα ιδιαίτερα χαρακτηριστικά του Opt-aiNet είναι η ικανότητά του να αναζητά δυναμικά το βέλτιστο μέγεθος του πληθυσμού. Στους περισσότερους αλγορίθμους βελτιστοποίησης, το μέγεθος των πιθανών λύσεων είναι είτε σταθερό είτε καθορίζεται μέσω δοκιμής και σφάλματος, το οποίο μπορεί να είναι χρονοβόρο και λιγότερο αποτελεσματικό. Ωστόσο, η δυναμική προσέγγιση του Opt-aiNet του επιτρέπει να προσαρμόζει το μέγεθος του πληθυσμού με βάση την πολυπλοκότητα και τις απαιτήσεις του εκάστοτε προβλήματος. Αυτό βασίζεται σε ένα κατώφλι καταστολής δικτύου και σε ένα σαφώς καθορισμένο κριτήριο διακοπής. Ο Opt-aiNet είναι ικανός να συνδυάζει την εκμετάλλευση με την εξερεύνηση του τοπίου καταλληλότητας. Αυτό σημαίνει ότι μπορεί τόσο να βελτιώσει τις υπάρχουσες καλές λύσεις όσο και να ανακαλύψει νέες περιοχές του χώρου αναζήτησης. Ο αλγόριθμος χρησιμοποιεί τόσο τοπικές όσο και παγκόσμιες μεθόδους αναζήτησης για την εύρεση νέων και καλύτερων λύσεων. Αυτό τον καθιστά ευέλικτο και αποτελεσματικό για μια ποικιλία προβλημάτων βελτιστοποίησης. Επιπλέον, ο Opt-aiNet έχει την ικανότητα να εντοπίζει και να διατηρεί σταθερές τοπικές βέλτιστες λύσεις, οι οποίες μπορεί να είναι ζωτικής σημασίας σε προβλήματα όπου υπάρχουν πολλαπλές καλές λύσεις.

Omni-aiNet: Είναι ένας ευέλικτος αλγόριθμος που έχει σχεδιαστεί για την αντιμετώπιση προβλημάτων βελτιστοποίησης ενός ή και πολλαπλών στόχων. Ενσωματώνει τις αρχές του omni-optimization που αποτελεί μια έννοια στη θεωρία της βελτιστοποίησης που στοχεύει στην εύρεση πολλαπλών τύπων βέλτιστων λύσεων για ένα δεδομένο πρόβλημα, αντί να εστιάζει σε μια μόνο βέλτιστη λύση. Στην περίπτωση του Omni-aiNet αυτό γίνεται με αλγορίθμους εμπνευσμένους από το ανοσοποιητικό σύστημα. Επίσης, ο Omni-aiNet είναι σε θέση να κατανοεί την εγγενή πολυπλοκότητα

του εκάστοτε προβλήματος βελτιστοποίησης και προσαρμόζεται ανάλογα με τη στρατηγική αναζήτησης. Αυτό τον καθιστά ιδιαίτερα ευέλικτο και εφαρμόσιμο σε ένα ευρύ φάσμα προβλημάτων. Όπως και ο Opt-aiNet, έτσι και ο Omni-aiNet μπορεί να προσαρμόζει δυναμικά το μέγεθος του πληθυσμού του κατά τη φάση εκτέλεσης. Αυτό καθορίζεται από ένα προκαθορισμένο κατώφλι καταστολής, το οποίο βοηθά στη διατήρηση της υπολογιστικής αποδοτικότητας. Επιπλέον, ο αλγόριθμος χρησιμοποιεί έναν νέο μηχανισμό πλέγματος (grid mechanism) για τον έλεγχο της διασποράς των λύσεων στον χώρο. Αυτό εξασφαλίζει ότι ο αλγόριθμος δεν συγκλίνει πρόωρα και εξερευνά ένα ποικίλο σύνολο λύσεων.

MOM-aiNet: Επεκτείνει τις δυνατότητες του aiNet στη βελτιστοποίηση πολλαπλών στόχων και πολλαπλών πληθυσμών, με έμφαση στις εργασίες παράλληλης ομαδοποίησης (biclustering). Ένα από τα ιδιαίτερα χαρακτηριστικά του MOM-aiNet είναι η ικανότητά του να επιστρέφει πολλαπλά σύνολα μη επικρατέστερων λύσεων. Αυτό είναι ιδιαίτερα χρήσιμο σε προβλήματα όπου υπάρχουν πολλές εξίσου καλές λύσεις. Ο αλγόριθμος χρησιμοποιεί την έννοια της κυριαρχίας για να αξιολογήσει και να συγκρίνει την ποιότητα των λύσεων. Αυτό προσθέτει ένα επιπλέον επίπεδο ανθεκτικότητας στη διαδικασία βελτιστοποίησης. Επιπρόσθετα, ο MOM-aiNet είναι σε θέση να παράγει παράλληλες συστάδες που είναι αυθαίρετα τοποθετημένες και ενδεχομένως επικαλυπτόμενες, παρέχοντας μια διαφοροποιημένη κατανόηση της υποκείμενης δομής δεδομένων. Πιο συγκεκριμένα, κάθε σύνολο μη επικρατέστερων λύσεων αντιστοιχεί δυνητικά σε παράλληλες συστάδες που εξάγουν διακριτές συσχετίσεις γραμμών και στηλών του πίνακα δεδομένων.

Opt-aiNet-AA-Clust: Είναι μια εξειδικευμένη παραλλαγή του opt-aiNet που έχει σχεδιαστεί για την πρόβλεψη της λειτουργίας των πρωτεϊνών. Εισάγει έναν νέο τρόπο αναπαράστασης των πρωτεϊνών για τη βελτίωση της ακρίβειας των αλγορίθμων ιεραρχικής ταξινόμησης. Ο αλγόριθμος ομαδοποιεί τα αμινοξέα σε λειτουργικές ομάδες όπως υδρόφοβες, ουδέτερες και πολικές. Αυτή η νέα αναπαράσταση ενισχύει την ακρίβεια πρόβλεψης για τις πρωτεϊνικές λειτουργίες. Ο Opt-aiNet-AA-Clust μπορεί να προβλέψει τις πρωτεϊνικές λειτουργίες σε πολλαπλά επίπεδα λεπτομέρειας, παρέχοντας μια πιο ολοκληρωμένη κατανόηση των ρόλων των πρωτεϊνών. Έχει την ιδιότητα να μετατρέπει τις αλληλουχίες αμινοξέων σε μια απλουστευμένη μορφή που αντιπροσωπεύει τις λειτουργικές ομάδες στις οποίες ανήκει κάθε αμινοξύ. Αυτή η απλούστευση βοηθά στην υπολογιστική αποτελεσματικότητα και την ακρίβεια πρόβλεψης του μοντέλου.

Ανακεφαλαιώνοντας, σε έναν αλγόριθμο aiNet, κάθε στοιχείο δικτύου αντιστοιχεί σε ένα μόριο αντισώματος. Η συγγένεια μεταξύ αντισωμάτων χρησιμοποιείται ως μέτρο της ομοιότητάς τους, με υψηλότερη συγγένεια να υποδηλώνει μεγαλύτερο βαθμό ομοιότητας. Κατά τη διάρκεια της διαδικασίας εκπαίδευσης, ο αλγόριθμος aiNet εντοπίζει τα αντισώματα που είναι πιο αποτελεσματικά στην αναγνώριση μοτίβων στα δεδομένα εκπαίδευσης. Αυτό το επιτυγχάνει συγκρίνοντας τη συγγένεια των αντισωμάτων με τα δεδομένα εισόδου και επιλέγοντας εκείνα με τη μεγαλύτερη συγγένεια. Ωστόσο, για να αποφευχθεί ο πλεονασμός στο δίκτυο και να εξασφαλιστεί η ποικιλομορφία μεταξύ των αντισωμάτων, ο αλγόριθμος aiNet ελέγχει επίσης τη συγγένεια μεταξύ ζευγών αντισωμάτων. Εάν η συγγένεια μεταξύ δύο αντισωμάτων είναι μεγαλύτερη από ένα κατώφλι καταστολής (network suppression threshold) που έχουμε ορίσει, το ένα από αυτά αφαιρείται από το δίκτυο. Με τον τρόπο αυτό διασφαλίζεται ότι το δίκτυο δεν εξειδικεύεται υπερβολικά σε ένα συγκεκριμένο υποσύνολο των δεδομένων εκπαίδευσης και ότι είναι σε θέση να αναγνωρίζει ένα ευρύ φάσμα μοτίβων [5].

Το μεγάλο πλεονεκτήματα των αλγορίθμων AINE έχει να κάνει με το γεγονός ότι το δίκτυο προσαρμόζεται συνεχώς για να διατηρήσει μια σταθερή κατάσταση που αντικατοπτρίζει τα συνολικά

αποτελέσματα της αλληλεπίδρασης με το περιβάλλον. Έπειτα, με τα ανοσολογικά δίκτυα επιτυγχάνεται αναγνώριση αντιγόνων με τη διατήρηση του ιδιοτυπικού αρχείου διασυνδεδεμένων Β-κυττάρων το οποίο προσαρμόζεται σε τοπικό επίπεδο και εμφανίζει αναδυόμενες ιδιότητες σε παγκόσμιο επίπεδο. Τα AINE είναι ένας ευέλικτος μηχανισμός επιλογής, αυτόνομος και πλήρως αποκεντρωμένος. Η διέγερση και η καταστολή θα σχηματίσουν ένα δίκτυο μεγάλης κλίμακας (μια παράλληλη κατανεμημένη αρχιτεκτονική επεξεργασίας) οδηγώντας στη σταθεροποίηση του δικτύου [28]. Εντούτοις, τα ανοσολογικά δίκτυα μπορεί να είναι πολύπλοκα και δυσνόητα. Έχουν περιορισμένη εφαρμοσιμότητα και μεγάλη επιβάρυνση της υπολογιστικής πολυπλοκότητας ενώ υπάρχει ακόμα έλλειψη κατανόησης της δυναμικής τους, γεγονός που καθιστά δύσκολη την υλοποίηση και την αποσφαλμάτωση [47].

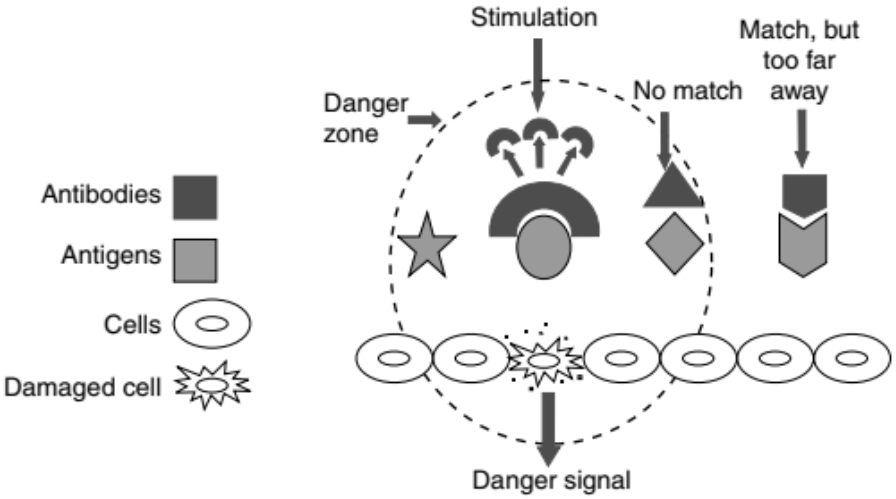
Οι αλγόριθμοι ανοσολογικών δικτύων χρησιμοποιούνται συνήθως σε διάφορους τομείς εφαρμογών, όπως:

- Ομαδοποίηση/μη επιβλεπόμενη ομαδοποίηση/ταξινόμηση [44],[29]
- Εξόρυξη δεδομένων / ανάλυση δεδομένων / οπτικοποίηση δεδομένων [32]
- Ταξινόμηση κειμένου [44],[29],[32]
- Διαιτησία (arbitration) συμπεριφοράς κινητών ρομπότ [32]
- Βελτιστοποίηση (βελτιστοποίηση πολυτροπικών συναρτήσεων) [32]

3.4.4 The Danger Theory - Dendritic Cell Algorithms (DCA)

Η Θεωρία Κινδύνου (ΘΚ) - Danger Theory (DT) προτείνει μια διαφορετική προοπτική για το πώς το ανοσοποιητικό σύστημα ανταποκρίνεται στις απειλές. Αντί να εστιάζει στην ξενικότητα ενός αντιγόνου (διάκριση εαυτού/ξένου), δίνει έμφαση στη σημασία των σημάτων κινδύνου που απελευθερώνονται ως απάντηση όταν τα κύτταρα τραυματίζονται ή υποδέχονται μεγάλη πίεση. Η θεωρία αυτή προτάθηκε για πρώτη φορά από την Polly Matzinger (1994) ως εναλλακτική λύση στο παραδοσιακό μοντέλο διάκρισης εαυτού/ξένου του ανοσοποιητικού συστήματος. Εμβαθύνοντας, η θεωρία υποδηλώνει ότι το ανοσοποιητικό σύστημα δεν ενεργοποιείται μόνο από την παρουσία ξένων αντιγόνων αλλά και από την παρουσία σημάτων κινδύνου που απελευθερώνονται από κατεστραμμένα ή προβληματικά κύτταρα και προειδοποιούν το ανοσοποιητικό σύστημα για την παρουσία πιθανών απειλών [48].

Η Εικόνα 3.4 απεικονίζει πώς θα μπορούσαμε να φανταστούμε μια ανοσολογική αντίδραση σύμφωνα με τη Θεωρία Κινδύνου. Όταν ένα κύτταρο βρίσκεται σε κίνδυνο, απελευθερώνει σήματα κινδύνου που δημιουργούν μια ζώνη κινδύνου γύρω του. Τα αντιγονοπαρουσιαστικά κύτταρα - Antigen-Presenting Cells (APC), όπως τα μακροφάγα, συλλαμβάνουν τα αντιγόνα που βρίσκονται κοντά, συμπεριλαμβανομένων εκείνων που προέρχονται από το κύτταρο που βρίσκεται σε κίνδυνο, και τα μεταφέρουν στον τοπικό λεμφαδένα. Εκεί, τα αντιγόνα παρουσιάζονται στα λεμφοκύτταρα, συμπεριλαμβανομένων των Β-λεμφοκυττάρων, τα οποία παράγουν αντισώματα που ταιριάζουν με τα αντιγόνα. Μόνο τα Β-λεμφοκύτταρα που αναγνωρίζουν αντιγόνα εντός της ζώνης κινδύνου θα διεγερθούν και θα υποστούν κλωνική επέκταση, ενώ εκείνα που δεν ταιριάζουν ή βρίσκονται πολύ μακριά δεν θα ενεργοποιηθούν. Αυτή η επιλεκτική διαδικασία διασφαλίζει ότι η ανοσολογική απόκριση προσαρμόζεται στα συγκεκριμένα αντιγόνα που βρίσκονται κοντά στην ζώνη κινδύνου, αντί να ανταποκρίνεται αδιακρίτως σε όλα τα αντιγόνα [5], [14]. Η θεωρία αυτή τονίζει τη σημασία του πλαισίου στο οποίο παρουσιάζονται τα αντιγόνα στο ανοσοποιητικό σύστημα, αντί να εστιάζει απλώς στα ίδια τα αντιγόνα.



Εικόνα 3.4: Απεικόνιση της ΘΚ (ζώνη κινδύνου, σήμα κινδύνου κ.λπ.) [14]

Το μοντέλο κινδύνου μπορεί να θεωρηθεί ως επέκταση του μοντέλου δύο σημάτων των Bretscher και Cohn, όπου προστίθεται η έννοια της συνδιέγερσης (co-stimulation) ως σήμα που δείχνει αν ένα αντιγόνο είναι επικίνδυνο ή όχι. Πιο συγκεκριμένα, σε αυτό το μοντέλο το πρώτο σήμα (σήμα 1) είναι η αναγνώριση του αντιγόνου, δηλαδή η ικανότητα των Τ-λεμφοκυττάρων και των Β-λεμφοκυττάρων να αναγνωρίζουν ένα συγκεκριμένο αντιγόνο μέσω των μοναδικών υποδοχέων τους. Το δεύτερο σήμα (σήμα 2) είναι η συνδιέγερση, η οποία επιβεβαιώνει την ξενικότητα του αντιγόνου και ενεργοποιεί το Τ ή το Β-λεμφοκύτταρο. Στη ΘΚ, αυτό το δεύτερο σήμα ερμηνεύεται ως σήμα που επιβεβαιώνει τον κίνδυνο που συνδέεται με το αντιγόνο και όχι απλώς την ξενικότητά του [49].

Η Polly Matzinger εφάρμοσε περαιτέρω τους τρεις νόμους των λεμφοκυττάρων (the laws of lymphocytes) στη ΘΚ [50]:

1. *Νόμος 1:* Ένα λεμφοκύτταρο ενεργοποιείται εάν και μόνο εάν λάβει τόσο το σήμα 1 όσο και το σήμα 2. Ελλείψει ενός από αυτά τα σήματα, τα λεμφοκύτταρα παραμένουν ανενεργά.
2. *Νόμος 2*: Ένα λεμφοκύτταρο δέχεται το σήμα 2 μόνο από τα αντιγονοπαρουσιαστικά κύτταρα (ή, στην περίπτωση των Β-λεμφκυττάρων, από τα Τ βοηθητικά κύτταρα). Τα Β-λεμφοκύτταρα μπορούν να λειτουργήσουν ως αντιγονοπαρουσιαστικά κύτταρα μόνο για έμπειρα Τ-λεμφοκύτταρα (μνήμης). Είναι επίσης σημαντικό να σημειωθεί ότι το σήμα 1 μπορεί να προέρχεται και από άλλα κύτταρα εκτός από τα αντιγονοπαρουσιαστικά κύτταρα.
3. *Νόμος 3*: Μόλις ενεργοποιηθούν, τα λεμφοκύτταρα δεν χρειάζονται το σήμα 2- επανέρχονται σε κατάσταση ηρεμίας μετά από σύντομο χρονικό διάστημα.

Αυτοί οι κανόνες ισχύουν συνήθως για όλα τα ώριμα λεμφοκύτταρα. Τα ανώριμα λεμφοκύτταρα δεν είναι σε θέση να δεχτούν το σήμα 2, γεγονός που συμβάλλει στο να διασφαλιστεί ότι δεν ανταποκρίνονται σε αυτοαντιγόνα και υφίστανται αρνητική επιλογή. Από την άλλη πλευρά, τα κύτταρα-ενεργοποιητές (effector cells) δεν απαιτούν το σήμα 2 για την ενεργοποίηση και ανταποκρίνονται μόνο στο σήμα 1. Αφού επιτελέσουν τις λειτουργίες τους ως δρώντα κύτταρα, επανέρχονται σε κατάσταση ηρεμίας λίγο αργότερα [5].

Ένας από τους περιορισμούς της ΘΚ είναι ότι η ακριβής φύση του σήματος κινδύνου δεν είναι καλά κατανοητή. Αυτή η αβεβαιότητα σχετικά με τη φύση του σήματος κινδύνου εγείρει ερωτήματα όσον αφορά τον τρόπο διάκρισης μεταξύ επικίνδυνων και μη επικίνδυνων ερεθισμάτων. Επίσης, υπάρχουν περιπτώσεις όπου το ανοσοποιητικό σύστημα πρέπει να αντιδράσει σε πιθανές απειλές, ακόμη και αν αυτές δεν είναι απαραίτητα επικίνδυνες από μόνες τους, όπως στην περίπτωση βλάβης ιστών από κοψίματα ή μεταμοσχεύσεις. Σε αυτές τις περιπτώσεις, το ανοσοποιητικό σύστημα πρέπει να είναι σε θέση να διακρίνει μεταξύ επικίνδυνων και μη επικίνδυνων σημάτων [14]. Επιπλέον, η ΘΚ δεν έχει συμβιβαστεί πλήρως με τα αυτοάνοσα νοσήματα, τα οποία συμβαίνουν όταν το ανοσοποιητικό σύστημα επιτίθεται λανθασμένα στα κύτταρα και τους ιστούς του ίδιου του οργανισμού. Αυτό υποδηλώνει ότι μπορεί να υπάρχουν περιορισμοί στην εστίαση της ΘΚ πάνω στα σήματα κινδύνου ως πρωταρχικό έναυσμα για τις ανοσολογικές αντιδράσεις [23].

Ο αλγόριθμος των δενδριτικών κυττάρων - Dendritic Cell Algorithm (DCA) είναι ένας αλγόριθμος που αναπτύχθηκε με βάση τη ΘΚ και είναι εμπνευσμένος από τη συμπεριφορά των δενδριτικών κυττάρων στους ιστούς του σώματος. Τα δενδριτικά κύτταρα συλλέγουν αντιγόνα και άλλα σήματα που παρέχουν μια εικόνα της τρέχουσας κατάστασης των ιστών και καθορίζουν αν το αντιγόνο έχει συλλεχθεί σε ασφαλές ή επικίνδυνο πλαίσιο. Ο αλγόριθμος των δενδριτικών κυττάρων έχει σχεδιαστεί για να ταξινομεί στοιχεία δεδομένων, όπως αντιγόνα, είτε ως καλοήθη (benign) είτε ως κακοήθη (malignant) με βάση την παρουσία ή την απουσία σημάτων που σχετίζονται με μη φυσιολογική συμπεριφορά (PAMP), κίνδυνο, ασφάλεια και προφλεγμονώδεις αντιδράσεις [15]. Τα σήματα αυτά προέρχονται από πραγματικά βιολογικά σήματα και τα χαρακτηριστικά τους συνοψίζονται ως εξής [51] :

- Τα σήματα PAMP είναι πρωτεΐνες που εκφράζονται αποκλειστικά από βακτήρια, οι οποίες προκαλούν την ωρίμανση των ανώριμων δενδριτικών κυττάρων σε πλήρως λειτουργικά δενδριτικά κύτταρα. Αυτή η απόκριση είναι ένας γρήγορος και ισχυρός τρόπος ενεργοποίησης του ανοσοποιητικού συστήματος ως απάντηση σε ένα παθογόνο.
- Τα σήματα κινδύνου παράγονται ως αποτέλεσμα απρογραμμάτιστου νεκρωτικού κυτταρικού θανάτου, ο οποίος οδηγεί στη χαοτική διάσπαση των εσωτερικών συστατικών και στη συσσώρευση σημάτων κινδύνου στον ιστό. Τα δενδριτικά κύτταρα είναι ευαίσθητα στις μεταβολές της συγκέντρωσης των σημάτων κινδύνου και η ανίχνευσή τους μπορεί να υποδείξει μια πιθανή ανωμαλία στον ιστό. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η παρουσία σημάτων κινδύνου δεν υποδεικνύει απαραίτητα μια ανώμαλη κατάσταση, αλλά μάλλον αυξάνει την πιθανότητα εμφάνισης μιας τέτοιας κατάστασης σε σύγκριση με τις κανονικές συνθήκες. Ο DCA αξιοποιεί αυτή την ευαισθησία στα σήματα κινδύνου προκειμένου να ανιχνεύσει ανωμαλίες και να ταξινομήσει ανάλογα τα στοιχεία δεδομένων.
- Τα ασφαλή σήματα παράγονται μέσω της διαδικασίας του φυσιολογικού κυτταρικού θανάτου, η οποία είναι μια αυστηρά ελεγχόμενη διαδικασία που λαμβάνει χώρα για ρυθμιστικούς λόγους. Όταν τα κύτταρα πεθαίνουν με αυτόν τον τρόπο, διάφορα σήματα απελευθερώνονται στον ιστό, συμπεριλαμβανομένων των "σημάτων ασφαλείας", τα οποία οδηγούν σε ανοσοκαταστολή. Η παρουσία ασφαλών σημάτων υποδηλώνει ότι δεν υπάρχουν ανωμαλίες και ότι το ανοσοποιητικό σύστημα μπορεί να αγνοήσει με ασφάλεια τα σήματα. Ο DCA αξιοποιεί την παρουσία ασφαλών σημάτων για να ταξινομήσει στοιχεία δεδομένων ως μη ανώμαλα και να διασφαλίσει ότι δεν ταξινομούνται εσφαλμένα ως επικίνδυνα.
- Οι φλεγμονώδεις κυτταροκίνες μπορούν να απελευθερωθούν ως αποτέλεσμα τραυματισμού ή ιστικής βλάβης, αλλά η διαδικασία της φλεγμονής δεν είναι αρκετή για να διεγείρει από μόνη

της τα δενδριτικά κύτταρα. Ωστόσο, οι φλεγμονώδεις κυτταροκίνες μπορούν να ενισχύσουν τις επιδράσεις των άλλων τριών κατηγοριών σημάτων (σήματα κινδύνου, PAMPs και ασφαλή σήματα), καθιστώντας ευκολότερο για τα δενδριτικά κύτταρα να ανιχνεύσουν πιθανές ανωμαλίες στον ιστό. Ο DCA εκμεταλλεύεται αυτό το φαινόμενο ενίσχυσης για να βελτιώσει την ικανότητά του να ανιχνεύει και να ταξινομεί ανωμαλίες.

Όταν έχουμε ένα πρόβλημα στο οποίο θέλουμε να εφαρμόσουμε τον DCA τα δεδομένα του προβλήματος θα ταξινομηθούν ως καλοήθη ή κακοήθη με βάση αυτά τα σήματα. Το σήμα PAMP είναι ιδιαίτερα ενδεικτικό μιας ανωμαλίας, ενώ το σήμα κινδύνου είναι μέτρια ενδεικτικό μιας μη φυσιολογικής συμπεριφοράς. Το ασφαλές σήμα υποδεικνύει την κανονική λειτουργία του συστήματος, ενώ το προφλεγμονώδες σήμα είναι ένα γενικό σημάδι δυσχέρειας του συστήματος. Η αντιστοίχιση των σημάτων στα στοιχεία δεδομένων είναι η κύρια πρόκληση της υλοποίησης του DCA. Απαιτεί βαθιά κατανόηση του προβληματικού τομέα και του τρόπου με τον οποίο τα σήματα σχετίζονται με την κανονική και μη κανονική συμπεριφορά του συστήματος ή της διαδικασίας που παρακολουθείται. Μια προσεκτική ανάλυση των σημάτων και των πιθανών πηγών μεταβολής τους είναι απαραίτητη για την ακριβή αντιστοίχισή τους στα στοιχεία δεδομένων. Μόλις καθοριστεί η αντιστοίχιση, ο DCA μπορεί στη συνέχεια να εκπαιδευτεί και να χρησιμοποιηθεί για την ταξινόμηση νέων στοιχείων δεδομένων με βάση τα σχετικά σήματα [51].

Η χρήση αυτών των σημάτων που προέρχονται από τις συνέπειες της συμπεριφοράς των στοιχείων δεδομένων και όχι από τη φυσική τους παρουσία, επιτρέπει στον αλγόριθμο των δενδριτικών κυττάρων να λειτουργεί σε δυναμικά μεταβαλλόμενα περιβάλλοντα. Ωστόσο, ένας από τους περιορισμούς του DCA είναι ότι επί του παρόντος δεν μπορεί να λειτουργήσει σε πραγματικό χρόνο [15],[51]. Αυτό σημαίνει ότι ο αλγόριθμος απαιτεί τη συλλογή και επεξεργασία όλων των δεδομένων εκ των προτέρων, αντί να είναι σε θέση να αναλύει συνεχώς νέα δεδομένα καθώς αυτά φτάνουν σε πραγματικό χρόνο. Ως εκ τούτου, τυχόν ανωμαλίες που εμφανίζονται στο σύστημα δεν μπορούν να εντοπιστούν και να ληφθούν άμεσα μέτρα. Αντ' αυτού, ο DCA απαιτεί ένα βήμα επεξεργασίας, όπου όλα τα δεδομένα που συλλέγονται αναλύονται και ταξινομούνται ως καλοήθη ή κακοήθη. Για να αντιμετωπίσουν τους περιορισμούς της λειτουργίας σε πραγματικό χρόνο, οι Lay και Bate (2007) ανέπτυξαν έναν DCA πραγματικού χρόνου που είναι ικανός να μεταβάλλει τις υπερβάσεις του χρονοδιαγράμματος σε λειτουργικά συστήματα πραγματικού χρόνου. Αυτή η πρόοδος επιτρέπει στον DCA να λειτουργεί με πιο ευέλικτο και προσαρμοστικό τρόπο, ο οποίος είναι κρίσιμος για πολλές εφαρμογές [52]. Ένα άλλο δυνητικό πρόβλημα του DCA είναι ότι η πολλαπλή δειγματοληψία αντιγόνων από τα δενδριτικά κύτταρα μπορεί να προκαλέσει λανθασμένη ταξινόμηση γύρω από τα όρια όπου τα στοιχεία δεδομένων εναλλάσσονται μεταξύ “ασφαλών” και “επικίνδυνων” πλαισίων [15]. Αυτό οφείλεται στο γεγονός ότι τα δενδριτικά κύτταρα μπορεί να μην είναι σε θέση να προσδιορίσουν με ακρίβεια το πλαίσιο του αντιγόνου, ιδίως όταν εφαρμόζεται σε προβλήματα όπου οι εναλλαγές πλαισίου στα στοιχεία δεδομένων είναι συχνές. Ως αποτέλεσμα, ο DCA ενδέχεται να ταξινομήσει ένα αντιγόνο ως ασφαλές ή επικίνδυνο εσφαλμένα, οδηγώντας σε λανθασμένη ταξινόμηση.

Ένας γενικός αλγόριθμος δενδριτικών κυττάρων [9],[15] αποτελείται συνήθως από τα ακόλουθα βήματα :

1. *Αρχικοποίηση*: Δημιουργία ενός πληθυσμού δενδριτικών κυττάρων, των παραμέτρων τους και του συνόλου δεδομένων (αντιγόνα).
2. *Επεξεργασία δεδομένων*: Κάθε αντιγόνο επεξεργάζεται από κάθε δενδριτικό κύτταρο και υπολογίζεται η συγγένεια του αντιγόνου με τους υποδοχείς του δενδριτικού κυττάρου.

3. *Υπολογισμός συγγένειας*: Ο υπολογισμός της συγγένειας περιλαμβάνει τον προσδιορισμό του βαθμού ταύτισης μεταξύ του αντιγόνου και των υποδοχέων του δενδριτικού κυττάρου. Αυτό γίνεται λαμβάνοντας υπόψη τη συγκέντρωση των σημάτων PAMP, κινδύνου, ασφάλειας και προφλεγμονωδών σημάτων που σχετίζονται με το αντιγόνο.
4. *Ταξινόμηση*: Μετά την εκπαίδευση, χρησιμοποιείται ο πληθυσμός των δενδριτικών κυττάρων για να ταξινομηθούν τα νέα δεδομένα είτε ως ανώμαλα είτε ως φυσιολογικά.
5. *Επανάληψη*: Η διαδικασία ταξινόμησης επαναλαμβάνεται για κάθε νέο στοιχείο δεδομένων, διασφαλίζοντας ότι όλα τα στοιχεία ταξινομούνται χρησιμοποιώντας τα εκπαιδευμένα δενδριτικά κύτταρα.
6. *Τερματισμός*: Διακοπή του αλγορίθμου μόλις ικανοποιηθεί ένα κριτήριο διακοπής (π.χ. μέγιστος αριθμός επαναλήψεων, επιθυμητό επίπεδο ακρίβειας κ.λπ.).
7. *Έξοδος*: Ένα σύνολο δεδομένων (αντιγόνων) ταξινομημένο σε δύο κατηγορίες: ασφαλή (καλοήθη) και επικίνδυνα (κακοήθη)

Συνοπτικά, ο αλγόριθμος ξεκινά με την αρχικοποίηση ενός πληθυσμού δενδριτικών κυττάρων και του συνόλου δεδομένων και ακολουθεί έναν κυκλικό και επαναληπτικό τρόπο εκπαίδευσης και ταξινόμησης των δενδριτικών κυττάρων. Μετά την εκπαίδευση, τα δενδριτικά κύτταρα χρησιμοποιούνται για την ταξινόμηση νέων στοιχείων δεδομένων. Κάθε στοιχείο δεδομένων αξιολογείται από κάθε δενδριτικό κύτταρο και η ταξινόμηση καθορίζεται με βάση την υψηλότερη βαθμολογία ταξινόμησης που λαμβάνεται από τις αποκρίσεις των δενδριτικών κυττάρων. Η ακρίβεια της ταξινόμησης βελτιώνεται με κάθε επανάληψη, καθώς τα δενδριτικά κύτταρα προσαρμόζουν τις παραμέτρους τους με βάση τις επιδόσεις τους στα αντιγόνα. Το αποτέλεσμα του αλγορίθμου είναι η ταξινόμηση των νέων δεδομένων ως ανώμαλα ή φυσιολογικά, με βάση την απόκριση των δενδριτικών κυττάρων και τις παραμέτρους τους. Να επισημάνουμε ότι οι συγκεκριμένες λεπτομέρειες της αξιολόγησης και των ενημερώσεων των παραμέτρων ενδέχεται να διαφέρουν ανάλογα με την υλοποίηση και τον τομέα του προβλήματος. Ο αλγόριθμος μπορεί να προσαρμοστεί ώστε να ταιριάζει σε διαφορετικές εργασίες ταξινόμησης και χαρακτηριστικά δεδομένων.

Στο πλαίσιο των ΤΑΣ, η Θεωρία Κινδύνου έχει εφαρμοστεί για την ανάπτυξη νέων αλγορίθμων για την ανίχνευση και ταξινόμηση ανωμαλιών [14],[32] αλλά και σε προβλήματα εξόρυξης δεδομένων [53] και ρομποτικής [54]. Αυτοί οι αλγόριθμοι χρησιμοποιούν σήματα κινδύνου ή βαθμολογίες ανωμαλίας για να εντοπίσουν μια εισβολή στο σύστημα, αντί να βασίζονται αποκλειστικά στην ομοιότητα ή ανομοιότητα των χαρακτηριστικών. Με την ενσωμάτωση της έννοιας του κινδύνου, τα ΤΑΣ μπορούν να προσαρμόζονται καλύτερα στις αλλαγές του περιβάλλοντος και να ανταποκρίνονται σε νέες απειλές, πράγμα που είναι σημαντικό σε πολλές εφαρμογές του πραγματικού κόσμου.

Εν κατακλείδι, συμπεραίνουμε ότι η ΘΚ προσφέρει μια μοναδική προοπτική για το ανοσοποιητικό σύστημα και τις αντιδράσεις του, αλλά υπάρχουν ακόμη αναπάντητα ερωτήματα και προκλήσεις που πρέπει να αντιμετωπιστούν για να είναι πλήρως εφαρμόσιμη στα τεχνητά ανοσοποιητικά συστήματα και στο σχεδιασμό αποτελεσματικών εφαρμογών του πραγματικού κόσμου.

Κεφάλαιο 4ο: Τεχνητά Ανοσοποιητικά Συστήματα και Οικονομικά Δεδομένα

4.1 Εισαγωγή

Η χρηματοοικονομική περιλαμβάνει τη μελέτη και την ανάλυση διαφόρων πτυχών που σχετίζονται με την κατανομή και τη διαχείριση των χρηματοοικονομικών πόρων. Αυτό περιλαμβάνει την κατανόηση του τρόπου με τον οποίο τα άτομα, οι επιχειρήσεις και οι οργανισμοί λαμβάνουν αποφάσεις σχετικά με την απόκτηση, τη χρήση και τη διάθεση χρημάτων, περιουσιακών στοιχείων και επενδύσεων [55]. Η εξέταση των κινδύνων είναι ζωτικής σημασίας στα χρηματοοικονομικά, καθώς περιλαμβάνει την αξιολόγηση και τη διαχείριση των πιθανών αβεβαιοτήτων και κινδύνων που συνδέονται με διάφορα χρηματοοικονομικά έργα και αποφάσεις.

Η οικονομική απάτη αναφέρεται στην πράξη απόκτησης οικονομικών οφελών με παράνομα και δόλια μέσα [56]. Τον τελευταίο καιρό, παρατηρείται αύξηση της απάτης στις χρηματοπιστωτικές συναλλαγές, του ξεπλύματος χρήματος και άλλων τύπων οικονομικής απάτης, γεγονός που θέτει σημαντικές προκλήσεις για τις εταιρείες και τους κλάδους. Η επιμονή της χρηματοπιστωτικής απάτης έχει δυσμενείς επιπτώσεις στην οικονομία και την κοινωνία, με αποτέλεσμα σημαντικές χρηματικές απώλειες σε καθημερινή βάση [57],[58].

Παραδοσιακά, οι μέθοδοι ανίχνευσης της απάτης ήταν χειροκίνητες, χρονοβόρες, δαπανηρές, ανακριβείς και συχνά ανεφάρμοστες. Ωστόσο, με την πρόοδο της τεχνητής νοημοσύνης, της μηχανικής μάθησης και των τεχνικών εξόρυξης δεδομένων, έχουν καταβληθεί προσπάθειες για την αξιοποίηση αυτών των τεχνολογιών στον εντοπισμό δόλιων δραστηριοτήτων στον χρηματοπιστωτικό τομέα. Έχουν χρησιμοποιηθεί τόσο επιβλεπόμενες όσο και μη επιβλεπόμενες μέθοδοι μηχανικής μάθησης για την πρόβλεψη και τον εντοπισμό δραστηριοτήτων απάτης [59],[60]

Μεταξύ αυτών των προσεγγίσεων, οι μέθοδοι ταξινόμησης έχουν κερδίσει δημοτικότητα για την ανίχνευση οικονομικών δόλιων συναλλαγών. Οι αλγόριθμοι ταξινόμησης χρησιμοποιούνται για τη δημιουργία μοντέλων που μπορούν να διακρίνουν μεταξύ νόμιμων και δόλιων συναλλαγών με βάση πρότυπα, χαρακτηριστικά και ιστορικά δεδομένα. Αυτά τα μοντέλα μπορούν στη συνέχεια να χρησιμοποιηθούν για την ταξινόμηση νέων συναλλαγών ως δυνητικά δόλιων ή νόμιμων, βοηθώντας στην πρόληψη και την ανίχνευση της οικονομικής απάτης.

4.2 Κατηγορίες οικονομικής απάτης

Υπάρχουν πολλοί διαφορετικοί τύποι οικονομικής απάτης, και μια σύντομη περιγραφή μερικών από τους σημαντικότερους τύπους θα παρατεθεί σε αυτή την ενότητα. Οι τύποι απάτης επιλέχθηκαν από τον κατάλογο που παρέχεται από το Ομοσπονδιακό Γραφείο Ερευνών των ΗΠΑ [61], [62].

4.2.1 Απάτη με πιστωτική κάρτα

Οι πιστωτικές κάρτες χρησιμοποιούνται συνήθως για ηλεκτρονικές οικονομικές συναλλαγές χωρίς την ανάγκη χρήσης φυσικών μετρητών. Η χρήση μιας πιστωτικής κάρτας χωρίς την κατάλληλη εξουσιοδότηση του ιδιοκτήτη θεωρείται παράνομη και δόλια. Όταν αποκτάται μη εξουσιοδοτημένη

πρόσβαση σε έναν λογαριασμό, κάθε συναλλαγή που πραγματοποιείται θεωρείται παράνομη [57]. Η απάτη με πιστωτικές κάρτες μπορεί να κατηγοριοποιηθεί σε δύο κύριους τύπους [63] : απάτη εκτός σύνδεσης και απάτη με απευθείας σύνδεση.

Η απάτη εκτός σύνδεσης αναφέρεται σε περιπτώσεις όπου οι απατεώνες χρησιμοποιούν κλεμμένες πιστωτικές κάρτες, που συχνά προέρχονται από γνήσιους κατόχους καρτών, για να πραγματοποιήσουν παράνομες συναλλαγές. Αυτό μπορεί να περιλαμβάνει φυσικές συναλλαγές, όπου η κλεμμένη κάρτα παρουσιάζεται στο χώρο ενός εμπόρου. Από την άλλη πλευρά, οι διαδικτυακοί απατεώνες επιδίδονται σε δόλιες δραστηριότητες κατά τη διάρκεια ηλεκτρονικών συναλλαγών που πραγματοποιούνται μέσω του διαδικτύου. Η ανωνυμία και η διαθεσιμότητα αυτών των απομακρυσμένων μεθόδων έχουν οδηγήσει στην επικράτηση του οργανωμένου εγκλήματος στην απάτη με πιστωτικές κάρτες.

Οι πληροφορίες του κατόχου της κάρτας μπορούν να αποκτηθούν με διάφορες μεθόδους. Το "ψάρεμα" (phising) περιλαμβάνει έναν απατεώνα που υποδύεται έναν υπάλληλο οικονομικών για να πείσει τον χρήστη να αποκαλύψει τα στοιχεία του. Οι “swipers” ή οι “skimmers”, όπως ονομάζονται, παρέχουν μια διεπαφή σε μια συσκευή ATM ή POS που μπορεί να διαβάσει απευθείας την κάρτα. Ολόκληρες βάσεις δεδομένων με τις πληροφορίες του χρήστη μπορούν να αποκτηθούν εάν ο απατεώνας είναι σε θέση να παραβιάσει την ασφάλεια του δικτύου των χρηματοπιστωτικών ιδρυμάτων ή να επιστρατεύσει τη βοήθεια ενός συνεργού εντός της εταιρείας.

4.2.2 Απάτη με κινητές αξίες/αξιόγραφα και εμπορεύματα

Η απάτη επί κινητών αξιών, γνωστή και ως απάτη επί εμπορευμάτων, αναφέρεται σε μια ποικιλία μεθόδων με τις οποίες ένα άτομο εξαπατάται για να επενδύσει σε μια εταιρεία με βάση ψευδείς πληροφορίες. Περιλαμβάνει τα σχήματα πυραμίδας, τα σχήματα Ponzi, την απάτη hedge fund, την απάτη συναλλάγματος και την υπεξαίρεση [57].

4.2.3 Απάτη στις οικονομικές καταστάσεις/εταιρική απάτη

Οι οικονομικές καταστάσεις είναι τα έγγραφα που εκδίδονται από μια εταιρεία που εξηγούν λεπτομέρειες όπως τα έξοδα, τα δάνεια, τα έσοδα και τα κέρδη [64]. Μπορούν επίσης να περιλαμβάνουν σχόλια από τη διοίκηση σχετικά με την απόδοση της επιχείρησης και τα αναμενόμενα ζητήματα που ενδέχεται να προκύψουν στο μέλλον **[**65]. Οι διάφορες χρηματοοικονομικές καταστάσεις που δημοσιεύει η εταιρεία δίνουν μια συνολική εικόνα της κατάστασης της εταιρείας και μπορούν να χρησιμοποιηθούν για να δείξουν πόσο επιτυχημένη είναι η εταιρεία, να επηρεάσουν τις τιμές των μετοχών και να καθορίσουν αν μπορούν να λάβουν δάνεια. Η απάτη των οικονομικών καταστάσεων, επίσης γνωστή ως εταιρική απάτη, περιλαμβάνει την παραποίηση αυτών των δηλώσεων για να κάνει την εταιρεία να εμφανίζεται πιο προσιτή. Οι λόγοι για τη διάπραξη απάτης στις χρηματοοικονομικές καταστάσεις περιλαμβάνουν τη βελτίωση της απόδοσης των μετοχών, τη μείωση των φορολογικών υποχρεώσεων ή ως προσπάθεια υπερβολής των επιδόσεων λόγω διοικητικής πίεσης [64]. Η διάγνωση της απάτης των χρηματοοικονομικών καταστάσεων μπορεί να είναι δύσκολη λόγω της γενικής έλλειψης κατανόησης του κλάδου, της σπάνιας συχνότητας με την οποία συμβαίνει και του γεγονότος ότι συνήθως διαπράττεται από άτομα με γνώσεις εντός του κλάδου, τα οποία είναι ικανά να συγκαλύψουν την απάτη τους **[**66].

Η Ένωση Πιστοποιημένων Ελεγκτών Απάτης των ΗΠΑ - Association of Certified Fraud Examiners (ACFE) έχει συμπεράνει μετά από έρευνα ότι το 10% των περιστατικών που αφορούν έγκλημα λευκού κολάρου – white collar crime περιλαμβάνει παραποίηση των οικονομικών καταστάσεων [67].

Η απάτη στις οικονομικές καταστάσεις είχε ως αποτέλεσμα τις πιο σημαντικές απώλειες μεταξύ αυτών.

4.2.4 Ασφαλιστική απάτη

Η ασφαλιστική απάτη αναφέρεται στην εσκεμμένη κατάχρηση ενός ασφαλιστηρίου συμβολαίου προκειμένου να αποκτηθούν παράνομες παροχές από μια ασφαλιστική εταιρεία. Τα ασφαλιστήρια συμβόλαια έχουν σχεδιαστεί για να προστατεύουν άτομα ή οργανισμούς από οικονομικούς κινδύνους. Ωστόσο, οι δόλιες αξιώσεις μπορούν να οδηγήσουν σε σημαντικές οικονομικές απώλειες για τις ασφαλιστικές εταιρείες και να επηρεάσουν τελικά τους καταναλωτές μέσω υψηλότερων ασφαλίστρων [68].

Οι δόλιες ασφαλιστικές απαιτήσεις είναι διαδεδομένες σε διάφορους τομείς, με την υγειονομική περίθαλψη και την ασφάλιση αυτοκινήτων να είναι οι κυριότεροι. Στον κλάδο της υγειονομικής περίθαλψης, η απάτη μπορεί να περιλαμβάνει την τιμολόγηση υπηρεσιών που δεν παρασχέθηκαν, τη διόγκωση των ιατρικών δαπανών ή την παροχή περιττών θεραπειών ή διαδικασιών [69]. Η απάτη στην ασφάλιση αυτοκινήτων μπορεί να περιλαμβάνει σκηνοθετημένα ατυχήματα, ψευδείς αξιώσεις για ζημιές ή τραυματισμούς του οχήματος ή υπερβολικές απώλειες [70]. Επιπλέον υπάρχουν οι ασφαλιστικές απάτες μεγαλύτερης κλίμακας, όπως η απάτη στην ασφάλιση καλλιεργειών, όπου ο ασφαλισμένος αγρότης δηλώνει ψευδως υπερβολικές απώλειες λόγω της μείωσης των γεωργικών τιμών ή των επιπτώσεων των φυσικών καταστροφών. Η ασφαλιστική απάτη μπορεί επίσης να περιλαμβάνει υπερβολική τιμολόγηση, διπλές απαιτήσεις, μίζες σε μεσίτες και αλλοίωση στοιχείων [57].

Ο οικονομικός αντίκτυπος της ασφαλιστικής απάτης είναι σημαντικός. Υπολογίζεται ότι η ασφαλιστική απάτη κοστίζει στις Ηνωμένες Πολιτείες πάνω από 300 δισεκατομμύρια δολάρια ετησίως [71]. Το κόστος αυτό μετακυλίεται τελικά στους καταναλωτές με τη μορφή υψηλότερων ασφαλίστρων, καθώς οι ασφαλιστικές εταιρείες προσπαθούν να μετριάσουν τις απώλειές τους.

4.2.5 Απάτη με ενυπόθηκα δάνεια

Η απάτη με υποθήκες/δάνεια είναι μια ειδική μορφή οικονομικής απάτης που αναφέρεται στη χειραγώγηση ενός ακινήτου ή εγγράφων υποθήκης/δανείου. Συχνά διαπράττεται για να παραποιηθεί η αξία ενός ακινήτου με σκοπό να επηρεάσει έναν δανειστή να χρηματοδοτήσει κάποιο δάνειο που έχει να κάνει με το ακίνητο. Ως υποθήκη νοείται η ουσιώδης ψευδής δήλωση του οφειλέτη σε οποιοδήποτε στάδιο της διαδικασίας υποβολής αίτησης, όταν ο ανάδοχος βασίζεται στα γεγονότα αυτά για να λάβει δάνειο ή πίστωση [57]. Στοχεύει σκόπιμα σε έγγραφα που σχετίζονται με μια υποθήκη τροποποιώντας τις πληροφορίες κατά τη διάρκεια των διαδικασιών υποβολής αίτησης για ενυπόθηκο δάνειο [58].

4.2.6 Απάτη στον κυβερνοχώρο

Η οικονομική απάτη στον κυβερνοχώρο είναι ένας όρος που περιλαμβάνει διάφορες εγκληματικές δραστηριότητες που διεξάγονται στον κυβερνοχώρο (cyberspace) με σκοπό το παράνομο οικονομικό κέρδος. Οι δράστες της οικονομικής κυβερνοαπάτης αποκρύπτουν σκόπιμα τις ενέργειές τους για να αναμειχθούν με την κανονική συμπεριφορά των χρηστών, καθιστώντας δύσκολο τον εντοπισμό τους. Ωστόσο, όταν οι δραστηριότητές τους αναλύονται συλλογικά, η ανωμαλία τους γίνεται πιο εμφανής [72]. Καθώς οι απατεώνες αποκτούν πρόσβαση σε προηγμένη τεχνολογία και τεχνικές δεξιότητες, η καταπολέμηση των τακτικών τους γίνεται όλο και πιο δύσκολη. Η σύγκλιση του οικονομικού

εγκλήματος και της ασφάλειας στον κυβερνοχώρο έχει ωθήσει τα χρηματοπιστωτικά ιδρύματα να αναπτύξουν εσωτερικές μεθόδους και εργαλεία, όπως η ανάλυση σε πραγματικό χρόνο (real-time analytics), για να προστατεύσουν τα περιουσιακά τους στοιχεία και να αποτρέψουν τις οικονομικές απώλειες [73].

Ωστόσο, τα παραδοσιακά μοντέλα και οι προσεγγίσεις παρουσιάζουν περιορισμούς στην αποτελεσματική πρόληψη και αντιμετώπιση αυτών των επιθέσεων. Ως εκ τούτου, νέες μέθοδοι αναπτύσσονται και εφαρμόζονται σε όλους τους οργανισμούς για τον μετριασμό περαιτέρω απωλειών των επιχειρήσεων, στα δεδομένα των πελατών και στη φήμη τους. Μια τέτοια προσέγγιση είναι η χρήση μοντέλων μηχανικής μάθησης και βαθιάς μάθησης, τα οποία αξιοποιούν τεχνικές τεχνητής νοημοσύνης για την ανάλυση τεράστιου όγκου δεδομένων, την ανίχνευση μοτίβων και τον εντοπισμό πιθανών απειλών ή δόλιων δραστηριοτήτων. Με την ανάπτυξη αυτών των προηγμένων μοντέλων, οι οργανισμοί μπορούν να βελτιώσουν την ικανότητά τους να ανιχνεύουν και να αποτρέπουν την οικονομική απάτη στον κυβερνοχώρο, ενισχύοντας έτσι την άμυνά τους και προστατεύοντας τα περιουσιακά τους στοιχεία και τα ενδιαφερόμενα μέρη από πιθανή ζημία [74].

4.2.7 Ξέπλυμα βρώμικου χρήματος

Η νομιμοποίηση εσόδων από παράνομες δραστηριότητες είναι μια διαδικασία που χρησιμοποιείται για απόκρυψη ή συγκάλυψη της προέλευσης παράνομων αποκτηθέντων κεφαλαίων ή περιουσιακών στοιχείων με στόχο να φανούν νόμιμα. Ο πρωταρχικός σκοπός της νομιμοποίησης εσόδων από παράνομες δραστηριότητες είναι η ενσωμάτωση των εσόδων από εγκληματικές δραστηριότητες στη νόμιμη οικονομία, επιτρέποντας στους εγκληματίες να απολαμβάνουν τα οφέλη των παράνομων κερδών τους χωρίς να προκαλούν υποψίες. Οι εγκληματίες εμπλέκονται στο ξέπλυμα χρήματος για να διασπάσουν τη σύνδεση μεταξύ των παράνομων δραστηριοτήτων που δημιούργησαν τα κεφάλαια και της πραγματικής τους πηγής. Με τον τρόπο αυτό, μπορούν να αποφύγουν τον εντοπισμό, τη δίωξη και τη δήμευση των παράνομων κερδών τους. Η νομιμοποίηση εσόδων από παράνομες δραστηριότητες περιλαμβάνει διάφορες πολύπλοκες συναλλαγές και τεχνικές για να κάνουν τα παράνομα κεφάλαια να φαίνονται νόμιμα, συχνά με τη συμμετοχή πολλών επιπέδων συναλλαγών και οντοτήτων [57].

4.3 Σχετικές εφαρμογές

Στην παρούσα ενότητα παρουσιάζουμε ορισμένες εργασίες που σχετίζονται με την εφαρμογή τεχνικών τεχνητής νοημοσύνης, μηχανικής μάθησης και τεχνητών ανοσοποιητικών συστημάτων στον τομέα της ανίχνευσης χρηματοοικονομικής απάτης. Αυτές οι εργασίες αποτελούν την πηγή έμπνευσης για την δημιουργία του δικού μας μοντέλου ΤΑΣ, για την εύρεση απάτης σε χρηματοοικονομικά δεδομένα.

4.3.1 Ανίχνευση απάτης πιστωτικών καρτών

Το 2008 οι Gadi, Wang και do Lago [75] παρουσίασαν μια μελέτη που συγκρίνει διάφορες μεθόδους ανίχνευσης απάτης με πιστωτικές κάρτες, συμπεριλαμβανομένων των νευρωνικών δικτύων, των Bayesian δικτύων και των Naïve Bayes δικτύων, καθώς και των δέντρων αποφάσεων και ενός συστήματος τεχνητής ανοσολογικής αναγνώρισης - Artificial Immune Recognition System (AIRS). Η βάση δεδομένων που χρησιμοποίησαν προέρχεται από μια μεγάλη τράπεζα στην Βραζιλία και καλύπτει συναλλαγές από τις 14 Ιουλίου 2004 έως τις 12 Σεπτεμβρίου 2004. Περιέχει 41.647 μητρώα, εκ των οποίων το 3,74% υποδηλώνουν ύποπτη δραστηριότητα. Σε αυτή την μελέτη, οι

παράμετροι των μεθόδων βελτιστοποιούνται με εξαντλητική αναζήτηση (exhaustive search) και γενετικό αλγόριθμο. Πιο συγκεκριμένα, οι παράμετροι των νευρωνικών δικτύων και του AIRS βελτιστοποιούνται με έναν γενετικό αλγόριθμο, ενώ οι άλλες μέθοδοι χρησιμοποιούν εξαντλητική αναζήτηση για να διερευνηθούν όλοι οι πιθανοί συνδυασμοί παραμέτρων και να βρεθεί το βέλτιστο σύνολο. Ο γενετικός αλγόριθμος ξεκινά με μια αρχική δεξαμενή 50 τυχαίων εκτελέσεων, ακολουθούμενη από 20 γενιές. Κάθε γενιά συνδυάζει δύο τυχαία επιλεγμένους υποψηφίους από τους 15 καλύτερους της προηγούμενης γενιάς. Τα αποτελέσματα δείχνουν ότι μετά τη βελτιστοποίηση των παραμέτρων του AIRS, ο αλγόριθμος αυτός παρουσιάζει το μικρότερο κόστος και την υψηλότερη ακρίβεια μεταξύ των συγκρινόμενων μεθόδων. Τα ευρήματα αυτά υπογραμμίζουν ότι τα ΤΑΣ θα μπορούσαν να αποτελέσουν μια βιώσιμη επιλογή για την ανίχνευση απάτης με πιστωτικές κάρτες, ιδίως όταν ληφθούν υπόψη ειδικές προκλήσεις όπως η ασυμμετρία των δεδομένων και τα διαφορετικά κόστη που σχετίζονται με τα ψευδώς θετικά και αρνητικά αποτελέσματα.

Το 2009 οι Kundu, Panigrahi, Sural, Majumdar [76] παρουσίασαν μια συμπεριφορική μέθοδο (behavior-based method) για την ανίχνευση απάτης με πιστωτικές κάρτες, εμπνευσμένη από τη βιοπληροφορική. Στην εργασία τους προτείνουν μια μέθοδο ευθυγράμμισης ακολουθιών (sequence alignment) σε δύο στάδια. Ο αλγόριθμος που δημιουργούν συνδυάζει τα πλεονεκτήματα δύο γνωστών αλγορίθμων ευθυγράμμισης ακολουθιών, του BLAST (Basic Local Alignment Search Tool) και του SSAHA (Sequence Search and Alignment by Hashing Algorithm). Το πρώτο στάδιο περιλαμβάνει έναν αναλυτή προφίλ (profile analyzer) που αξιολογεί την ομοιότητα μεταξύ μιας εισερχόμενης ακολουθίας συναλλαγών και των προηγούμενων ακολουθιών δαπανών του γνήσιου κατόχου κάρτας. Αυτό γίνεται με τη χρήση τεχνικών ευθυγράμμισης ακολουθιών. Το δεύτερο στάδιο περιλαμβάνει έναν αναλυτή αποκλίσεων (deviation analyzer), ο οποίος λαμβάνει τις ασυνήθιστες συναλλαγές που εντοπίζονται από τον αναλυτή προφίλ και τις ευθυγραμμίζει με την προηγούμενη δόλια συμπεριφορά για να διαπιστώσει αν είναι πράγματι δόλιες. Στόχος των συγγραφέων είναι να συνδυάσουν τις τεχνικές ανίχνευσης ανωμαλιών και ανίχνευσης κατάχρησης για να βελτιώσουν την ακρίβεια και την ταχύτητα των συστημάτων ανίχνευσης απάτης. Μετρώντας την ομοιότητα μεταξύ δύο συναλλαγών και αναλύοντας την κάθε συναλλαγή, καταφέρνουν με τον αλγόριθμό τους να εντοπίσουν αποκλίσεις από την κανονική συμπεριφορά κάτι που υποδηλώνει απάτη. Το προτεινόμενο σύστημα βασίζεται στη διάσταση του χρόνου-ποσού, προσφέροντας μια πιο ολοκληρωμένη προσέγγιση για την ανάλυση της συμπεριφοράς δαπανών και τη βελτίωση της αποτελεσματικότητας των μοντέλων ανίχνευσης απάτης. Ο αλγόριθμος στοχεύει σε υψηλά αληθώς θετικά αποτελέσματα (σωστά αναγνωρισμένες δόλιες συναλλαγές) και χαμηλά ψευδώς θετικά αποτελέσματα (νόμιμες συναλλαγές που εσφαλμένα χαρακτηρίζονται ως δόλιες). Στο τέλος αναφέρουν ότι ο αλγόριθμος BLAH αποδίδει έως και 86% αληθή θετικά αποτελέσματα και λιγότερο από 10% ψευδώς θετικά αποτελέσματα. Αντιμετωπίζει όμως ορισμένους περιορισμούς των συμπεριφορικών μεθόδων και ενδέχεται να εξακολουθεί να αντιμετωπίζει προκλήσεις όσον αφορά την κάλυψη όλων των πιθανών κανονικών σεναρίων. Επίσης απαιτείται περαιτέρω έρευνα και αξιολόγηση των επιδόσεων του αλγορίθμου σε σενάρια πραγματικού χρόνου για να εκτιμηθεί η αποτελεσματικότητά του σε πρακτικές εφαρμογές.

Στη μελέτη των Brabazon, Cahill, Keenan, Walsh [77] που εκδόθηκε το 2010, καταδεικνύεται η αποτελεσματικότητα των ΤΑΣ στον εντοπισμό απάτης με πιστωτικές κάρτες σε διαδικτυακές συναλλαγές. Η μελέτη διεξάγεται πάνω σε ένα μεγάλο σύνολο δεδομένων που λαμβάνεται από έναν διαδικτυακό λιανοπωλητή με την επωνυμία WebBiz. Περιλαμβάνει 4 εκατομμύρια συναλλαγές από 462.279 μοναδικούς πελάτες, με 5.417 συναλλαγές να έχουν χαρακτηριστεί ως δόλιες. Εφαρμόζονται τρεις αλγόριθμοι ΤΑΣ και συγκρίνονται με ένα μοντέλο λογιστικής παλινδρόμησης. Ο πρώτος αλγόριθμος είναι ένας μη τροποποιημένος αλγόριθμος αρνητικής επιλογής - Unmodified Negative

Selection Algorithm (UNSA). Λειτουργεί με την τυχαία δημιουργία ανιχνευτών που αντιπροσωπεύουν συναλλαγές και τον υπολογισμό των αποστάσεων μεταξύ αυτών των ανιχνευτών και ενός συνόλου δειγμάτων "εαυτού" (δηλαδή νόμιμων συναλλαγών). Εάν ο μέσος όρος ενός προκαθορισμένου αριθμού μικρότερων αποστάσεων είναι μικρότερος από μια ορισμένη ακτίνα ανίχνευσης, ο ανιχνευτής αντικαθίσταται από έναν νέο τυχαία παραγόμενο. Διαφορετικά, ο ανιχνευτής προστίθεται στο σύνολο ανιχνευτών. Η διαδικασία επαναλαμβάνεται έως ότου το σύνολο ανιχνευτών είναι πλήρες. Ο δεύτερος αλγόριθμος είναι ένας τροποποιημένος αλγόριθμος αρνητικής επιλογής - Modified Negative Selection Algorithm (MNSA), παρόμοιος με τον UNSA, αλλά περιλαμβάνει μια μεταβλητή "ηλικία" για κάθε ανιχνευτή. Η μεταβλητή αυτή χρησιμεύει ουσιαστικά ως μηχανισμός ενημέρωσης και τελικά απόρριψης των ανιχνευτών που δεν είναι πλέον αποτελεσματικοί στον εντοπισμό ανωμαλιών ή πιθανών δόλιων συναλλαγών. Εάν ο μέσος όρος των μικρότερων αποστάσεων ενός ανιχνευτή είναι μικρότερος από την ακτίνα ανίχνευσης, ο ανιχνευτής μετακινείται. Ο τρίτος αλγόριθμος είναι ένας τυπικός αλγόριθμος κλωνικής επιλογής. Αυτοί οι αλγόριθμοι συγκρίθηκαν με ένα μοντέλο λογιστικής παλινδρόμησης για να αξιολογηθεί η αποτελεσματικότητά τους στον εντοπισμό δόλιων συναλλαγών. Τα αποτελέσματα υποδηλώνουν ότι οι αλγόριθμοι ΤΑΣ, συγκεκριμένα οι δύο αλγόριθμοι αρνητικής επιλογής, μπορούν να εντοπίσουν ύποπτες συναλλαγές χωρίς προηγούμενη έκθεση σε όλα τα πιθανά μοτίβα απάτης κατά την εκπαίδευση. Σε σύγκριση όμως με το μοντέλο λογιστικής παλινδρόμησης, οι αλγόριθμοι ΤΑΣ αποδείχτηκαν κατώτεροι. Η λογιστική παλινδρόμηση ταξινόμησε με ακρίβεια το 99,632% των συναλλαγών, αλλά ταξινόμησε εσφαλμένα το 85,167% των δόλιων συναλλαγών.

Την ίδια χρονιά το υβριδικό μοντέλο του Krivko [78] αποσκοπεί στην αντιμετώπιση των περιορισμών τόσο των εποπτευόμενων όσο και των μη εποπτευόμενων μεθοδολογιών, συνδυάζοντας ένα συμπεριφορικό μοντέλο με ένα σύστημα βασισμένο σε κανόνες (rule based system). Το σύνολο δεδομένων που χρησιμοποιεί αποτελείται από περίπου 189 εκατομμύρια συναλλαγές που πραγματοποιήθηκαν μεταξύ 1 Οκτωβρίου 2007 και 30 Απριλίου 2008. Το υβριδικό μοντέλο συνδυάζει την ταξινόμηση μιας κατηγορίας (one-class classification) και τις προσεγγίσεις που βασίζονται σε κανόνες. Το μοντέλο αυτό λειτουργεί σε δύο επίπεδα. Στο πρώτο επίπεδο παρακολουθείται κάθε απόκλιση από το μοντέλο λογαριασμού της συγκεντρωτικής συμπεριφοράς δαπανών σε ένα χρονικό παράθυρο και αποδίδεται μια βαθμολογία ανάλογα με το επίπεδο υποψίας απάτης. Στο δεύτερο επίπεδο, οι συναλλαγές που βαθμολογούνται πάνω από ένα καθορισμένο όριο διαβιβάζονται για περαιτέρω βελτίωση σε φίλτρα βασισμένα σε κανόνες. Μια περίπτωση που παραβιάζει οποιονδήποτε από τους κανόνες επισημαίνεται ως ύποπτη για απάτη. Οι λογαριασμοί διαχωρίζονται σε διάφορες ομάδες συμπεριφοράς και ένα μοντέλο προσαρμόζεται σε κάθε ομάδα αντί να χειρίζεται κάθε λογαριασμό ξεχωριστά. Αυτό μειώνει τον αριθμό των παραμέτρων, ενώ εξακολουθεί να ταιριάζει αποτελεσματικά τη συμπεριφορά του λογαριασμού με τα μοντέλα. Τέλος το μοντέλο αποδίδει μια βαθμολογία ύποπτου σε κάθε λογαριασμό, επιτρέποντας την άμεση αντίδραση και την ανίχνευση απάτης. Η προσέγγιση αυτή παρουσιάζει πολλά υποσχόμενα αποτελέσματα, αλλά μπορεί να είναι πολύπλοκη και χρονοβόρα.

Το 2011, στην μελέτη τους, οι Bhattacharyya, Jha, Tharakunnel και Westland [79], εξετάζουν την αποτελεσματικότητα δύο προηγμένων τεχνικών εξόρυξης δεδομένων, των μηχανών διανυσμάτων υποστήριξης - Support Vector Machines (SVM) και των τυχαίων δασών - random forests, μαζί με τη λογιστική παλινδρόμηση, για την ανίχνευση και τον έλεγχο απάτης με πιστωτικές κάρτες. Η μελέτη βασίζεται σε πραγματικά δεδομένα από μια διεθνή επιχείρηση πιστωτικών καρτών. Η έρευνα αξιολογεί διάφορες τεχνικές δειγματοληψίας και μέτρα απόδοσης, με στόχο τη βελτίωση των μεθόδων ανίχνευσης απάτης ενόψει των εξελισσόμενων πρακτικών απάτης. Τα ευρήματα δείχνουν ότι τα

τυχαία δάση επέδειξαν συνολικά καλύτερες επιδόσεις σε διάφορα μέτρα απόδοσης έναντι άλλων τεχνικών. Διαπιστώθηκε ότι είναι υπολογιστικά αποδοτικά και κατέγραψαν περισσότερες περιπτώσεις απάτης με λιγότερα ψευδώς θετικά αποτελέσματα. Οι συγγραφείς στο τέλος τονίζουν την ανάγκη περαιτέρω έρευνας για τη βελτίωση της αποτελεσματικότητας των τεχνικών εξόρυξης δεδομένων στην ανίχνευση απάτης με πιστωτικές κάρτες.

Το 2012, οι Wong, Ray, Stephens και Lewis, πρότειναν στην μελέτη τους [80] μια αρχιτεκτονική συστήματος ανίχνευσης απάτης σε πιστωτικές κάρτες με βάση την αρνητική επιλογή και τον εμβολιασμό. Το σύνολο δεδομένων που χρησιμοποιήθηκε ελήφθη από μια μεγάλη αυστραλιανή τράπεζα. Τα δεδομένα αποτελούνταν από 640.361 συνολικές συναλλαγές που αφορούσαν 21.746 πιστωτικές κάρτες. Οι ανιχνευτές δημιουργούνται με τη χρήση δόλιων εγγραφών και υποβάλλονται σε μετάλλαξη. Ύστερα υπολογίζεται η απόσταση μεταξύ των μεταλλαγμένων κυττάρων και των δόλιων εγγραφών και, εάν υπερβαίνει ένα κατώτατο όριο, ενεργοποιείται η αρνητική επιλογή. Το ΤΑΣ που παρουσιάζεται σε αυτό το κείμενο αποτελεί μια πολλά υποσχόμενη λύση συνδυάζοντας τα πλεονεκτήματα των συστημάτων που βασίζονται σε κανόνες και των νευρωνικών δικτύων. Οι προτεινόμενοι μηχανισμοί, όπως η διαδικασία εμβολιασμού και η διαδικασία εξέλιξης των κυττάρων μνήμης, βελτιώνουν σημαντικά τις επιδόσεις του συστήματος και θα μπορούσαν ενδεχομένως να εφαρμοστούν σε άλλους προβληματικούς τομείς, όπως η διαχείριση της απάτης στην ασφάλιση υγείας και η εισβολή σε δίκτυο.

Στην μελέτη που εκδώσαν το 2014 οι Halvaiee και Akbari [81] ασχολήθηκαν επίσης με το αυξανόμενο ζήτημα της απάτης με πιστωτικές κάρτες στις ηλεκτρονικές συναλλαγές και πρότειναν ένα νέο μοντέλο που ονόμασαν AIS-based Fraud Detection Model (AFDM) και χρησιμοποιεί ΤΑΣ. Η μελέτη επικεντρώνεται στη βελτίωση της ακρίβειας, τη μείωση του κόστους και την ενίσχυση του χρόνου απόκρισης του συστήματος σε σύγκριση με τους υπάρχοντες αλγορίθμους. Οι συγγραφείς χρησιμοποιούν έναν αλγόριθμο AIRS και υλοποιούν το σύστημα ανίχνευσης απάτης σε ένα σύστημα αρχείων που βασίζεται σε νέφος (Hadoop) για παράλληλη επεξεργασία μεγάλων συνόλων δεδομένων. Στο τέλος, κατάφεραν να βελτιώσουν το ποσοστό ανίχνευσης έως και 23%, να μειώσουν το κόστος έως και 85% και τον χρόνο εκπαίδευσης έως και 40%.

4.3.2 Ανίχνευση εταιρικής απάτης

Το 2007, οι Hoogs, Bethany, Lacomb, Senturk [82] ανέδειξαν τις προκλήσεις της ανίχνευσης απάτης στις οικονομικές καταστάσεις και τους περιορισμούς των υφιστάμενων μοντέλων, όπως η λογιστική παλινδρόμηση και τα νευρωνικά δίκτυα. Εισήγαγαν μια προσέγγιση βασισμένη σε γενετικό αλγόριθμο για τον εντοπισμό ενδεικτικών μοτίβων απάτης σε οικονομικές καταστάσεις, χρησιμοποιώντας δημόσια διαθέσιμα δεδομένα. Ο αλγόριθμος χρησιμοποιεί ένα σύνολο 85 συγκριτικών μετρήσεων και εταιρικών χαρακτηριστικών, συμπεριλαμβανομένων συγκεκριμένων χρηματοοικονομικών μετρήσεων, δεικτών και ιστορικών δεικτών απόδοσης. Οι γενετικοί αλγόριθμοι είναι κατάλληλοι για την ανίχνευση απάτης επειδή μπορούν να χειριστούν μη γραμμικές σχέσεις μεταξύ πολλαπλών μεταβλητών και να εξερευνήσουν αποτελεσματικά μεγάλους χώρους αναζήτησης. Τα αποτελέσματα καταδεικνύουν ότι τα μοτίβα που παρήγαγε ο γενετικός αλγόριθμος ταξινόμησαν με ακρίβεια το 63% των εταιρειών της κατηγορίας-στόχου (που κατηγορούνται για απάτη) και το 95% των εταιρειών της κατηγορίας ομότιμων (που δεν είναι δόλιες) του δείγματος.

Η μελέτη των Humpherys, Moffitt, Burns, Burgoon και Felix που εκδόθηκε το 2011 [83], διερευνά τη στρατηγική χρήση παραπλανητικής γλώσσας στη διαχειριστική οικονομική απάτη (managerial financial fraud) αναλύοντας γλωσσικά στοιχεία που εξάγονται από δημόσια διαθέσιμες οικονομικές

καταστάσεις. Η μελέτη διαπίστωσε ότι οι δόλιες γνωστοποιήσεις παρουσιάζουν διακριτά μοτίβα, συμπεριλαμβανομένης επιπλέον γλώσσας ενεργοποίησης, ευχάριστης γλώσσας, ομαδικές αναφορές και λιγότερη λεξιλογική ποικιλομορφία σε σύγκριση με τις μη δόλιες γνωστοποιήσεις. Η έρευνα καταδεικνύει τις δυνατότητες της γλωσσικής ανάλυσης ως εργαλείο για τον εντοπισμό αμφισβητήσιμων οικονομικών γνωστοποιήσεων και την αξιολόγηση του κινδύνου απάτης. Οι συγγραφείς χρησιμοποιούν ένα σύνθετο μοντέλο που αναφέρεται ως "24-variable model" για τον εντοπισμό εταιρικής απάτης. Το μοντέλο αυτό κατασκευάστηκε με τη χρήση ενός συστήματος υποστήριξης αποφάσεων που ονομάζεται Agent99 Analyzer, το οποίο χρησιμοποιεί διάφορους αλγορίθμους ταξινόμησης μετά την εξαγωγή στοιχείων. Με γνώμονα τη θεωρητική κατανόηση και τη διερευνητική ανάλυση παραγόντων, το μοντέλο των 24 μεταβλητών μειώθηκε σε ένα μοντέλο 10 μεταβλητών. Αυτό το μειωμένο μοντέλο είχε ίση ή καλύτερη ακρίβεια στην ταξινόμηση. Δημιουργήθηκε επίσης ένα περαιτέρω απλουστευμένο μοντέλο τεσσάρων μεταβλητών και δοκιμάστηκε με τη χρήση λογιστικής παλινδρόμησης. Αυτό το μοντέλο επέδειξε επίσης καλή απόδοση. Τέλος, χρησιμοπιώντας το μοντέλο των 10 μεταβλητών σε συνδυασμό με ταξινομητές όπως οι Naive Bayes και C4.5 (αλγόριθμος δέντρων απόφασης) οι συγγραφείς πέτυχαν την μέγιστη ακρίβεια ταξινόμησης (67,3%), υποστηρίζοντας έτσι περαιτέρω την αποτελεσματικότητα των γλωσσικών αναλύσεων στην ανίχνευση απάτης. Τα ευρήματα υπογραμμίζουν την ανάγκη για πιο αξιόπιστες μεθόδους εντοπισμού της απάτης στις οικονομικές καταστάσεις, ιδίως μέσω της εξέτασης των γλωσσικών χαρακτηριστικών.

Την ίδια χρονιά, οι Pediredla, Ravi, Rao, Bose στην μελέτη που δημοσίευσαν [64], παρουσίασαν μια μεθοδολογία για τον εντοπισμό απάτης στις οικονομικές καταστάσεις κινεζικών εταιρειών με τη χρήση τεχνικών εξόρυξης δεδομένων. Το σύνολο δεδομένων που χρησιμοποιήθηκε αποτελείται από χρηματοοικονομικές πληροφορίες 202 εταιρειών εισηγμένων σε κινεζικά χρηματιστήρια, με 101 δόλιες και 101 μη δόλιες εταιρείες. Περιλαμβάνει 35 χρηματοοικονομικούς δείκτες που αντικατοπτρίζουν τη ρευστότητα, την ασφάλεια, την αποδοτικότητα και την αποτελεσματικότητα. Οι συγγραφείς πραγματοποίησαν μετασχηματισμό και κανονικοποίηση του συνόλου δεδομένων ως μέρος του σταδίου προεπεξεργασίας των δεδομένων. Εφάρμοσαν 10-fold διασταυρούμενη επικύρωση (10-fold cross validation) για να βελτιώσουν την αξιοπιστία των αποτελεσμάτων. Οι τεχνικές εξόρυξης δεδομένων που χρησιμοποιήθηκαν στην ανάλυση ήταν τα νευρωνικά δίκτυα τροφοδότησης πολλαπλών στρωμάτων - Multilayer Feedforward Neural Network (MLFF), οι μηχανές διανυσμάτων υποστήριξης, ο γενετικός αλγόριθμος, η ομαδική μέθοδος χειρισμού δεδομένων - Group Method of Data Handling (GMDH), η λογιστική παλινδρόμηση και τα πιθανοτικά νευρωνικά δίκτυα - Probabilistic Neural Network (PNN). Η μελέτη κατέληξε στο συμπέρασμα ότι το PNN χωρίς επιλογή χαρακτηριστικών υπερείχε έναντι άλλων τεχνικών, ενώ ο γενετικός αλγόριθμος είχε καλή απόδοση μετά την επιλογή χαρακτηριστικών.

4.3.3 Ανίχνευση ασφαλιστικής απάτης

Το 2012, οι Kirlidog και Asuk, στην μελέτη τους [84] εξετάζουν τη χρήση τεχνικών εξόρυξης δεδομένων, και συγκεκριμένα την ανάλυση ανίχνευσης ανωμαλιών, για την ανίχνευση απάτης σε μια ασφαλιστική εταιρεία. Οι συγγραφείς χρησιμοποιούν τη βάση δεδομένων μιας τουρκικής ασφαλιστικής εταιρείας, η οποία περιέχει λεπτομερή αρχεία αποζημιώσεων καθώς και άλλες απαραίτητες πληροφορίες, όπως οι επιχειρηματικοί εταίροι και οι πελάτες. Η βάση δεδομένων περιέχει 808.348 εγγραφές με χρονικό εύρος από το 2001 έως το 2009. Με τη χρήση αλγόριθμου SVM κατηγοριοποιούν μεμονωμένες εγγραφές ως κανονικές ή ανώμαλες. Ο αλγόριθμος καθορίζει ένα όριο που διαχωρίζει τις κανονικές και τις ανώμαλες εγγραφές και κάθε εγγραφή συγκρίνεται με

αυτό το όριο για να καθοριστεί η ταξινόμησή της. Τα αποτελέσματα καταδεικνύουν την αποτελεσματικότητα της εξόρυξης δεδομένων στην ανίχνευση πιθανής απάτης σε ασφαλιστικές απαιτήσεις υγείας. Τονίζεται επίσης η ανάγκη να εκπαιδευτούν οι ασφαλιστικοί εμπειρογνώμονες στην αποτελεσματική χρήση αυτής της τεχνολογίας.

Η έρευνα των Peng, You [85] που εκδόθηκε το 2016, προτείνει έναν βελτιωμένο αλγόριθμο νευρωνικού δικτύου για την ανίχνευση απάτης στην ιατρική ασφάλιση. Η μέθοδος συνδυάζει ένα πολυστρωματικό νευρωνικό δίκτυο Perceptron – Multilayer Perceptron (MLP) με ένα νευρωνικό δίκτυο που βασίζεται στην διαδικασία της αναλυτικής ιεράρχησης - Analytic Contribution Hierarchy Process (ACHP) και πραγματοποιεί βελτιώσεις με βάση τα χαρακτηριστικά της απάτης στην ιατρική ασφάλιση. Οι συγγραφείς επιλέγουν τις πιο συχνές εγγραφές από μια βάση δεδομένων ιατρικών αρχείων μιας πόλης στην επαρχία Σαντόνγκ της Κίνας. Η βάση δεδομένων περιέχει περιπτώσεις απάτης ασφάλισης ιατρικής περίθαλψης που διερευνήθηκαν σε 15 περιοχές. Ένα δέντρο φάσματος φαρμακοποιίας - Pharmacopoeia Spectrum Tree (PST) χρησιμοποιείται για την ομαδοποίηση παρόμοιων ιατρικών αντικειμένων με βάση ορισμένα χαρακτηριστικά ή ιδιότητες. Αυτή η ομαδοποίηση βοηθά στον εντοπισμό μοτίβων ή ανωμαλιών που θα μπορούσαν να υποδηλώνουν ύποπτη συμπεριφορά. Ο αλγόριθμος υπολογίζει το ποσοστό συμβολής των παραγόντων ανίχνευσης απάτης στα ιατρικά αντικείμενα για κάθε περίπτωση, χρησιμοποιώντας το ποσοστό συμβολής ιεραρχίας και την πολυδιάστατη απόσταση χώρου. Με την ανάλυση των συστάδων, το PST βοηθά στον προσδιορισμό των παραγόντων που είναι πιο σημαντικοί για την ανίχνευση της απάτης. Αυτοί οι παράγοντες χρησιμοποιούνται στη συνέχεια στο μοντέλο νευρωνικού δικτύου για μεγαλύτερη ακρίβεια στην ανίχνευση απάτης. Τα πειραματικά αποτελέσματα δείχνουν ότι η ακρίβεια του βελτιωμένου νευρωνικού δικτύου στην ανίχνευση απάτης έφτασε το 86%, ξεπερνώντας άλλες μεθόδους εξόρυξης δεδομένων χωρίς επίβλεψη. Επιπλέον, η μέθοδος μπορεί να υπολογίσει το ποσοστό συμβολής κάθε παράγοντα ανίχνευσης απάτης, το οποίο αποτελεί μοναδικό χαρακτηριστικό σε σύγκριση με άλλες μεθόδους εξόρυξης δεδομένων. Ωστόσο, υπάρχουν περιθώρια βελτίωσης όσον αφορά τη διερεύνηση διαφορετικών αρχιτεκτονικών νευρωνικών δικτύων και την εξεύρεση πιο ισχυρών μεθόδων για την αξιολόγηση της δυνατότητας κάθε παράγοντα εισόδου στην ανίχνευση απάτης.

Η έρευνα των Aslam, Hunjra, Ftiti, Louhichi, Shams, που εκδόθηκε το 2022 [86] επικεντρώνεται στην ανίχνευση της απάτης στην ασφάλιση αυτοκινήτων, η οποία αποτελεί σημαντικό ζήτημα στον ασφαλιστικό κλάδο. Η μελέτη παρουσιάζει ένα προγνωστικό μοντέλο για την ανίχνευση απάτης χρησιμοποιώντας μια μέθοδο επιλογής χαρακτηριστικών που βασίζεται στα τυχαία δάση. Στη συνέχεια, παρουσιάζει τρία μοντέλα μηχανικής μάθησης - λογιστική παλινδρόμηση, SVM και Naive Bayes - και αξιολογεί την απόδοσή τους χρησιμοποιώντας μετρικές αξιολόγησης όπως η ακρίβεια, η ανάκληση, η ορθότητα και το F1-Score. Συνολικά, όλα τα μοντέλα σημείωσαν καλή βαθμολογία όσον αφορά την ακρίβεια αλλά ο SVM έχει ισχυρότερες δυνατότητες πρόβλεψης.

4.3.4 Ανίχνευση απάτης στον κυβερνοχώρο

Το 2010 οι Huang, Tawfik, Nagar δημοσίευσαν μια μελέτη [87] που επικεντρώνεται στην ανίχνευση της διαδικτυακής απάτης σε συστήματα Video-on-Demand. Το προτεινόμενο υβριδικό μοντέλο συνδυάζει δύο αλγορίθμους ΤΑΣ με μεθόδους που βασίζονται στη συμπεριφορά για την ανίχνευση εισβολής με τη χρήση δέντρων ταξινόμησης και παλινδρόμησης - Classification and Regression Trees (CART). Οι συγγραφείς χρησιμοποιούν συνθετικά δεδομένα που δημιουργήθηκαν για 7 μήνες και περιέχουν 600 κανονικούς χρήστες και 100 “εισβολείς”. Τα δεδομένα περιλαμβάνουν διάφορα γεγονότα όπως αποτυχημένες προσπάθειες σύνδεσης, επιτυχημένες παραγγελίες ταινιών κ.λπ. Ο ένας

αλγόριθμος, που είναι εμπνευσμένος από ένα βιολογικό μοντέλο αναγνώρισης προτύπων, ονομάζεται CSPRA (Conserved Self Pattern Recognition Algorithm) και έχει δύο φάσεις: μια φάση εκμάθησης όπου κατανοεί τη συμπεριφορά των κανονικών χρηστών και μια φάση ανίχνευσης όπου χρησιμοποιεί ανιχνευτές για να ταξινομήσει τα νέα δεδομένα ως κανονικά ή ανώμαλα. Ο άλλος αλγόριθμος, είναι ένας DCA που συσχετίζει διαφορετικές ροές δεδομένων με τη μορφή αντιγόνων και σημάτων και χαρακτηρίζει ομάδες πανομοιότυπων αντιγόνων ως φυσιολογικές ή ανώμαλες. Έχει τέσσερις κύριες φάσεις: Αρχικοποίηση, δειγματοληψία, ωρίμανση και φάση αποτελεσμάτων. Τα πειραματικά αποτελέσματα καταδεικνύουν ότι η υβριδική μέθοδος υπερτερεί των μεμονωμένων αλγορίθμων όσον αφορά το ποσοστό ανίχνευσης, τους ψευδείς συναγερμούς και τον χειρισμό συνόλων δεδομένων υψηλής διάστασης. Το μοντέλο αποσκοπεί στη βελτίωση του τρέχοντος αγωγού διαχείρισης κινδύνου - Risk Management Pipeline (RMP) με την αξιοποίηση των ΤΑΣ για την ανίχνευση απάτης μέσω δεδομένων καταγραφής.

Το 2016 οι Monamo, Marivate και Twala [88] πρότειναν μια πολύπλευρη προσέγγιση για την κατανόηση της απάτης Bitcoin από παγκόσμιες και τοπικές προοπτικές. Χρησιμοποίησαν τεχνικές ομαδοποίησης k-μέσων, kd-δέντρων, τυχαία δάση και μοντέλα δυαδικής παλινδρόμησης. Η μελέτη χρησιμοποιεί δεδομένα συναλλαγών από το δίκτυο Bitcoin και κατηγοριοποιεί τις περιπτώσεις ως απάτη ή μη απάτη με βάση προκαθορισμένες αναλογίες. Το σύνολο δεδομένων αναλύεται με τη χρήση kd-δέντρων και trimmed k-means για τον εντοπισμό της κανονικής έναντι της ανώμαλης δραστηριότητας. Τα αποτελέσματα υποδηλώνουν ότι τόσο οι παγκόσμιες όσο και οι τοπικές προοπτικές παρουσιάζουν καλές επιδόσεις στον εντοπισμό απάτης Bitcoin, με εξαίρεση τα τυχαία δάση, τα οποία παρουσιάζουν σχεδόν τέλεια αποτελέσματα και στις δύο διαστάσεις. Αυτό δείχνει ότι τα χαρακτηριστικά που εξάγονται για τη μελέτη παρέχουν μια ολοκληρωμένη περιγραφή του δικτύου Bitcoin. Η μεθοδολογία περιλαμβάνει την επισήμανση των καθολικών ακραίων τιμών (global outliers) με βάση τις αποστάσεις από τα κεντροειδή (centroids) και την επισήμανση των τοπικών ακραίων τιμών (local outliers) με βάση τις αποστάσεις από τους πλησιέστερους γείτονες.

4.3.5 Ανίχνευση ξεπλύματος βρώμικου χρήματος

Το 2006, οι Gao, Xu, Wang [89] εξέτασαν την εφαρμογή της τεχνολογίας των ευφυών πρακτόρων στον τομέα της καταπολέμησης του ξεπλύματος χρήματος - Anti-Money Laundering (AML) για να ξεπεραστούν οι περιορισμοί των παραδοσιακών λύσεων που βασίζονται σε κανόνες. Η εργασία υπογραμμίζει την ανάγκη για αποτελεσματικά συστήματα AML και παρουσιάζει ένα ευφυές σύστημα AML με βάση πράκτορες - Intelligent Agent-based AML System (IAMLS) που μπορεί να παρακολουθεί τις χρηματοοικονομικές συναλλαγές, να εντοπίζει ασυνήθιστη συμπεριφορά και να διαχωρίζει τις συναλλαγές που αποτελούν κίνδυνο για τα χρηματοπιστωτικά ιδρύματα. Το IAMLS είναι ικανό να μαθαίνει και να προσαρμόζεται σε νέα σχήματα νομιμοποίησης εσόδων από παράνομες δραστηριότητες και υιοθετεί μια επιχειρησιακή προσέγγιση αναλύοντας προφίλ πελατών και δεδομένα συναλλαγών.

Η μελέτη των Zhou, Wang, Zhang, Liu, Jin [90] παρουσιάζει μια προσέγγιση για την αντιμετώπιση του κρίσιμου ζητήματος του εντοπισμού κακόβουλων λογαριασμών που εμπλέκονται σε δραστηριότητες νομιμοποίησης εσόδων από παράνομες δραστηριότητες εντός των διαδικτυακών κοινωνικών δικτύων. Η αυξανόμενη δημοτικότητα του εικονικού συναλλάγματος (virtual currency) στα κοινωνικά δίκτυα έχει προσελκύσει επιτήδειους που εκμεταλλεύονται διάφορες μεθόδους για να αποκτήσουν παράνομα εικονικό συνάλλαγμα και στη συνέχεια να το ξεπλύνουν με σημαντικά κέρδη. Η μελέτη εξετάζει πρωτίστως τη συμπεριφορά των χρηστών με βάση τα δεδομένα δραστηριότητας που λαμβάνονται από το Tencent QQ, ένα από τα μεγαλύτερα κοινωνικά δίκτυα παγκοσμίως, για να

διακρίνει μεταξύ κακόβουλων και αθώων λογαριασμών. Προτείνεται μια πολυεπίπεδη προσέγγιση που λαμβάνει υπόψη τη σκοπιμότητα του λογαριασμού, τις γεωγραφικές συνδέσεις και τα μοτίβα συναλλαγών για τον εντοπισμό κακόβουλων λογαριασμών που εμπλέκονται σε ξέπλυμα χρήματος. Εισάγεται επίσης μια μέθοδος με βάση την τοποθεσία σε συνδυασμό με μηχανές διανυσμάτων υποστήριξης, τυχαία δάση και λογιστική παλινδρόμηση ως στατιστικούς ταξινομητές, επιτυγχάνοντας υψηλό ποσοστό ανίχνευσης (94,2%) των κακόβουλων λογαριασμών και χαμηλό ποσοστό ψευδώς θετικών στοιχείων (0,97%).

Προηγούμενες μελέτες στην ανίχνευση της χρηματοπιστωτικής απάτης επικεντρώθηκαν σε μεθόδους ταξινόμησης και παλινδρόμησης με επίβλεψη, όπως η τεχνική SVM, τα νευρωνικά δίκτυα και η λογιστική παλινδρόμηση. Με βάση τα άρθρα που εξετάστηκαν, τα αποτελέσματα έδειξαν ότι οι αλγόριθμοι SVM και τα νευρωνικά δίκτυα είναι οι δημοφιλέστεροι αλγόριθμοι μηχανικής μάθησης που χρησιμοποιούνται, ενώ οι αλγόριθμοι ΤΑΣ βρίσκονται σε πιο πειραματικό στάδιο αλλά παρουσιάζουν υποσχόμενα αποτελέσματα. Έπειτα, η απάτη με πιστωτικές κάρτες είναι ο πιο δημοφιλής τύπος απάτης στη βιβλιογραφία. Αρκετοί ερευνητές ασχολούνται με την ανίχνευση απάτης με πιστωτικές κάρτες και έχουν αναπτυχθεί πολλές μέθοδοι.

Πίνακας 3.1: Τεχνικές και οι αντίστοιχες περιπτώσεις απάτης που έχουν χρησιμοποιηθεί

Τεχνικές	Τύπος Απάτης	Αναφορά
Naive Bayes	Πιστωτικές κάρτες, εταιρική απάτη, ασφαλιστική απάτη	[66], [76], [83], [86]
Νευρωνικά Δίκτυα	Πιστωτικές κάρτες, εταιρική απάτη, ασφαλιστική απάτη	[64], [66], [76], [80], [85]
Ευφυείς Πράκτορες	Ξέπλυμα βρώμικου χρήματος	[89]
Δέντρα Αποφάσεων	Πιστωτικές κάρτες, εταιρική απάτη	[76], [83]
Τυχαία Δάση	Πιστωτικές κάρτες, ασφαλιστική απάτη, απάτη στον κυβερνοχώρο, ξέπλυμα βρώμικου χρήματος	[79], [86], [88], [90]
Λογιστική Παλινδρόμηση	Πιστωτικές κάρτες, ασφαλιστική απάτη, ξέπλυμα βρώμικου χρήματος	[64], [77], [79], [82], [86], [90]
Γενετικοί Αλγόριθμοι	Πιστωτικές κάρτες, εταιρική απάτη	[64], [75], [82]
Μηχανές Διανυσμάτων Υποστήριξης	Πιστωτικές κάρτες, εταιρική απάτη, ασφαλιστική απάτη, ξέπλυμα βρώμικου χρήματος	[64], [79], [84], [86], [90]
Τεχνητά Ανοσοποιητικά Συστήματα	Πιστωτικές κάρτες, απάτη στον κυβερνοχώρο	[75], [77], [80], [81], [87]

Συμπεριφορικά Μοντέλα	Πιστωτικές κάρτες	[76]
Μοντέλα βασισμένα σε Κανόνες	Πιστωτικές κάρτες	[78], [80]

Στους Πίνακες 3.1 και 3.2 συνοψίζονται οι τεχνικές ανίχνευσης απάτης και οι τύποι απάτης που συναντήσαμε στην βιβλιογραφία. Ωστόσο, η ανίχνευση απάτης σε πραγματικό χρόνο παραμένει ένα ζήτημα. Η χρήση μεθόδων που εκμεταλλεύονται πολλαπλούς αλγορίθμους για την ταξινόμηση δειγμάτων αποτελεί μια αυξανόμενη τάση και δείχνει να έχει καλά αποτελέσματα. Τέλος, η συνολική πρόκληση έγκειται στην εξεύρεση ενός συστήματος που να επιτυγχάνει ισορροπία μεταξύ ακρίβειας, χρονικής αποδοτικότητας και σχέσης κόστους-αποτελεσματικότητας. Η ανίχνευση απάτης σε πραγματικό χρόνο απαιτεί μεθόδους που να μπορούν να προσαρμόζονται στη μεταβαλλόμενη συμπεριφορά των χρηστών, να ελαχιστοποιούν τα ψευδώς θετικά αποτελέσματα και να εξετάζουν ένα ευρύ φάσμα σεναρίων, διατηρώντας παράλληλα λογικούς χρόνους επεξεργασίας και κόστος. Η αντιμετώπιση αυτών των προκλήσεων παραμένει ένας συνεχής τομέας έρευνας και ανάπτυξης στον τομέα της ανίχνευσης χρηματοοικονομικής απάτης.

Πίνακας 3.2 : Τύποι απάτης και οι αντίστοιχες τεχνικές που έχουν χρησιμοποιηθεί για την εύρεσή τους

Τύπος Απάτης	Τεχνικές	Αναφορά
Πιστωτικές κάρτες	Naive Bayes, νευρωνικά δίκτυα, δέντρα αποφάσεων, τυχαία δάση, λογιστική παλινδρόμηση, γενετικοί αλγόριθμοι, μηχανές διανυσμάτων υποστήριξης, τεχνητά ανοσοποιητικά συστήματα, συμπεριφορικά μοντέλα, μοντέλα βασισμένα σε κανόνες	[75], [76], [77], [78], [79], [80], [81]
Εταιρική απάτη	Naive Bayes, νευρωνικά δίκτυα, δέντρα αποφάσεων, γενετικοί αλγόριθμοι, μηχανές διανυσμάτων υποστήριξης,	[64], [82], [83]
Ασφαλιστική απάτη	Naive Bayes, νευρωνικά δίκτυα, δέντρα αποφάσεων, τυχαία δάση, λογιστική παλινδρόμηση, μηχανές διανυσμάτων υποστήριξης	[69], [70], [84], [85], [86]
Ξέπλυμα βρώμικου χρήματος	Ευφυείς Πράκτορες, τυχαία δάση, λογιστική παλινδρόμηση, μηχανές διανυσμάτων υποστήριξης	[89], [90]
Απάτη στον κυβερνοχώρο	Τυχαία δάση, τεχνητά ανοσοποιητικά συστήματα	[87], [88]

Κεφάλαιο 5ο: Ανάπτυξη Εφαρμογής

5.1 Εισαγωγή

Ο αλγόριθμος που αναπτύξαμε είναι ένας αλγόριθμος βασισμένος σε ΤΑΣ, ο οποίος κατηγοριοποιεί δεδομένα από δύο διαφορετικά σύνολα δεδομένων ανάλογα με το αν υπάρχει απάτη ή όχι. Στο παρόν κεφάλαιο παρέχουμε μια περιγραφή των συνόλων δεδομένων που χρησιμοποιήθηκαν και στη συνέχεια την προεπεξεργασία που ακολουθήσαμε για να ετοιμάσουμε τα δεδομένα για τον αλγόριθμο. Έπειτα παρουσιάζουμε το μοντέλο κατηγοριοποίησης που δημιουργήσαμε και βασίζεται στην αρνητική επιλογή. Η ενότητα ολοκληρώνεται με την παράθεση συγκριτικών αποτελεσμάτων μεταξύ του αλγορίθμου που δημιουργήσαμε και άλλων γνωστών και πιο διαδεδομένων αλγορίθμων μηχανικής μάθησης.

5.2 Σύνολα δεδομένων

Ο αλγόριθμος Αρνητικής Επιλογής Εύρεσης Απάτης - Negative Selection Fraud Detection Algorithm (NSFDA) συντάχθηκε σε γλώσσα python και εφαρμόστηκε σε δύο σύνολα δεδομένων.

Το πρώτο σύνολο δεδομένων (DS1) έχει να κάνει με τον τομέα της ασφαλιστικής απάτης. Πιο συγκεκριμένα, περιέχει πληροφορίες για ασφαλίσεις αυτοκινήτων, δεδομένα τα οποία είναι δημόσια διαθέσιμα και παρέχονται από το λογισμικό Angoss Knowledge-Seeker [91],[92]. Αυτό το σύνολο δεδομένων περιέχει 15.420 εγγραφές, από τις οποίες μόνο το 6% (923 εγγραφές) αποτελούν ασφαλιστική απάτη, γεγονός που υποδηλώνει υψηλή ανισορροπία κλάσεων. Έχει 32 χαρακτηριστικά σε σύνολο εκ των οποίων 6 είναι αριθμητικά, 25 είναι κατηγορικά και τέλος, η μεταβλητή κλάσης που περιέχει την ετικέτα – “απάτη” ή “μη απάτη”. Εξ όσων γνωρίζουμε, αυτό το σύνολο δεδομένων για απάτες στον τομέα της ασφάλισης αυτοκινήτου είναι το μοναδικό διαθέσιμο στην ακαδημαϊκή βιβλιογραφία.

Το δεύτερο σύνολο δεδομένων (DS2) έχει να κάνει με την απάτη σε πιστωτικές κάρτες [93]. Συλλέχθηκε και αναλύθηκε κατά τη διάρκεια ερευνητικής συνεργασίας της εταιρείας Worldline και του Machine Learning Group του Ελεύθερου Πανεπιστημίου των Βρυξελλών (Université Libre de Bruxelles) [94] για την εξόρυξη μεγάλων δεδομένων και την ανίχνευση απάτης. Το σύνολο δεδομένων περιλαμβάνει συναλλαγές που πραγματοποιήθηκαν με πιστωτικές κάρτες τον Σεπτέμβριο

του 2013 από Ευρωπαίους κατόχους καρτών. Αυτό το σύνολο δεδομένων περιέχει 284.807 συναλλαγές που πραγματοποιήθηκαν σε δύο ημέρες, όπου έχουμε 492 συναλλαγές που υποδηλώνουν απάτη. Το σύνολο δεδομένων είναι εξαιρετικά μη ισορροπημένο, καθώς η θετική κατηγορία (απάτη) αντιπροσωπεύει το 0,172% όλων των συναλλαγών. Περιέχει μόνο αριθμητικές μεταβλητές εισόδου οι οποίες είναι το αποτέλεσμα ενός μετασχηματισμού ανάλυσης κύριων συνιστωσών - Principal Component Analysis (PCA). Δυστυχώς, λόγω ζητημάτων εμπιστευτικότητας, τα αρχικά χαρακτηριστικά, οι περισσότερες πληροφορίες υποβάθρου σχετικά με τα δεδομένα είναι κρυπτογραφημένα. Τα χαρακτηριστικά V1, V2, ... V28 είναι οι κύριες συνιστώσες που προέκυψαν με PCA. Τα μόνα χαρακτηριστικά που δεν έχουν μετασχηματιστεί με PCA είναι τα "Time" και "Amount". Το χαρακτηριστικό "Time" περιέχει τα δευτερόλεπτα που πέρασαν μεταξύ κάθε συναλλαγής και της πρώτης συναλλαγής στο σύνολο δεδομένων. Το χαρακτηριστικό "Amount" είναι το ποσό της συναλλαγής ενώ το χαρακτηριστικό "Class" είναι η μεταβλητή απόκρισης και παίρνει την τιμή 1 σε περίπτωση απάτης και 0 σε αντίθετη περίπτωση.

5.3 Προεπεξεργασία δεδομένων

Η προεπεξεργασία δεδομένων είναι ένα κρίσιμο βήμα στον τομέα της μηχανικής μάθησης που περιλαμβάνει τον καθαρισμό, τον μετασχηματισμό και την οργάνωση των ακατέργαστων δεδομένων σε μορφή κατάλληλη για την εκπαίδευση και την αξιολόγηση των μοντέλων μηχανικής μάθησης.

Αρχικά έγινε η μετατροπή των κατηγορικών στηλών σε αριθμητικές με την τεχνική Label Encoding της βιβλιοθήκης scikit-learn. Αυτός ο μετασχηματισμός επιτρέπει στους αλγορίθμους μηχανικής μάθησης να εργάζονται με κατηγορικά δεδομένα καθώς απαιτούν ως είσοδο αριθμητικά δεδομένα. Αυτό το βήμα μετατρέπει τα μη αριθμητικά δεδομένα σε μορφή που μπορεί να χρησιμοποιηθεί από τον αλγόριθμο. Έπειτα διασφαλίσαμε ότι το σύνολο δεδομένων δεν περιέχει διπλές γραμμές, το οποίο είναι ένα συνηθισμένο βήμα προεπεξεργασίας για τη βελτίωση της ποιότητας και της αξιοπιστίας της ανάλυσης και της μοντελοποίησης των δεδομένων. Ύστερα εφαρμόσαμε κανονικοποίηση Z-Score - Z-Score Normalization στα αριθμητικά χαρακτηριστικά χρησιμοποιώντας την κλάση StandardScaler της βιβλιοθήκης scikit-learn. Αυτή η διαδικασία μετατρέπει τις αριθμητικές τιμές κάθε χαρακτηριστικού ώστε να έχουν μέση τιμή 0 και τυπική απόκλιση 1. Τυποποιεί τα χαρακτηριστικά αφαιρώντας τον μέσο όρο και κλιμακώνοντάς τα σε μοναδιαία διακύμανση. Συγκεκριμένα, για κάθε χαρακτηριστικό, μετασχηματίζει τα δεδομένα σύμφωνα με την εξίσωση 5.1 [95]:

$$z = \frac{(x-u)}{s} \qquad \text{(Εξ. 5.1)}$$

Όπου:

- x είναι ένα αρχικό σημείο δεδομένων (ή τιμή χαρακτηριστικού).
- u είναι ο μέσος όρος του χαρακτηριστικού.
- s είναι η τυπική απόκλιση του χαρακτηριστικού
- z είναι η τυποποιημένη (ή κλιμακωτή) τιμή.

Η τυπική κλιμάκωση είναι σημαντική επειδή πολλοί αλγόριθμοι μηχανικής μάθησης αποδίδουν καλύτερα όταν τα χαρακτηριστικά βρίσκονται σε παρόμοια κλίμακα. Βοηθά στην αποτροπή του να κυριαρχούν τα χαρακτηριστικά με μεγαλύτερα μεγέθη στη διαδικασία μάθησης.

Στη συνέχεια χωρίσαμε το σύνολο δεδομένων σε ένα σύνολο εκπαίδευσης και ένα σύνολο δοκιμών. Αυτό γίνεται για να εκπαιδευτεί το μοντέλο σε ένα τμήμα των δεδομένων και να αξιολογηθεί η

απόδοσή του σε ένα άλλο τμήμα. Τα δεδομένα χωρίζονται σε αναλογία 80-20, όπου το 80% χρησιμοποιήθηκε για εκπαίδευση και το 20% για δοκιμή. Αυτό βοηθά στην αποφυγή της υπερπροσαρμογής (overfitting) και δίνει μια εκτίμηση του πόσο καλά γενικεύεται το μοντέλο σε νέα δεδομένα.

Η παραπάνω προεπεξεργασία έγινε και στα δύο σύνολα δεδομένων.

5.4 Negative Selection Fraud Detection Algorithm

Στον τομέα της ανίχνευσης ανωμαλιών, ιδίως όταν εμπνέεται από τους μηχανισμούς του ανοσοποιητικού συστήματος, οι έννοιες του “εαυτού” και του “ξένου” παίζουν καθοριστικό ρόλο. Τα δεδομένα “εαυτού” αντιπροσωπεύουν την κανονική, αναμενόμενη συμπεριφορά ή τα μοτίβα, ενώ τα δεδομένα “ξένου” υποδηλώνουν ανωμαλίες ή απροσδόκητα μοτίβα. Οι κύριες εφαρμογές των αλγόριθμων αρνητικής επιλογής αφορούν τον τομέα της ανίχνευσης ανωμαλιών και για αυτό κάναμε αυτή την επιλογή. Ένας NSA αποτελείται από τρεις φάσεις: τον προσδιορισμό του “εαυτού”, τη δημιουργία ανιχνευτών και την παρακολούθηση της εμφάνισης ανωμαλιών. Στο πλαίσιο του αλγορίθμου που δημιουργήσαμε, τα δεδομένα “εαυτού” περιλαμβάνουν τις εγγραφές που δεν αποτελούν απάτη, οι οποίες είναι πιο συνηθισμένες και αντιπροσωπεύουν τον κανόνα. Αντίθετα, τα δεδομένα “ξένου” αποτελούνται από τις εγγραφές που υποδηλώνουν απάτη, οι οποίες αποτελούν ανωμαλίες που το σύστημα στοχεύει να εντοπίσει. Εντούτοις, χωρίσαμε περαιτέρω το σύνολο εκπαίδευσης σε δύο υποσύνολα, σύνολο δεδομένων “εαυτού” (εγγραφές που δεν περιέχουν απάτη) και σύνολο δεδομένων “ξένου” (εγγραφές που περιέχουν απάτη). Η διαδικασία διαχωρισμού των δεδομένων σε αυτές τις δύο κατηγορίες είναι ζωτικής σημασίας για τον αλγόριθμο αρνητικής επιλογή. Εν ολίγοις, με τη διάκριση μεταξύ των δύο, ένας αλγόριθμος αρνητικής επιλογής μπορεί να δημιουργήσει ανιχνευτές (detectors) που είναι ευαίσθητοι στα “ξένα” μοτίβα χωρίς να ενεργοποιούνται από τα μοτίβα “εαυτού”, διασφαλίζοντας ότι δεν θα ταξινομηθούν λανθασμένα τα “ξένα” μοτίβα ως φυσιολογικά. Το επόμενο βήμα είναι η παραγωγή αυτών των ανιχνευτών.

Υπάρχουν αρκετές μέθοδοι για την δημιουργία ανιχνευτών σε έναν αλγόριθμο αρνητικής επιλογής, κάποιους από τους οποίους παρουσιάσαμε στο Κεφάλαιο 3. Εμείς επιλέξαμε μια τυχαία προσέγγιση μέσω ενός αλγόριθμου ομαδοποίησης, του αλγόριθμου Κ-Μέσων, για τον εντοπισμό πιθανών υποψηφίων ανιχνευτών. Ο στόχος αυτής της διαδικασίας ομαδοποίησης είναι να συλλάβουμε αντιπροσωπευτικά μοτίβα μέσα στα δεδομένα του “εαυτού”, τα οποία θα χρησιμοποιηθούν αργότερα ως πιθανοί υποψήφιοι ανιχνευτές. Αυτά τα μοτίβα, που αντιπροσωπεύονται από τα κεντροειδή των συστάδων που παράγει ο αλγόριθμος Κ-Μέσων, χρησιμεύουν ως σημείο εκκίνησης για τη δημιουργία ανιχνευτών που μπορούν να αναγνωρίσουν ανωμαλίες. Στο τέλος της διαδικασίας ομαδοποίησης, κάθε σημείο δεδομένων στο σύνολο δεδομένων “εαυτού” αντιστοιχίζεται σε μία από τις "Κ" συστάδες. Το πιο σημαντικό είναι ότι με την ομαδοποίηση προσδιορίζονται "Κ" κεντροειδή, όπου κάθε κεντροειδές είναι ένα αντιπροσωπευτικό σημείο της αντίστοιχης συστάδας. Αυτά τα κεντροειδή χρησιμεύουν ως πιθανοί υποψήφιοι για τη δημιουργία ανιχνευτών. Ο αλγόριθμος ομαδοποίησης λειτουργεί επαναληπτικά για να αναθέσει κάθε σημείο δεδομένων σε μία από τις "Κ" συστάδες με βάση την ομοιότητα/συγγένεια των χαρακτηριστικών. Ο κανόνας συγγένειας καθορίζει την ομοιότητα μεταξύ δύο μοτίβων για την ταξινόμησή τους ως “ξένα” ή “εαυτού”. Το μέτρο ομοιότητας που επιλέξαμε είναι η Ευκλείδεια απόσταση. Στη συνέχεια, κάθε υποψήφιος ανιχνευτής ελέγχεται σε σχέση με τα δεδομένα “ξένου”. Εάν ο υποψήφιος ανιχνευτής απέχει επαρκώς από όλα τα σημεία δεδομένων “ξένου” (όπως καθορίζεται από ένα προκαθορισμένο κατώφλι), θεωρείται έγκυρος

ανιχνευτής και προστίθεται στον κατάλογο ανιχνευτών αλλιώς απορρίπτεται. Με τον τρόπο αυτό διασφαλίζεται ότι οι ανιχνευτές είναι ευαίσθητοι στις ανωμαλίες, ενώ παράλληλα είναι απρόσβλητοι στα κανονικά μοτίβα.

Μόλις δημιουργηθούν οι ανιχνευτές, χρησιμεύουν ως βάση για τη διαδικασία ταξινόμησης. Για κάθε σημείο δεδομένων που πρέπει να ταξινομηθεί, ο NSFDA υπολογίζει την απόστασή του από κάθε ανιχνευτή. Και πάλι, η Ευκλείδεια απόσταση είναι το μέτρο που χρησιμοποιούμε για να καθοριστεί πόσο κοντά βρίσκεται ένα σημείο δεδομένων σε έναν ανιχνευτή. Το προκαθορισμένο κατώφλι παίζει καθοριστικό ρόλο στην ταξινόμηση. Εάν το σημείο δεδομένων βρίσκεται εντός της απόστασης κατωφλίου από οποιονδήποτε ανιχνευτή, επισημαίνεται ως "ξένο" ή ανώμαλο. Αντίθετα, εάν το σημείο δεδομένων βρίσκεται πέραν της απόστασης κατωφλίου από όλους τους ανιχνευτές, ταξινομείται ως "εαυτού" ή κανονικό. Το αποτέλεσμα της απόφασης βάσει κατωφλίου για κάθε σημείο δεδομένων είναι μια δυαδική ταξινόμηση:

- 0 : Μη Απάτη
- 1 : Απάτη

Αυτές οι προβλέψεις στη συνέχεια συγκρίνονται με τις πραγματικές τιμές για να αξιολογηθεί η απόδοση του NSFDA.

Πριν από την εφαρμογή του NSFDA, το μοντέλο πρέπει να αρχικοποιηθεί με δύο συγκεκριμένες παραμέτρους που καθορίζουν τη συμπεριφορά του. Η πρώτη παράμετρος είναι ο αριθμός των συστάδων που θα προσπαθήσει να βρει ο αλγόριθμος K-Μέσων στα δεδομένα "εαυτού". Αυτές οι συστάδες θα χρησιμεύσουν ως πιθανοί υποψήφιοι για ανιχνευτές. Ένας μεγάλος αριθμός συστάδων σημαίνει μια πιο λεπτομερή αναπαράσταση των δεδομένων του "εαυτού", οδηγώντας σε έναν δυνητικά μεγαλύτερο αριθμό υποψηφίων ανιχνευτών. Η επιλογή του αριθμού των συστάδων μπορεί να επηρεάσει την ευαισθησία και την ειδικότητα των παραγόμενων ανιχνευτών. Η δεύτερη παράμετρος είναι το κατώφλι (threshold) που καθορίζει την απόσταση εντός της οποίας ένα σημείο δεδομένων θεωρείται κοντά σε έναν ανιχνευτή.

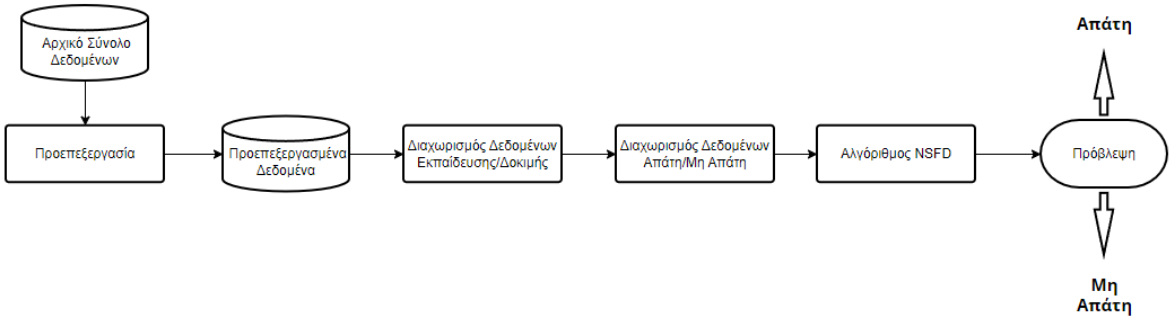
Στο Σχήμα 5.1 παρουσιάζεται το διάγραμμα ροής του NSFDA ενώ στην Εικόνα 5.1 παρουσιάζεται σε ψευδογλώσσα ο κώδικας του NSFDA

Παρακάτω παρουσιάζεται μια βηματική αναπαράσταση του προσαρμοσμένου αλγόριθμου NSFDA:

1. *Προεπεξεργασία δεδομένων :* Φόρτωση συνόλου δεδομένων. Αφαίρεση διπλοτύπων. Κωδικοποίηση κατηγορικών στηλών.
2. *Διαχωρισμός δεδομένων :* Διαχωρισμός του συνόλου δεδομένων σε σύνολα εκπαίδευσης και δοκιμής. Περαιτέρω διαχωρισμός των δεδομένων εκπαίδευσης σε δεδομένα που δεν περιέχουν απάτη (δεδομένα "εαυτού") και σε δεδομένα που περιέχουν απάτη (δεδομένα "ξένου").
3. *Αρχικοποίηση NSFDA:* Ορισμός αριθμού συστάδων. Ορισμός κατωφλίου.
4. *Εκπαίδευση :* Εφαρμογή ομαδοποίησης K-Means στα δεδομένα "εαυτού". Προσδιορισμός των κεντροειδών των συστάδων ως πιθανών υποψηφίων ανιχνευτών.
5. *Δημιουργία ανιχνευτών*: Για κάθε κεντροειδές (υποψήφιο): Υπολογισμός της απόστασής του από κάθε σημείο του συνόλου δεδομένων "ξένου". Εάν ο υποψήφιος είναι απομακρυσμένος από όλα τα σημεία δεδομένων "ξένου" (πέραν του κατωφλίου), πρόσθεσέ τον στον κατάλογο των ανιχνευτών.
6. Ταξινόμηση : Για κάθε σημείο δεδομένων στο σύνολο δεδομένων: Υπολογίστε την απόστασή του από κάθε ανιχνευτή. Εάν το σημείο δεδομένων είναι κοντά σε οποιονδήποτε ανιχνευτή

(εντός του κατωφλίου), ταξινομήστε το ως “ξένο” (απάτη). Διαφορετικά, ταξινομήστε το ως “εαυτός”.

7. *Έξοδος :* Σύγκριση των προβλεπόμενων ετικετών με τις πραγματικές ετικέτες.



Σχήμα 5.1 : Διάγραμμα ροής NSFDA

```
BEGIN

   // Data Preprocessing
  dataset = LoadDataset()
  dataset = RemoveDuplicates(dataset)
  dataset = EncodeCategoricalColumns(dataset)

  // Split Data
  training_set, testing_set = SplitDataset(dataset)
  self_data = ExtractData(training_set, label=0)  // 0: Non-fraud
  non_self_data = ExtractData(training_set, label=1)  // 1: Fraud

  // Initialize NSFDA
  n_clusters, threshold = InitializeNSFDAParameters()

  // Clustering the "Self" Data
  kmeans_model = ApplyKMeans(self_data, n_clusters)
  centroids = GetCentroids(kmeans_model)

  // Generate Detectors
  detectors = []
  FOR each centroid IN centroids:
     IF IsDistantFromAll(centroid, non_self_data, threshold):
        detectors.ADD(centroid)
     END IF
  END FOR

  // Classification
  labels = []
  FOR each data_point IN testing_set:
     IF IsCloseToAnyDetector(data_point, detectors, threshold):
        labels.ADD(1)  // 1: Fraud
     ELSE:
        labels.ADD(0)  // 0: Non-fraud
     END IF
  END FOR

  // Evaluation
  IF true_labels_available:
     CompareLabels(labels, true_labels)
     DisplayClassificationReport(labels, true_labels)
     DisplayAUPRC(labels, true_labels)
  END IF

END
```

Εικόνα 5.1 : Αλγόριθμος NSFD

5.5 Μοντέλα Κατηγοριοποιητών

Επιλέξαμε πέντε γνωστά μοντέλα κατηγοριοποίησης με επιβλεπόμενη μάθηση για να παραθέσουμε μια σύγκριση μεταξύ αυτών των μοντέλων και του μοντέλου NSFDA. Κάθε μοντέλο έχει συγκεκριμένες παραμέτρους που επηρεάζουν τη συμπεριφορά του κατά την εκπαίδευση και την πρόβλεψη. Η επιλογή των παραμέτρων λαμβάνει υπόψη τα χαρακτηριστικά του προβλήματος ανίχνευσης απάτης, όπως η ανισορροπία των κλάσεων και η ανάγκη αναπαραγωγιμότητας. Οι συγκεκριμένες τιμές των παραμέτρων καθορίστηκαν μετά από πειραματισμούς. Ας δούμε κάθε μοντέλο και τις σχετικές παραμέτρους του:

Λογιστική Παλινδρόμηση: Η λογιστική παλινδρόμηση είναι ένας απλός αλλά αποτελεσματικός αλγόριθμος γραμμικής ταξινόμησης. Χρησιμοποιείται συχνά ως βασικό μοντέλο λόγω της ερμηνευσιμότητάς του και της ευκολίας υλοποίησής του. Θέσαμε την τιμή του μέγιστου αριθμού

επαναλήψεων για να συγκλίνει ο επιλύτης στις 500 επαναλήψεις. Δεδομένου ότι το σύνολο δεδομένων είναι πολύπλοκο, ο ορισμός μιας υψηλότερης τιμής (500) διασφαλίζει ότι ο αλγόριθμος βελτιστοποίησης έχει αρκετές επαναλήψεις για να βρει λύση. Το σύνολο δεδομένων είναι ανισόρροπο, με λιγότερες περιπτώσεις απάτης. Για αυτό τον λόγο αναθέσαμε υψηλότερα βάρη στην κλάση μειοψηφίας (απάτη) κατά τη διάρκεια της εκπαίδευσης, ώστε να αποτραπεί η μεροληψία του μοντέλου προς την κλάση πλειοψηφίας. Αυτό μπορεί να βοηθήσει το μοντέλο να αποδώσει καλύτερα στην κλάση της μειονότητας.

Δέντρα Αποφάσεων: Τα δέντρα αποφάσεων χωρίζουν τα δεδομένα σε υποσύνολα με βάση τις τιμές των χαρακτηριστικών. Κάθε δέντρο αποφάσεων αποτελείται από εσωτερικούς κόμβους οι οποίοι αναπαριστούν τις αποφάσεις που αντιστοιχούν στα υπερεπίπεδα ή σημεία διαμερισμού (δηλαδή σε ποιον ημιχώρο ανήκει ένα καθορισμένο σημείο), καθώς και από κόμβους-φύλλα που αναπαριστούν περιοχές ή διαμερίσεις του χώρου δεδομένων, οι οποίοι έχουν ως ετικέτα την πλειοψηφική κατηγορία (στην περιπτωσή μας 0 που δηλώνει μη απάτη) [96]. Παρομοίως, τα βάρη της κλάσης παραμετροποιήθηκαν κατάλληλα για να χειρίζεται η ανισορροπία των κλάσεων.

Τυχαία Δάση: Τα τυχαία δάση είναι ένα σύνολο δέντρων αποφάσεων, τα οποία συμβάλλουν στη μείωση της υπερπροσαρμογής και στη βελτίωση της γενίκευσης. Θέσαμε τον αριθμό των δέντρων στο δάσος ίσο με 100. Ένας μεγαλύτερος αριθμός οδηγεί γενικά σε καλύτερες επιδόσεις, αλλά μπορεί επίσης να αυξήσει τον υπολογιστικό χρόνο. Εδώ, επιλέγονται 100 δέντρα ως μια λογική ισορροπία.

SVM: Οι μηχανές διανυσμάτων υποστήριξης αποτελούν μια μέθοδο κατηγοριοποίησης που βασίζεται σε γραμμικούς διαχωρισμούς μέγιστου περιθωρίου. Ο στόχος είναι να βρεθεί το βέλτιστο υπερεπίπεδο που μεγιστοποιεί το κενό ή περιθώριο μεταξύ των κλάσεων. Ο κατηγοριοποιητής SVM είναι ισχυρός τόσο για γραμμική όσο και για μη γραμμική ταξινόμηση. Μπορεί να χειριστεί δεδομένα υψηλών διαστάσεων και λειτουργεί καλά με σύνολα δεδομένων μικρού έως μεσαίου μεγέθους [96]. Η παράμετρος βάρους κλάσεων έχει τεθεί κι εδώ να είναι ισορροπημένη ενώ έχουμε ενεργοποιήσει την παράμετρο εκτιμήσεων πιθανότητας που είναι χρήσιμη για τον υπολογισμό μετρικών αξιολόγησης των αποτελεσμάτων που θα δούμε στην συνέχεια.

Naive Bayes: Ένας κατηγοριοποιητής Bayes χρησιμοποιεί το θεώρημα του Bayes για να προβλέψει ότι η ζητούμενη κατηγορία είναι εκείνη που μεγιστοποιεί την εκ των υστέρων πιθανότητα (posterior probability). Ο Naive Bayes είναι ένας πιθανοτικός αλγόριθμος που υποθέτει ότι τα γνωρίσματα είναι ανεξάρτητα και είναι υπολογιστικά αποδοτικός και απλός στην υλοποίηση. Παρόλο που μπορεί να μην αποτυπώνει τις πολύπλοκες σχέσεις τόσο καλά όσο κάποια άλλα μοντέλα, χρησιμοποιείται συχνά ως βασική γραμμή [96]. Στην υλοποίησή μας χρησιμοποιήσαμε κατανομή Gauss για τα χαρακτηριστικά κάθε κλάσης.

XGBoost: Ο κατηγοριοποιητής XGBoost είναι μια ensemble τεχνική που έχει στόχο να συνδυάσει τις προβλέψεις πολλών μοντέλων πρόβλεψης που έχουν κατασκευαστεί με έναν δεδομένο αλγόριθμο μάθησης, προκειμένου να βελτιώσουν τη γενικευσιμότητα/ανθεκτικότητα σε σχέση με έναν μεμονωμένο μοντέλο πρόβλεψης. Δημιουργεί ένα σύνολο μοντέλων πρόβλεψης, συνήθως δέντρα αποφάσεων, με τρόπο που να γίνεται σταδιακά [97].

5.6 Αποτελέσματα συγκριτικών μετρήσεων

Η επιλογή των μετρικών αξιολόγησης που χρησιμοποιούνται όταν εργαζόμαστε με μη ισορροπημένα σύνολα δεδομένων είναι εξαιρετικά σημαντική. Για παράδειγμα, η ακρίβεια (accuracy) είναι η πιο

κοινή μετρική απόδοσης και ορίζεται ως ο λόγος των σωστά προβλεπόμενων παρατηρήσεων προς το συνολικό αριθμό παρατηρήσεων [96]. Η ακρίβεια δεν κάνει διάκριση μεταξύ τύπων σφαλμάτων (ψευδώς θετικά έναντι ψευδώς αρνητικών). Σε πολλά σενάρια του πραγματικού κόσμου, αυτά τα σφάλματα έχουν διαφορετικές επιπτώσεις. Για παράδειγμα, στην ανίχνευση απάτης, ένα ψευδώς αρνητικό (αποτυχία εντοπισμού μιας απάτης) μπορεί να έχει σοβαρότερες συνέπειες από ένα ψευδώς θετικό (λανθασμένη επισήμανση μιας συναλλαγής ως απάτη). Επομένως η ακρίβεια είναι ανεπαρκής ως δείκτης απόδοσης όταν υπάρχει σημαντική ανισορροπία κλάσεων στα δεδομένα, καθώς μια προεπιλεγμένη πρόβλεψη όλων των περιπτώσεων στην πλειοψηφούσα τάξη θα δείξει υψηλή τιμή απόδοσης. Επομένως, οι παραδοσιακές μετρικές αξιολόγησης κατηγοριοποίησης δεν ανταποκρίνονται επαρκώς στις απαιτήσεις απόδοσης της δικιάς μας εφαρμογής.

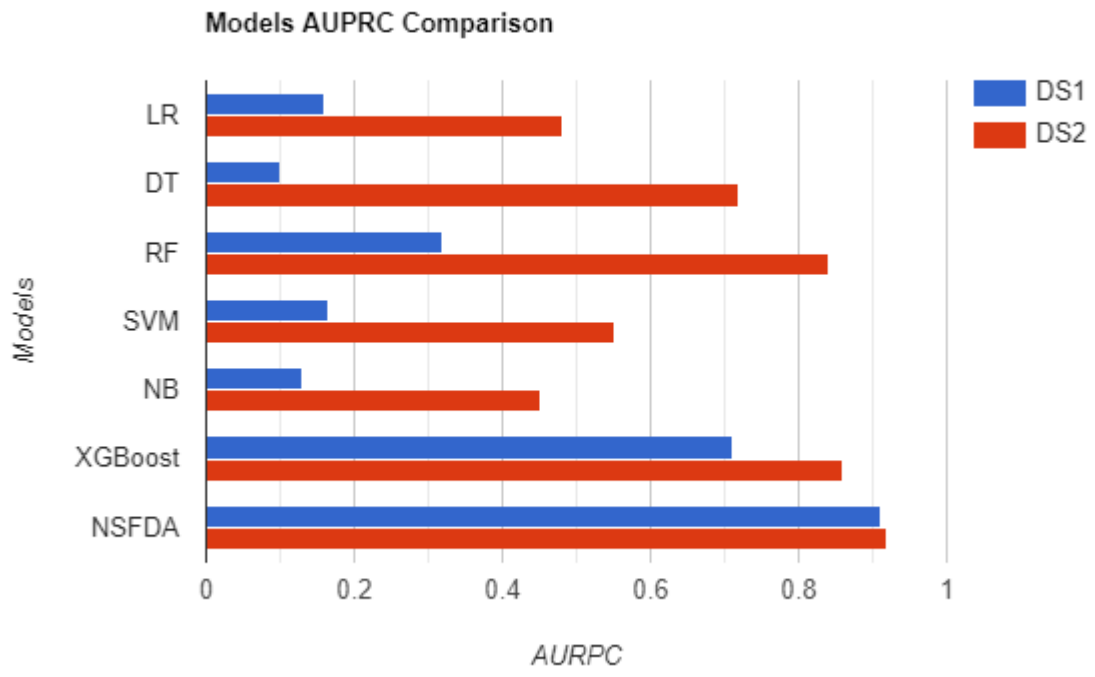
Η περιοχή κάτω από την καμπύλη ορθότητας/ανάκλησης - Area Under Precision/Recall Curve (AUPRC) είναι μια ευρέως χρησιμοποιούμενη μετρική για την αξιολόγηση της απόδοσης δυαδικών μοντέλων ταξινόμησης [98]. Η AUPRC παρέχει πολύτιμες πληροφορίες σχετικά με την ικανότητα ενός μοντέλου να διακρίνει μεταξύ θετικών και αρνητικών περιπτώσεων, καθιστώντας την ιδιαίτερα κατάλληλη για την αξιολόγηση της αποτελεσματικότητας των αλγορίθμων ανίχνευσης απάτης. Στην ανίχνευση απάτης, η εστίαση είναι συχνά ο σωστός εντοπισμός της θετικής κατηγορίας (εγγραφες με απάτη) με παράλληλη ελαχιστοποίηση των ψευδώς θετικών αποτελεσμάτων. Η ορθότητα (precision) και η ανάκληση (recall) είναι δύο σημαντικές μετρικές για την αξιολόγηση αυτού του συμβιβασμού. Η ορθότητα αναφέρεται στο κλάσμα των αληθώς θετικών προβλέψεων μεταξύ όλων των θετικών προβλέψεων [96]. Απαντά στο ερώτημα: "Από όλες τις περιπτώσεις που ταξινομούνται ως θετικές, πόσες είναι πραγματικά θετικές;" Η ανάκληση (ή ευαισθησία) αναφέρεται στο κλάσμα των αληθώς θετικών προβλέψεων μεταξύ όλων των πραγματικών θετικών περιπτώσεων [96]. Απαντά στην ερώτηση: "Από όλες τις πραγματικές θετικές περιπτώσεις, πόσες ταξινομήθηκαν σωστά;" Η AUPRC συνοψίζει την αντιστάθμιση ορθότητας/ανάκλησης σε διάφορα κατώτατα όρια πιθανότητας, βοηθώντας στην επιλογή ενός κατάλληλου κατωφλίου που εξισορροπεί την ορθότητα και την ανάκληση. Στην ανίχνευση απάτης, η υψηλή ανάκληση είναι ζωτικής σημασίας, διότι είναι σημαντικό να εντοπιστούν όσο το δυνατόν περισσότερες πραγματικές περιπτώσεις απάτης. Ταυτόχρονα, η υψηλή ορθότητα είναι απαραίτητη για να αποφευχθεί η εσφαλμένη ταξινόμηση πάρα πολλών νόμιμων συναλλαγών ως απάτη, γεγονός που μπορεί να οδηγήσει σε λειτουργικές προκλήσεις και δυσαρέσκεια των πελατών.

Συνοψίζοντας, η AUPRC είναι μια κατάλληλη μετρική για την ανίχνευση απάτης λόγω της εστίασής της στη θετική κλάση, της ανθεκτικότητάς της στην ανισορροπία κλάσεων και της ικανότητάς της να παρέχει πληροφορίες σχετικά με την απόδοση του μοντέλου σε διαφορετικές συμβιβαστικές λύσεις μεταξύ ορθότητας/ανάκλησης. Κατά την αντιμετώπιση δεδομένων με ανισόρροπες κλάσεις και την ιεράρχηση της ανίχνευσης σπάνιων συμβάντων, η AUPRC είναι η πιο κατατοπιστική μετρική και υιοθετείται ευρέως για την αξιολόγηση των επιδόσεων των μοντέλων ανίχνευσης απάτης [99].

Έτσι, αποφασίσαμε να μετρήσουμε την συνολική απόδοση του κάθε μοντέλου συγκρίνοντας τις τιμές AUPRC. Στον Πίνακα 5.1 παρουσιάζονται οι τιμές AUPRC κάθε μοντέλου και για τα δύο σύνολα δεδομένων και στην Εικόνα 5.2 παρουσιάζεται ένα ραβδόγραμμα σύγκρισης των αποτελεσμάτων των μοντέλων για κάθε σύνολο δεδομένων.

Πίνακας 5.1 : Τιμή AUPRC κάθε μοντέλου για κάθε σύνολο δεδομένων

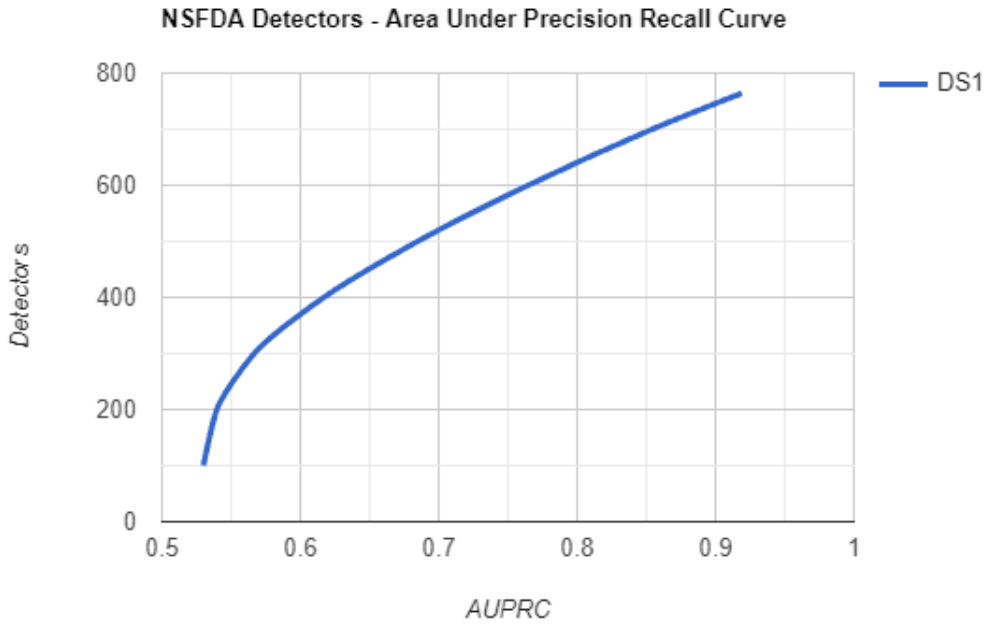
Μοντέλο	DS1	DS2
Λογιστική Παλινδρόμηση	0.1680	0.4897
Δέντρα Αποφάσεων	0.1046	0.7219
Τυχαία Δάσοι	0.3235	0.8475
Μηχανές Διανυσμάτων Υποστήριξης	0.1648	0.5504
Naive Bayes	0.1388	0.4529
XGBoost	0.7117	0.8650
NSFDA	0.9190	0.9219



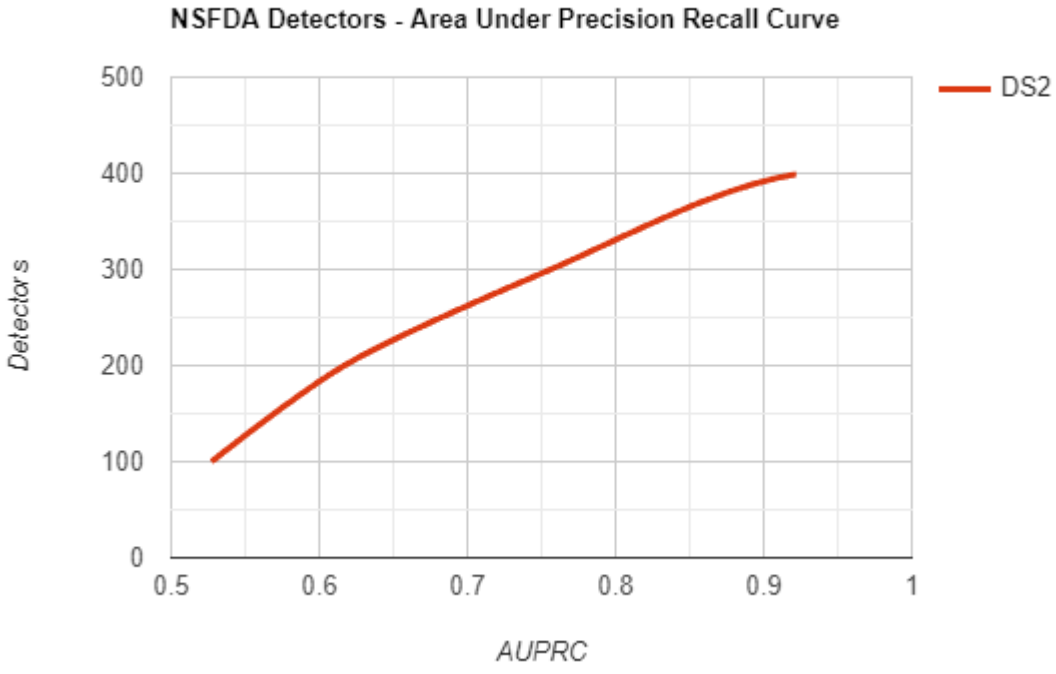
Εικόνα 5.2 : Σύγκριση μοντέλων με βάση τις καμπύλες ορθότητας/ανάκλησης

Παρατηρούμε ότι ο NSFDA έχει αρκετά καλές επιδόσεις και στα δύο σύνολα δεδομένων με 0,9190 στο DS1 και 0,9219 στο DS2. Αυτό δείχνει ότι το μοντέλο μπορεί να εντοπίσει αποτελεσματικά ένα σημαντικό μέρος των περιπτώσεων απάτης (υψηλή ανάκληση), διατηρώντας παράλληλα ένα χαμηλό ποσοστό ψευδώς θετικών αποτελεσμάτων (υψηλή ορθότητα). Ο XGBoost έχει το υψηλότερο AUPRC (0,7117 στο DS1 και 0,8650 στο DS2) μεταξύ των μοντέλων μηχανικής μάθησης. Επιπλέον παρατηρούμε ότι στο DS2 παίρνουμε καλύτερα αποτελέσματα σε σύγκριση με το DS1. Αυτό είναι αναμενόμενο, καθώς ο μεγαλύτερος όγκος δεδομένων παρέχει στα μοντέλα καλύτερη αναπαράσταση των υποκείμενων μοτίβων.

Να προσθέσουμε ότι στην περίπτωση του NSFDA η παράμετρος που καθορίζει τον αριθμό των συστάδων του αλγόριθμου ομαδοποίησης K-Μέσων και κατα συνέπεια τον αριθμό των ανιχνευτών που θα παραχθούν παίζει τον μεγαλύτερο ρόλο στο αποτέλεσμα. Όπως βλέπουμε και στις Εικόνες 5.3 και 5.4, όσο αυξάνεται ο αριθμός των ανιχνευτών τόσο μεγαλύτερη είναι και η τιμή AUPRC. Αυτό μας εξασφαλίζει ότι με την είσοδο καινούργιων δειγμάτων και την δημιουργία παραπανω ανιχνευτών θα ταξινομηθούν και τα καινούρια δείγματα.



Εικόνα 5.3 : Διάγραμμα Ανιχνευτών - AUPRC συνόλου δεδομένων DS1



Εικόνα 5.4: Διάγραμμα Ανιχνευτών - AUPRC συνόλου δεδομένων DS2

Όταν εξετάζουμε τα μοντέλα με βάση την μετρική AUPRC, ο αλγόριθμος αρνητικής επιλογής (NSFDA) υπερέχει όλων των άλλων μοντέλων μηχανικής μάθησης στη σύγκριση με σημαντική διαφορά. Μεταξύ των παραδοσιακών μοντέλων μηχανικής μάθησης, ο XGBoost επιδεικνύει την καλύτερη απόδοση.

Ωστόσο, είναι σημαντικό να λαμβάνονται υπόψη και άλλοι παράγοντες, όπως η ερμηνευσιμότητα, το υπολογιστικό κόστος και η ευκολία ανάπτυξης, κατά την επιλογή ενός μοντέλου για πραγματικές εφαρμογές. Στην ανίχνευση απάτης, οι περιπτώσεις που προβλέπονται ως πιθανή απάτη αναλαμβάνονται για διερεύνηση ή για κάποια περαιτέρω ενέργεια, η οποία περιλαμβάνει κάποιο κόστος. Η ακριβής ταυτοποίηση των περιπτώσεων απάτης συμβάλλει στην αποφυγή του κόστους που προκύπτει από δόλια δραστηριότητα, το οποίο είναι γενικά μεγαλύτερο από το κόστος διερεύνησης μιας πιθανής δόλιας συναλλαγής. Ωστόσο, το εν λόγω κόστος από μη εντοπισθείσα απάτη θα προκύψει για περιπτώσεις απάτης που δεν καταγράφονται από το μοντέλο.

Ένα μοντέλο με υψηλή τιμή AUPRC υποδηλώνει ότι όταν το μοντέλο επισημαίνει μια συναλλαγή ως απάτη, υπάρχει μεγάλη πιθανότητα να είναι πράγματι απάτη. Αυτό μπορεί να μειώσει το λειτουργικό κόστος όσον αφορά τις χειροκίνητες αναθεωρήσεις. Αντίστροφα, υποδεικνύει επίσης ότι το μοντέλο μπορεί να ανιχνεύσει ένα σημαντικό μέρος των πραγματικών περιπτώσεων απάτης, ελαχιστοποιώντας τις πιθανές απώλειες λόγω απάτης.

Κεφάλαιο 6ο: Μελλοντικές Εργασίες και Έρευνα

Η μεγαλύτερη δυσκολία στην ανάπτυξη ενός αλγόριθμου αρνητικής επιλογής και εν προκειμένω στην ανάπτυξη του μοντέλου μας εντοπίζεται στην διαδικασία δημιουργίας των ανιχνευτών. Στο Κεφάλαιο 3 προτείνονται διάφοροι μέθοδοι δημιουργίας ανιχνευτών με τους οποίους θα μπορούσε να υπάρξει πειραματισμός για να βρούμε μια καλύτερη μέθοδο δημιουργίας ανιχνευτών.

Έπειτα, η επεκτασιμότητα (scalability) του NSFDA αποτελεί επίσης αντικείμενο περαιτέρω μελέτης. Καθώς αυξάνεται ο όγκος ή οι διαστάσεις των δεδομένων, οι υπολογιστικές απαιτήσεις του NSFDA μπορούν να αυξηθούν σημαντικά, θέτοντας προκλήσεις για εφαρμογές πραγματικού χρόνου ή μεγάλης κλίμακας. Η υπολογιστική πολυπλοκότητα αποτελεί κεντρικό μέλημα του NSFDA, ιδίως λόγω του εγγενούς μηχανισμού δημιουργίας ανιχνευτών και της διαδικασίας αντιστοίχισής τους. Ο συνδυασμός του NSFDA με άλλους αλγορίθμους ή μεθόδους μπορεί να κατανείμει το υπολογιστικό φορτίο και να κάνει το συνολικό σύστημα πιο κλιμακούμενο. Σε μελλοντικές βελτιώσεις μπορούμε να δημιουργήσουμε ένα υβριδικό μοντέλο που να είναι σε θέση να χειριστεί τόσο το ανισόρροπο σύνολο δεδομένων όσο και το πρόβλημα του πραγματικού χρόνου, ώστε να έχουμε μια απάντηση κατά τη διάρκεια της εκτέλεσης της οικονομικής συναλλαγής, με βελτιωμένη ακρίβεια. Καθώς αλλάζουν τα δεδομένα σε πραγματικό χρόνο, θα πρέπει να εξελίσσονται και οι ανιχνευτές. Η Προσαρμοστική Μάθηση (Adaptive Learning) είναι μια προσθήκη που θα μπορεί να καθοδηγήσει τη δημιουργία ή την απόσυρση των ανιχνευτών με βάση το μεταβαλλόμενο τοπίο των δεδομένων.

Εν τέλει χρειάζεται περαιτέρω πρακτική μελέτη και πειραματισμός γύρω από άλλες μεθόδους και αλγόριθμους ΤΑΣ, ειδικά τεχνικές που έχουν να κάνουν με την Θεωρία Κινδύνου και τα δενδριτικά κύτταρα αλλά και τα ανοσοποιητικά δίκτυα.

Κεφάλαιο 7ο: Επίλογος

Αντλώντας έμπνευση από το βιολογικό ανοσοποιητικό σύστημα, τα Τεχνητά Ανοσοποιητικά Συστήματα έχουν αναδειχθεί ως ένα πολλά υποσχόμενο υπολογιστικό εργαλείο με ποικίλες εφαρμογές. Στο πλαίσιο του χρηματοπιστωτικού τομέα, όπου οι απάτες γίνονται όλο και πιο περίπλοκες, η ανάγκη για ευφυή και προσαρμοστικά συστήματα ανίχνευσης είναι υψίστης σημασίας. Το μοντέλο NSFDA, που αναπτύχθηκε στην παρούσα πτυχιακή εργασία, αποτελεί ένα βήμα προς τα εμπρός προς αυτή την κατεύθυνση.

Η ανάπτυξη και η εφαρμογή του NSFDA, που βασίζεται στις αρχές της θεωρίας της αρνητικής επιλογής, ανέδειξε τις δυνατότητες των ΤΑΣ στον τομέα της ανίχνευσης της οικονομικής απάτης. Η συγκριτική ανάλυση των αποτελεσμάτων των μοντέλων, υπέδειξε ότι το μοντέλο NSFDA υπερέχει όλων των άλλων μοντέλων μηχανικής μάθησης με μεγάλη διαφορά. Αυτό υπογραμμίζει την προσαρμοστικότητα και την ανθεκτικότητα των μοντέλων που βασίζονται στα ΤΑΣ όσον αφορά την αντιμετώπιση των προκλήσεων της ανίχνευσης απάτης.

Ενώ ο NSFDA αναδεικνύει τις δυνατότητες των ΤΑΣ στην ανίχνευση ανωμαλιών, υπάρχουν πάντα περιθώρια βελτίωσης. Οι μελλοντικές εργασίες μπορούν να επικεντρωθούν στην τελειοποίηση του αλγορίθμου, στην ενσωμάτωσή του με άλλα μοντέλα τεχνητής νοημοσύνης και μηχανικής μάθησης και στη διερεύνηση της δυνατότητας εφαρμογής του σε άλλους τομείς. Επιπλέον, καθώς το χρηματοπιστωτικό τοπίο συνεχίζει να εξελίσσεται, η συνεχής έρευνα θα είναι απαραίτητη για να διασφαλιστεί ότι τα συστήματα ανίχνευσης παραμένουν μπροστά από τους απατεώνες.

Εν κατακλείδι, ο δυναμικός κόσμος της οικονομικής απάτης απαιτεί εξίσου δυναμικές λύσεις. Το βιολογικό ανοσοποιητικό σύστημα, με την προσαρμοστικότητα και την ανθεκτικότητά του, προσφέρει ένα σχέδιο για την ανάπτυξη τέτοιων λύσεων. Αξιοποιώντας τη δύναμη των τεχνητών ανοσοποιητικών συστημάτων, μπορούμε να ανοίξουμε το δρόμο για ένα ασφαλέστερο οικονομικό μέλλον.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] A Abul K. Abbas, Andrew H. Lichtman, *Cellular and molecular immunology*, 5th ed. Saunders, Philadelphia, 2003.

[2] Charles A Janeway, Jr, Paul Travers, Mark Walport, and Mark J Shlomchik, *Immunobiology: The Immune System in Health and Disease, The Front Line of Host Defense*, 5th ed. New York: Garland Science, 2001.

[3] Richard A. Goldsby, Barbara Anne Osborne, Janis Kuby, Thomas J. Kindt, *Kuby Immunology*, 6th ed. New York: W.H. Freeman, 2007.

[4] Sulabha Pathak, Urmi Palan, *Immunology: Essential and Fundamental*, 2nd ed. Enfield, New Hampshire: Science Publishers, 2005.

[5] Fernando Nino, Dipankar Dasgupta, *Immunological Computation : Theory and Applications*, 1st ed. New York: Auerbach Publications, 2008.

[6] Jacqueline Stanley, *Essentials of Immunology and Serology*. Australia: Delmar Thomson Learning, 2002.

[7] J. H. Holland, "Using Classifier Systems to Study Adaptive Nonlinear Networks," in *Lectures in the Sciences of Complexity: Proceedings of the 1988 Complex Systems Summer School*, Santa Fe Institute., 1988.

[8] Stephanie Forrest, "A biologically inspired immune system for computers," in *Proceedings of Artificial Life IV: The Fourth International Workshop on the Synthesis and Simulation of Living Systems, MIT Press*, 1994.

[9] Jon Timmis & Paul S. Andrews, "A Beginners Guide to Artificial Immune Systems," in *In Silico Immunology*, Jon Timmis Darren Flower, Ed. Boston, MA: Springer, 2007, pp. 47-62.

[10] Paul S. Andrews, Nick D. L. Owens, Edward Clark, Jon Timmis, "An interdisciplinary perspectives on artificial immune systems," *Evolutionary Intelligence*, March 2008.

[11] Leandro Nunes de Castro, Jon Timmis, *Artificial Immune Systems: A New Computational Approach*. London, UK: Springer-Verlag, September 2002.

[12] A. Hone, T. Stibor, E. Clark, J. Timmis, "Theoretical advances in artificial immune systems," *Theoretical Computer Science*, vol. 403, no. 1, pp. 11-32, August 2008.

[13] Nivedita Majumdar, Senhua Yu, Dipankar Dasgupta, "MILA - Multilevel Immune Learning Algorithm," in *Conference: Genetic and Evolutionary Computation - GECCO 2003, Genetic and Evolutionary Computation Conference*, Chicago, IL, 2003.

[14] Steve Cayzer, Uwe Aickelin, "The Danger Theory and Its Application to Artificial Immune Systems," in *The 1st International Conference on Artificial Immune Systems (ICARIS)*, Canterbury, England, 2002.

[15] Uwe Aickelin, Steve Cayzer, Julie Greensmith, "Introducing Dendritic Cells as a Novel Immune-

Inspired Algorithm for Anomaly Detection," in *4th International Conference*, Banff, Alberta, Canada, 2005, pp. 153-167.

[16] Dipankar Dasgupta, Senhua Yu, "Conserved Self Pattern Recognition Algorithm," in *7th International Conference on Artificial Immune Systems, ICARIS*, Phuket, Thailand, 2008, pp. 279–290.

[17] Mário M. Freire, Paulo A.P. Fazendeiro, Pedro R.M. Inácio Diogo A.B. Fernandes, "Applications of artificial immune systems to computer security: A survey," *Journal of Information Security and Applications*, vol. 35, pp. 138-159, August 2017.

[18] Shouju Ren, Wenhuang Liu, Xiu Li, Bing Li, Lin Lei, Jianyong Tuo, "Artificial immune system for fraud detection," in *IEEE International Conference on Systems, Man and Cybernetics*, The Hague, The Netherlands, 2004.

[19] Guanzheng TAN, Mohamed Lamine Toure & Zeyad M. Alfawaer Dioubate Mamady, "An Artificial Immune System Based Multi-Agent Robotic Cooperation," in *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics*, 2008, pp. 60–67.

[20] Somesh Katta M. S. Prasasd Babu, "Artificial immune recognition systems in medical diagnosis," in *6th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, China, 2015, pp. 1082-1087.

[21] Susana C. Esquivel & Carlos A. Coello Victoria S. Aragón, "Artificial Immune System for Solving Dynamic Constrained Optimization Problems," in *Metaheuristics for Dynamic Optimization*, Amir Nakib, Patrick Siarry Enrique Alba, Ed.: Springer, 2013, pp. 225-263.

[22] N Av Mitchison, William E Paul, Arthur M Silverstein, David W Talmage, Martin G Weigert Melvin Cohn, "Reflections on the clonal-selection theory," *Nature Reviews Immunology*, vol. 7, no. 10, pp. 823–830, November 2007.

[23] Senhua Yu, Luis Fernando Nino, Dipankar Dasgupta, "Recent Advances in Artificial Immune Systems: Models and Applications," *Applied Soft Computing*, vol. 11, no. 2, pp. 1574-1587, March 2011.

[24] Jason Brownlee, "Clonal selection theory and Clonalg: the clonal selection classification algorithm (CSCA)," Swinburne University of Technology, Melbourne, Australia, Technical Report January 2005.

[25] Fernando J. Von Zuben, Leandro De Castro, "The Clonal Selection Algorithm with Engineering Applications," in *Workshop Proceedings, Workshop on Artificial Immune Systems and Their Applications*, Las Vegas, 2000.

[26] Jon Timmis, Leandro De Castro, *Artificial Immune Systems: A New Computational Intelligence Approach*.: Springer-Verlag, 2002.

[27] Jennifer A. White & Simon M. Garrett, "Improved Pattern Recognition with Artificial Clonal Selection," in *Artificial Immune Systems, Second International Conference, ICARIS* , Edinburgh, UK, 2003, pp. 181–193.

[28] Nor Azah Abdul Aziz, Fadhlina M Razali, Norita Md Norwawi, Nurlida Basir Roznim Mohamad Rasli, "A Preliminary Survey on Artificial Immune Systems (AIS): A Review on Their Techniques, Strengths and Drawbacks," *International Journal of Academic Research in Business and Social Sciences*, pp. 121-144, September 2019.

[29] Mamta Bhusry, Prashant Kamal Mishra, "Artificial Immune System: State of the Art Approach," *International Journal of Computer Applications*, vol. 120, no. 20, pp. 25-32, June 2015.

[30] Marek Kubale, Jacek Dabrowski, "Computer experiments with a parallel clonal selection algorithm for the Graph Coloring Problem," in *2008 IEEE International Symposium on Parallel and Distributed Processing*, Miami, FL, 2008, pp. 1-6.

[31] Giuseppe Nicosia, Mario Pavone Vincenzo Cutello, "Real coded clonal selection algorithm for unconstrained global optimization using a hybrid inversely proportional hypermutation operator," in *Proceedings of the 2006 ACM Symposium on Applied Computing (SAC)*, Dijon, France, 2006.

[32] Jon Timmis Emma Hart, "Application areas of AIS: The past, the present and the future," *Applied Soft Computing*, vol. 8, no. 1, pp. 191-201, January 2008.

[33] Fernando J. Von Zuben, Leandro De Castro, "Learning and Optimization Using the Clonal Selection Principle," *IEEE Transactions on Evolutionary Computation*, vol. 6, pp. 239 - 251, July 2002.

[34] Ana Pilar González-Rodríguez, Beatriz Suárez-Álvarez, Alejandro López-Soto, Leticia Huergo-Zapico, Carlos Lopez-Larrea Segundo Gonzalez, "Conceptual aspects of self and nonself discrimination," *Self/Nonself—Immune Recognition and Signaling*, pp. 19-25, January 2011.

[35] Andy M. Tyrrell, D. W. Bradley, "Immunotronics - Novel finite-state-machine architectures with build-in self-test using self-nonself differentiation," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 3, pp. 227-238, June 2002.

[36] Z. Ji & F. Gonzalez D. Dasgupta, "Artificial immune system (AIS) research in the last five years," in *The 2003 Congress on Evolutionary Computation*, Canberra, Australia, 2003.

[37] Dipankar Dasgupta Zhou Ji, "Revisiting Negative Selection Algorithms," *Evolutionary Computation*, vol. 15, no. 2, pp. 223–251, June 2007.

[38] Dat Tran, Dharmendra Sharma Wanli Ma, "Negative selection as a means of discovering unknown temporal patterns," in *ICIS 2010: International Conference on Intelligent Systems*, Tokyo, Japan, 2010.

[39] A.S. Perelson, L. Allen, R. Cherukuri S. Forrest, "Self-nonself discrimination in a computer," in *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press*, Oakland, CA, USA, 1994.

[40] Jian Zhang, Jingjing Ma, Licheng Jiao Maoguo Gong, "An efficient negative selection algorithm with further training for anomaly detection," *Knowledge-Based Systems*, vol. 30, pp. 185-191, June 2012.

[41] Ming-hong LIAO, Gang XIAO Zhang-zan JIN, "Survey of negative selection algorithms,"

Journal on Communications, vol. 34, no. 1, pp. 159-170, 2013.

[42] Xiaojie Liu, Tao Li, Caiming Liu, Lingxi Peng, Feixian Sun Jinquan Zeng, "A self-adaptive negative selection algorithm used for anomaly detection," *Progress in Natural Science*, vol. 19, no. 2, pp. 261-266, February 2009.

[43] Liang Gao, Xinyu Li, Hui Li Long Wen, "A new genetic algorithm based evolutionary neural architecture search for image classification," *Swarm and Evolutionary Computation*, December 2022.

[44] A. A. S., Hatim, M. A. K., & Nabil, A. I. Khaled, "Artificial immune clonal selection classification algorithms for classifying malware and benign processing using API call sequences," *International Journal of Computer Science and Network Security (IJCSNS)*, 2010.

[45] Klaus Eichmann, "The idiotypic network theory," in *The Network Collective*.: Birkhäuser, 2008, pp. 82–94.

[46] Jon Timmis, Ennise Cooke, Mark Neal & Clive King John Hunt, "Jisys: The Envelopment of an Artificial Immune System for Real World Applications," in *Artificial Immune Systems and Their Applications*, Dipankar Dasgupta, Ed., 1999, pp. 157–186.

[47] Emma Hart & Peter Ross, "Studies on the Implications of Shape-Space Models for Idiotypic Networks," in *International Conference on Artificial Immune Systems*, 2004, pp. 413–426.

[48] Polly Matzinger, "The danger model: a renewed sense of self," *SCIENCE*, vol. 296 , no. 5566, April 2002.

[49] Melvin Cohn, Peter Bretscher, "A Theory of Self-Nonself Discrimination," *SCIENCE*, vol. 169 , no. 3950, September 1970.

[50] Polly Matzinger, "Tolerance, danger, and the extended family," *Annual Review of Immunology*, vol. 12, 1994.

[51] Uwe Aickelin, Jamie Twycross, Julie Greensmith, "Articulation and Clarification of the Dendritic Cell Algorithm," in *International Conference on Artificial Immune Systems*, 2006, pp. 404–417.

[52] Lain Bate, Nicholas Lay, "Applying artificial immune systems to real-time embedded systems," in *IEEE Congress on Evolutionary Computation*, Singapore, 2007, pp. 3743-3750.

[53] Uwe Aickelin, Jamie Twycross, Julie Greensmith, "Detecting Danger: Applying a Novel Immunological Concept to Intrusion Detection Systems," in *6th International Conference in Adaptive Computing in Design and Manufacture (ACDM 2004 Poster)*, Bristol, UK, 2004.

[54] Fernando Niño, Gerardo Quintana, Camilo Eduardo Prieto, "A goalkeeper strategy in robot soccer," in *2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence)*, Hong Kong, China, 2008, pp. 3443-3447.

[55] Michael C. Ehrhardt, Eugene F. Brigham, *Financial Management: Theory & Practice*, 15th ed.: Cengage Learning, 2013.

[56] S. Andrew Gadsden, John Yawney, Waleed Hilal, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Systems with Applications*, vol. 193,

December 2021.

[57] Kyungho Lee, Dahee Choi, "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation," *Security and Communication Networks*, vol. 2018, September 2018.

[58] Yong Hu, Y.H. Wong, Yijun Chen, Xin Sun, E.W.T. Ngai, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems*, vol. 50, no. 3, pp. 559-569, February 2011.

[59] Javier Gimeno, Santiago Moral-Rubio, Sergio Muñoz-Romero, José-Luis Rojo-Álvarez, Jacobo Chaquet, "On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis through Interpretable Autoencoders," *Applied Sciences*, vol. 12, April 2022.

[60] Pritheega Magalingam, Khaled Gubran Al-Hashedi, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Computer Science Review*, vol. 40, May 2021.

[61] (2010-2011, October 1, 2009 – September 30, 2011) FBI, Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Year, Department of Justice, United States. [Online]. https://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011

[62] FBI, Federal Bureau of Investigation, White-Collar Crime. [Online]. https://www.fbi.gov/investigate/white-collar-crime

[63] Sanjeev Jha, Kurian Tharakunnel, J. Christopher Westland, Siddhartha Bhattacharyya, "Data mining for credit card fraud: A comparative study.," *Decision Support Systems*, vol. 50, no. 3, pp. 602-613, February 2011.

[64] Vadlamani Ravi, G. Raghava Rao, Indranil Bose, Ravi Sankar Pediredla, "Detection of financial statement fraud and feature selection using data mining techniques," *Decision Support Systems* , vol. 50, no. 2, pp. 491-500, January 2011.

[65] Surya B Yadav, Fletcher H. Glancy, "A computational model for financial reporting fraud detection," *Decision Support Systems*, vol. 50, no. 3, pp. 595-601, February 2011.

[66] Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, Sam Maes, "Credit card fraud detection using Bayesian and neural networks," in *Proceedings of the First International NAISO Congress on NEURO FUZZY THECHNOLOGIES*, Havana, Cuba, 2002.

[67] Andrew Bloomenthal. (2019) Detecting Financial Statement Fraud. [Online]. https://www.investopedia.com/articles/financial-theory/11/detecting-financial-fraud.asp

[68] Roberto Henriques, Petr Hájek, "Mining Corporate Annual Reports for Intelligent Detection of Financial Statement Fraud – A Comparative Study of Machine Learning Methods," *Knowledge-Based Systems*, pp. 139–152, May 2017.

[69] S. Dhivya Murugan, Shanmuham Anbarasi, "Fraud detection using outlier predictor in health insurance data," in *International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, 2017, pp. 1-6.

[70] Suvasini Panigrahi, Sharmila Subudhi, "Effect of Class Imbalanceness in Detecting Automobile Insurance Fraud," in *2nd International Conference on Data Science and Business Analytics (ICDSBA)*, ChangSha, China, 2018, pp. 528-531.

[71] Legal Alerts. (2023, March) Insurance Fraud Costs the U.S. $308 Billion Annually. [Online]. https://www.conroysimberg.com/blog/insurance-fraud-costs-the-u-s-308-billion-annually/

[72] Wei Xu, Xinting Huang, Kunlin Yang, Qili Wang, "Enhancing Intraday Stock Price Manipulation Detection by Leveraging Recurrent Neural Networks with Ensemble Learning," *Neurocomputing*, vol. 347, pp. 46-58, June 2019.

[73] Sheikh Khaled Ghafoor, William Eberle, Sheikh Rabiul Islam, "Mining Illegal Insider Trading of Stocks: A Proactive Approach," in *2018 IEEE International Conference on Big Data*, Seattle, WA, USA, 2018.

[74] Sami Abu-El-Haija, Fred Morstatter, Greg Ver Steeg, Aram Galstyan, Mehrnoosh Mirtaheri, "Identifying and Analyzing Cryptocurrency Manipulations in Social Media," in *IEEE Transactions on Computational Social Systems*, 2019, pp. 607–617.

[75] Xidi Wang, Alair Pereira do Lago, Manoel Fernando Alonso Gadi, "Credit Card Fraud Detection with Artificial Immune System," in *International Conference on Artificial Immune Systems*, Phuket, Thailand, 2008, pp. 119–131.

[76] Suvasini Panigrahi, Shamik Sural, Arun K. Majumdar, Amlan Kundu, "BLAST-SSAHA hybridization for credit card fraud detection," *IEEE Transactions on Dependable and Secure Computing* , vol. 6, no. 4, pp. 309-315, October 2009.

[77] Jane Cahill, Peter Keenan, Daniel Walsh, Anthony Brabazon, "Identifying online credit card fraud using Artificial Immune Systems," in *IEEE Congress on Evolutionary Computation*, 2010.

[78] M. Krivko, "A hybrid model for plastic card fraud detection systems," *Expert Systems with Applications*, vol. 37, no. 8, pp. 6070-6076, August 2010.

[79] Sanjeev Jha, Kurian Tharakunnel, J. Christopher Westland, Siddhartha Bhattacharyya, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602-613, February 2011.

[80] Pradeep Ray, Greg Stephens, Lundy Lewis Nicholas Wong, "Artificial immune systems for the detection of credit card fraud: An architecture, prototype and preliminary results," *Information Systems Journal*, vol. 22, no. 1, pp. 53-76, February 2011.

[81] Mohammad Kazem, Akbari Neda, Soltani Halvaiee, "A novel model for credit card fraud detection using Artificial Immune Systems," *Applied Soft Computing*, vol. 24, pp. 40-49, November 2014.

[82] Thomas Kiehl, Christina Lacomb, Deniz Senturk Bethany Hoogs, "A genetic algorithm approach to detecting temporal patterns indicative of financial statement fraud," *Intelligent Systems in Accounting Finance & Management*, vol. 15, pp. 41-56, July 2007.

[83] Kevin C. Moffitt, Mary B. Burns, Judee K. Burgoon, William F. Felix Sean L. Humpherys, "Identification of fraudulent financial statements using linguistic credibility analysis," *Decision*

Support Systems, vol. 50, no. 3, pp. 585-594, February 2011.

[84] Cuneyt Asuk, Melih Kirlidog, "A Fraud Detection Approach with Data Mining in Health Insurance," *Procedia - Social and Behavioral Sciences*, vol. 62, pp. 989-994, October 2012.

[85] Mengzhuo You, Hao Peng, "The Health Care Fraud Detection Using the Pharmacopoeia Spectrum Tree and Neural Network Analytic Contribution Hierarchy Process," in *IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, 2016, pp. 2006-2011.

[86] Ahmed Imran Hunjra, Zied Ftiti, Wael Louhichi, Tahira Shams, Faheem Aslam, "Insurance fraud detection: Evidence from artificial intelligence and machine learning," *Research in International Business and Finance*, vol. 62, 2022.

[87] H. Tawfik, A.K. Nagar, R. Huang, "A novel hybrid artificial immune inspired approach for online break-in fraud detection," *Procedia Computer Science*, vol. 1, no. 1, pp. 2733-2742, May 2010.

[88] Vukosi Marivate, Bhesipho Twala, Patrick M. Monamo, "A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers," in *15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Anaheim, CA, USA, 2016, pp. 188-194.

[89] Dongming Xu, Huaiqing Wang, Yingfeng Wang, Shijia Gao, "Intelligent Anti-Money Laundering System," in *2006 IEEE International Conference on Service Operations and Logistics, and Informatics*, Shanghai, China, 2006, pp. 851-856.

[90] Ximi Wang, Junjie Zhang, Peng Zhang, Lili Liu, Huan Jin, Hongbo Jin, Yadong Zhou, "Analyzing and Detecting Money-Laundering Accounts in Online Social Networks," *IEEE Network*, vol. 32, no. 3, pp. 115-121, May 2018.

[91] Angoss KnowledgeSEEKER® and KnowledgeSTUDIO® Version 8.0. [Online]. https://www.prnewswire.com/news-releases/angoss-knowledgeseeker-and-knowledgestudio-version-80-151517245.html

[92] Kaggle - Dataset to predict Vehicle Insurance Fraud by Angoss Knowledge Seeker. [Online]. https://www.kaggle.com/datasets/khusheekapoor/vehicle-insurance-fraud-detection

[93] Kaggle - Anonymized credit card transactions labeled as fraudulent or genuine. [Online]. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud?page=2

[94] Machine Learning Group (MLG). [Online]. https://mlg.ulb.ac.be/wordpress/

[95] scikit-learn. [Online]. https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.StandardScaler.html

[96] Wagner Meira Jr, Mohammed J. Zaki, *Data Mining and Analysis: Fundamental Concepts and Algorithms*, 1st ed.: Cambridge University Press, 2014.

[97] XGBoost Documentation. [Online]. https://xgboost.readthedocs.io/en/stable/

[98] scikit-learn. [Online]. https://scikit-learn.org/stable/auto_examples/model_selection/plot_precision_recall.html

[99] Kevin H. Eng, C. David Page, Kendrick Boyd, "Area under the Precision-Recall Curve: Point Estimates and Confidence Intervals," in *Machine Learning and Knowledge Discovery in Databases*, Berlin, Heidelberg, 2013, pp. 451–466.