ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΜΣ «ΕΠΙΣΤΗΜΗ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑ ΥΠΟΛΟΓΙΣΤΩΝ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αξιοποίηση αποθηκευμένων δεδομένων σε περιβάλλοντα blockchain από εφαρμογές αλγορίθμων Μηχανικής Μάθησης

Τσιώμος Κωνσταντίνος

Α.Μ.: 2022202102019

Επιβλέπων:

Καθηγητής Βασιλάκης Κωνσταντίνος

Τρίπολη, Μάιος 2024

Πίνακας περιεχομένων

Πίνακας εικόνων

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει την αξιοποίηση δεδομένων που έχουν αποθηκευτεί σε περιβάλλοντα blockchain από εφαρμογές αλγορίθμων Μηχανικής Μάθησης. Με την αυξανόμενη σημασία της ασφάλειας των δεδομένων και της ιδιωτικότητας, η διαλειτουργικότητα μεταξύ της τεχνολογίας blockchain και των αλγορίθμων Μηχανικής Μάθησης και ο συνδυασμός τους ανοίγουν νέες προοπτικές για την ανάπτυξη ασφαλών, διαφανών, και αποτελεσματικών εφαρμογών.

Στο πλαίσιο αυτό, η εργασία αναλύει τις βασικές έννοιες της Μηχανικής Μάθησης και της κρυπτογραφίας, εξετάζοντας τη χρήση της ομομορφικής κρυπτογραφίας ως έναν τρόπο προστασίας της απορρήτου των δεδομένων. Επιπλέον, παρουσιάζει την τεχνολογία blockchain και τα χαρακτηριστικά της, συμπεριλαμβανομένων των έξυπνων συμβολαίων και των αποκεντρωμένων εφαρμογών.

Το κύριο μέρος της εργασίας εξετάζει την αξιοποίηση των ομομορφικών αλγορίθμων σε δεδομένα blockchain για εφαρμογές Μηχανικής Μάθησης. Μέσα από μια ανάλυση του σημερινού τοπίου και των προκλήσεων, εξετάζονται επίσης διάφορα πεδία εφαρμογής, όπως η υγεία, ο χρηματοπιστωτικός τομέας, η εφοδιαστική αλυσίδα, η δημόσια διοίκηση και η ενέργεια.

Η εργασία αυτή προσφέρει μια συνεκτική εικόνα του πώς η Μηχανική Μάθηση και η τεχνολογία blockchain μπορούν να συνδυαστούν για την ανάπτυξη πρωτοποριακών λύσεων που αξιοποιούν με ασφαλή τρόπο τα δεδομένα σε διάφορους τομείς. Τέλος, η εργασία παρουσιάζει μια ενδεικτική προοπτική για το μέλλον της έρευνας και της ανάπτυξης σε αυτό τον αναδυόμενο τομέα.

Abstract

This thesis examines the exploitation of data stored in blockchain environments by machine learning algorithms. With the increasing importance of data security and privacy, the interoperability between blockchain technology and machine learning algorithms, as well as their cooperation, create new potential for the development of secure, transparent, and efficient applications.

In this context, this thesis analyses the basic concepts of machine learning and cryptography, examining the use of homomorphic cryptography as a means for the protection of data secrecy. Furthermore, it presents the blockchain technology and its characteristics, including smart contracts and decentralized applications.

The main part of this thesis examines the exploitation of homomorphic algorithms on blockchain data for machine learning applications. Through an analysis of the current state of the field and the related challenges, different areas of application are also considered including health, finance, logistics, public administration and energy.

This thesis presents a concise view on how machine learning and blockchain technology can be combined towards the development of innovative solutions which utilize data in a safe fashion, across different sectors. Finally, the thesis presents an indicative outlook regarding the future of research and development in this emerging field.

1 Εισαγωγή

Η προοδευτική εξέλιξη στις τεχνολογίες, κυρίως τις τελευταίες δεκαετίες, έχει διαμορφώσει ένα περιβάλλον όπου τα δεδομένα και οι πληροφορίες αποκτούν αυξανόμενη σημασία σε όλα τα πεδία των ανθρώπινων δραστηριοτήτων. Η συλλογή, αποθήκευση και ανάλυση δεδομένων έχουν γίνει πλέον αναπόσπαστο μέρος της σύγχρονης κοινωνίας, επηρεάζοντας την οικονομία, την επιστήμη, την ιατρική, την εκπαίδευση και πολλούς άλλους τομείς. Η Μηχανική Μάθηση αναδεικνύεται ως ένα ισχυρό εργαλείο που επιτρέπει την αυτόματη ανάλυση και την εξαγωγή πληροφοριών από αυτά τα δεδομένα. Παράλληλα, η κρυπτογραφία και η τεχνολογία Blockchain έχουν εισαχθεί ως ασφαλείς μέθοδοι για την αποθήκευση και την διαχείριση πληροφοριών, προσφέροντας διαφάνεια, ακεραιότητα και ασφάλεια στις διαδικασίες αποθήκευσης και μεταφοράς δεδομένων. Στο πλαίσιο αυτό, αυτή η εργασία εξετάζει την αξιοποίηση δεδομένων που έχουν αποθηκευτεί σε περιβάλλοντα Blockchain από εφαρμογές αλγορίθμων Μηχανικής Μάθησης, με στόχο την αξιοποίηση αυτού του συνδυασμού τεχνολογιών για την ανάπτυξη καινοτόμων λύσεων σε ποικίλους τομείς, προωθώντας την ασφάλεια, την αποτελεσματικότητα και τη διαφάνεια στην επεξεργασία δεδομένων.

1.1 Σκοπός της έρευνας

Βασικός στόχος αυτής της έρευνας είναι να αναδείξει τον τρόπο με τον οποίο τα μοντέλα Μηχανικής Μάθησης μπορούν να χρησιμοποιηθούν αποτελεσματικά και σε συνέργεια με ομομορφικούς αλγορίθμους για την ανάλυση και την αξιοποίηση δεδομένων που αποθηκεύονται σε περιβάλλοντα Blockchain, αναζητώντας τρόπους για να αξιοποιήσει το δυναμικό των συγκεκριμένων τεχνολογιών.

Η έρευνα μελετά τη δυνατότητα χρήσης ομομορφικής κρυπτογραφίας για την ασφαλή ανάλυση δεδομένων σε ένα περιβάλλον Blockchain και εξετάζει την αποδοτικότητα και την αποτελεσματικότητα αυτής της προσέγγισης. Τα αποτελέσματα αυτής της έρευνας μπορούν να εφαρμοστούν σε διάφορους τομείς, όπως η υγεία, ο χρηματοπιστωτικός τομέας, η εφοδιαστική αλυσίδα και η δημόσια διοίκηση, προσφέροντας νέες δυνατότητες για την αξιοποίηση των δεδομένων και την επίλυση προβλημάτων πραγματικού κόσμου.

Παράλληλα, η έρευνα αναγνωρίζει τις προκλήσεις που προκύπτουν κατά την εφαρμογή εξεταζόμενων τεχνολογιών. Αυτές οι προκλήσεις περιλαμβάνουν τη διαφορετική δομή και την ασφάλεια των δεδομένων σε ένα περιβάλλον Blockchain, την εκτέλεση αλγορίθμων Μηχανικής Μάθησης σε κρυπτογραφημένα δεδομένα, και την αποτελεσματική διαχείριση της απόδοσης και της ιδιωτικότητας των μοντέλων Μηχανικής Μάθησης.

Με την ολοκλήρωση αυτής της έρευνας, προτείνονται λύσεις για εφαρμογή σε βασικούς τομείς της ανθρώπινης δραστηριότητας, με την ελπίδα να προσφερθεί νέο όραμα για τη συνδυασμένη χρήση της Μηχανικής Μάθησης και κρυπτογραφικών τεχνολογιών, προωθώντας την ανάπτυξη καινοτόμων εφαρμογών που μπορούν να ωφελήσουν την κοινωνίας και την επιχειρηματικότητας, σε μια εποχή που η αξιοποίηση των δεδομένων είναι πρωταρχικής σημασίας.

1.2 Δομή της Εργασίας

Η παρούσα εργασία πραγματεύεται την αξιοποίηση κρυπτογραφικών τεχνολογιών, και πιο συγκεκριμένα των ομομορφικών αλγορίθμων και του Blockchain, από μοντέλα Μηχανικής Μάθησης. Για την καλύτερη απόδοση και κατανόηση του περιεχόμενου, η εργασία έχει χωριστεί σε επτά (7) κεφάλαια στα οποία παρουσιάζονται κλιμακωτά όλες τις απαραίτητες πληροφορίες.

Στο πρώτο κεφάλαιο, γίνεται μια εισαγωγή στην Μηχανική Μάθηση, η οποία περιλαμβάνει μία ιστορική αναδρομή που αναδεικνύει την πορεία της ανθρωπότητας προς την ανάπτυξη αυτής της τεχνολογίας. Ξεκινώντας από ένα απλό εργαλείο, εξετάζονται τα στάδια εξέλιξης που οδήγησαν στην ανάπτυξη του αυτόματου ελέγχου και, τελικά, στα ευφυή συστήματα. Παράλληλα, παρουσιάζονται ορισμένες βασικές τεχνικές της Τεχνητής Νοημοσύνης προκειμένου να δοθεί στον αναγνώστη μια συνολική εικόνα για τον τρόπο εφαρμογής αυτής της τεχνολογίας ως σύγχρονο εργαλείο.

Στο δεύτερο κεφάλαιο, πραγματοποιείται μία εισαγωγή στο πεδίο της κρυπτογραφίας, παρέχοντας μια επισκόπηση της εξέλιξής της μέσα από την ιστορία, όπου αναπτύχθηκε αυτή η τεχνολογία ξεκινώντας με τη χρήση απλών εργαλείων μέχρι την εμφάνιση προηγμένων αλγορίθμων κρυπτογράφησης. Επιπλέον, παρουσιάζονται οι βασικές έννοιες της κρυπτογραφίας καθώς και η σύγχρονη εξέλιξή της. Επίσης, αναλύονται οι κύριοι αλγόριθμοι κρυπτογράφησης που αποτελούν βασικά εργαλεία στη διατήρηση της ασφάλειας των δεδομένων.

Στο τρίτο κεφάλαιο της εργασίας, γίνεται αναφορά στην Ομομορφική Κρυπτογραφία, μια σημαντική τεχνική που επιτρέπει την ασφαλή επεξεργασία δεδομένων σε κρυπτογραφημένη μορφή. Σε αυτό το κεφάλαιο, παρουσιάζεται μια σύνοψη της Ομομορφικής Κρυπτογραφίας και των σχετικών αλγορίθμων, εισάγοντας τα κυριότερα στοιχεία για αυτή τη σημαντική περιοχή του τομέα της Κρυπτογραφίας.

Το τέταρτο κεφάλαιο, εστιάζει στην τεχνολογία του Blockchain, παρουσιάζοντας τις ιδιότητες, τις λειτουργίες και τα πλεονεκτήματα της τεχνολογίας αυτής.

Στο πέμπτο κεφάλαιο εξετάζεται η αξιοποίηση των ομομορφικών αλγορίθμων σε δεδομένα που αποθηκεύονται σε περιβάλλοντα Blockchain για εφαρμογές Μηχανικής Μάθησης. Στο κεφάλαιο αυτό γίνεται ανασκόπηση της έρευνας που σχετίζεται με τη συνδυασμένη χρήση των ομομορφικών αλγορίθμων και της τεχνολογίας Blockchain στον τομέα της Μηχανικής Μάθησης. Στην έκταση αυτού του κεφαλαίου εξετάζονται και οι προκλήσεις που οδηγούν στην ανάγκη για αυτήν την έρευνα και παρουσιάζονται συγκεκριμένα πεδία εφαρμογής.

Στο έκτο κεφάλαιο της εργασίας, δίνεται έμφαση στην ανάπτυξη καινοτόμων λύσεων στον χώρο της τομής μεταξύ Τεχνητής Νοημοσύνης και κρυπτογραφικών τεχνολογιών. Παρουσιάζονται προοπτικές που εξετάζουν πώς αυτός ο χώρος μπορεί να συνεισφέρει σε καινοτόμες εφαρμογές και στην αντιμετώπιση προκλήσεων που σχετίζονται με την αποτελεσματική υλοποίησή των εφαρμογών και καταγράφονται μερικές ενδεικτικές λύσεις που κρίνονται πρόσφορες για περαιτέρω έρευνα και ανάπτυξη.

Στο τελευταίο κεφάλαιο της εργασίας, ανακεφαλαιώνονται τα κύρια ευρήματα και συμπεράσματα που προέκυψαν κατά τη διάρκεια της έρευνας. Σε αυτό το κεφάλαιο, παρουσιάζεται μια σύνοψη της σημασίας της συνδυασμένης χρήσης της τεχνητής νοημοσύνης, της κρυπτογραφίας και της τεχνολογίας Blockchain στον σύγχρονο ψηφιακό κόσμο, και πώς αυτοί οι τομείς μπορούν δημιουργήσουν μια νέα δυναμική και να οδηγήσουν τις εξελίξεις στην καινοτομία, μετασχηματίζοντας το τεχνολογικό τοπίο τα επόμενα χρόνια.

2 Μηχανική Μάθηση

2.1 Κατηγορίες μάθησης

Η Μηχανική Μάθηση αποτελεί αντικείμενο της επιστήμης υπολογιστών και λειτουργεί ως εργαλείο για τον εντοπισμό και την αναγνώριση μοτίβων αλλά και την ανάλυση δεδομένων. Οι αλγόριθμοι Μηχανικής Μάθησης "μαθαίνουν" από διαθέσιμα σύνολα δεδομένων (datasets) τα οποία αφορούν ένα αντικείμενο μελέτης. Στη συνέχεια τα μοντέλα αυτά μπορούν να επιστρέψουν ιδιαίτερα ακριβή αποτελέσματα ή προβλέψεις, βασιζόμενα στη γνώση που αποκόμισαν από τα σύνολα δεδομένων εκπαίδευσης (*μτφρ.* training datasets). Οι βασικότερες κατηγορίες εκπαίδευσης των αλγορίθμων είναι:

1. **Επιτηρούμενη Μάθηση** (*μτφρ. Supervised Learning*) Το μοντέλο τίθεται υπό καθεστώς εκπαίδευσης, δεχόμενο ένα σύνολο δεδομένων που περιέχει παραδειγματικές εισόδους, όπου κάθε μία από αυτές συνοδεύεται από τα αντίστοιχα επιθυμητά αποτελέσματα (μία *ετικέτα* [label] που αντιστοιχίζει την είσοδο σε μία κατηγορία, ένα αριθμητικό αποτέλεσμα κ.λπ.). Σκοπός της εκπαιδευτικής διαδικασίας είναι να εκπαιδευτεί το μοντέλο ώστε να "μάθει" ένα γενικό μοτίβο (κανόνα) και να παρέχει ακριβή αποτελέσματα για κάθε νέα είσοδο (ή σύνολο νέων εισόδων).
2. **Μη Επιτηρούμενη Μάθηση** (*μτφρ. Unsupervised Learning*): Το μοντέλο που τίθεται υπό καθεστώς εκπαίδευσης καλείται να ανακαλύψει από μόνο του μοτίβα εντός των παραδειγματικών δεδομένων εισόδου, χωρίς να του έχει χορηγηθεί κάποια πρότερη γνώση με τη μορφή των επιθυμητών αποτελεσμάτων που να έχουν αντιστοιχηθεί στις παραδειγματικές εισόδους (Usama et al., 2019).
3. Οι διαδικασίες της επιτηρούμενης και της μη επιτηρούμενης μάθησης μπορούν να συνδυαστούν σε μία διαδικασία **Ημι-επιτηρούμενης Μάθησης** (*μτφρ. Semi-supervised Learning*) (Cunningham, Cord and Delany 2008). Η ημι-επιτηρούμενη μάθηση χρησιμοποιείται ιδίως σε περιπτώσεις όπου το σύνολο δεδομένων εκπαίδευσης δεν είναι επαρκώς εκτενές (π.χ. λόγω απουσίας μεγάλου αριθμού δεδομένων εισόδου τα οποία συνοδεύονται με το αντίστοιχο επιθυμητό αποτέλεσμα), και συνδυάζει τις ετικέτες που έχουν παρασχεθεί σε (περιορισμένα) δεδομένα εισόδου με τα μοτίβα που εξάγονται από τα δεδομένα τα οποία δεν συνοδεύονται από ετικέτες.
4. **Ενισχυτική Μάθηση** (*μτφρ. Reinforcement Learning*): Το υπό εκπαίδευση μοντέλο "τοποθετείται" εντός ενός δυναμικού περιβάλλοντος και καλείται να αλληλεπιδράσει με αυτό, ώσπου να επιτευχθεί ένας προκαθορισμένος στόχος. Σε αυτή την κατηγορία εκπαίδευσης δεν ορίζονται εξ αρχής οι διαδικασίες με τις οποίες το μοντέλο θα φτάσει στον προκαθορισμένο στόχο αλλά επιβραβεύεται κάθε φορά που πλησιάζει όλο και περισσότερο σε αυτόν. Το μοντέλο αξιοποιεί τις πληροφορίες επιβράβευσης που λαμβάνει, συνήθως εν είδει βαθμολογίας, για να αναπροσαρμόζει καταλλήλως τη λειτουργία του και να επιτυγχάνει καλύτερες επιδόσεις ώσπου να φτάσει στη βέλτιστη επιθυμητή λύση (Kaelbling, Littman and Moore 1996).

Ως κλάδος, η Μηχανική Μάθηση διαθέτει πληθώρα μεθόδων επίλυσης προβλημάτων, με κάθε μία εξ αυτών να ανταποκρίνεται καλύτερα σε διαφορετικούς τύπους προβλημάτων. Κατά την εκπαίδευσή του, κάθε αλγόριθμος συνοδεύεται από ποιοτικά χαρακτηριστικά που περιγράφουν την αποτελεσματικότητά του, όπως για παράδειγμα τα ποσοστά ακριβείας, το ποσοστό σφάλματος, ο

πίνακας σύγχυσης, κ.λπ. Η αποτελεσματικότητα ενός μοντέλου εξαρτάται αφενός από την ποιότητα και την ποσότητα των δεδομένων εκπαίδευσης, και αφετέρου από την επιλογή του κατάλληλου αλγορίθμου εκπαίδευσης ο οποίος οφείλει να είναι ορθώς παραμετροποιημένος ώστε να ανταποκρίνεται αποτελεσματικά στις ανάγκες του προβλήματος.

2.2 Κατηγορίες αλγορίθμων Μηχανικής Μάθησης

Η Μηχανική Μάθηση περιλαμβάνει μια πληθώρα αλγορίθμων που επιτρέπουν στους υπολογιστές να μάθουν από τα δεδομένα και να κάνουν προβλέψεις ή να ταξινομήσουν τις πληροφορίες. Η μηχανική μάθηση ενσωματώνει διάφορους τύπους αλγορίθμων, όπως οι αλγόριθμοι παλινδρόμησης (regression), ταξινόμησης (classification), ομαδοποίησης (clustering), εξελικτικούς αλγόριθμους (evolutionary algorithms) και τεχνητά νευρωνικά δίκτυα (artificial neural networks).

Οι αλγόριθμοι παλινδρόμησης στοχεύουν στην πρόβλεψη ενός συνεχούς στόχου με βάση ένα ή περισσότερα χαρακτηριστικά, ενώ οι αλγόριθμοι ταξινόμησης ασχολούνται με τον καθορισμό της κατηγορίας στην οποία ανήκει ένα δεδομένο. Από την άλλη πλευρά, οι αλγόριθμοι ομαδοποίησης αναζητούν δομές και ομάδες μέσα στα δεδομένα χωρίς να έχουν προηγούμενες ετικέτες συσχετισμένες με τα δεδομένα. Οι εξελικτικοί αλγόριθμοι, εμπνευσμένοι από τη βιολογική εξέλιξη, εφαρμόζουν προσομοιώσεις επιλογής, διασταύρωσης και μετάλλαξης για να βρουν λύσεις σε προβλήματα βελτιστοποίησης. Τέλος, τα τεχνητά νευρωνικά δίκτυα είναι μαθηματικά μοντέλα εμπνευσμένα από τη δομή και τη λειτουργία του ανθρώπινου εγκεφάλου, και χρησιμοποιούνται για πολύπλοκες διεργασίες μάθησης και πρόβλεψης (Ayodele 2010).

Μέσα από αυτούς τους αλγορίθμους, η μηχανική μάθηση ανακαλύπτει γνώση και παρέχει σημαντικές προοπτικές σε πολλούς τομείς της τεχνολογίας και της επιστήμης. Στις επόμενες παραγράφους παρουσιάζονται αναλυτικότερα οι ανωτέρω αναφερθείσες κατηγορίες.

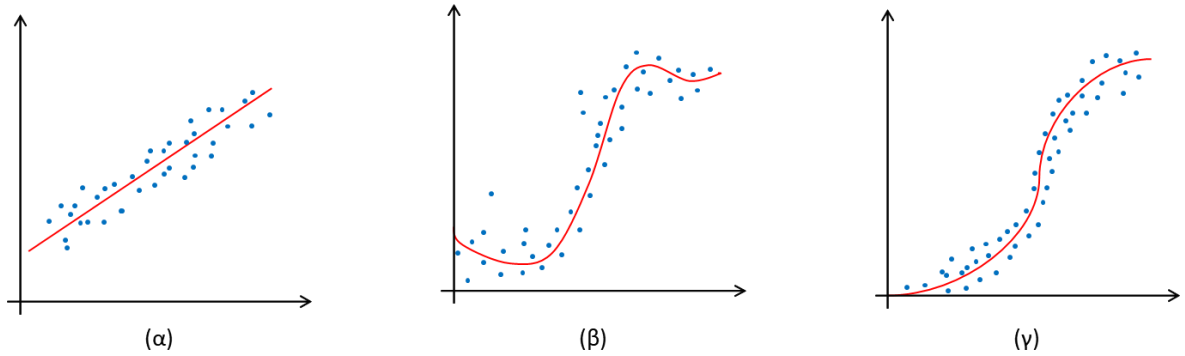
2.2.1 Παλινδρόμηση (Regression)

Το πεδίο της Στατιστικής που μελετά τις σχέσεις μεταξύ ενός πλήθους μεταβλητών με σκοπό την πρόβλεψη μίας εξ αυτών, ονομάζεται Ανάλυση Παλινδρόμησης (*μτφρ. Regression Analysis*). Στη Μηχανική Μάθηση, η σχετική εκπαιδευτική διαδικασία καλείται απλά Παλινδρόμηση (*μτφρ. Regression*).

Η Παλινδρόμηση αποτελεί μία μέθοδο επιτηρούμενης μηχανικής μάθησης. Σκοπός της είναι, μέσω ενός συνόλου δεδομένων, να οδηγήσει το μοντέλο στην ανακάλυψη μίας μαθηματικής συνάρτησης **f** η οποία, μετά το πέρας της εκπαίδευσης, θα χρησιμοποιείται από το μοντέλο για να προβλέπει με ακρίβεια εξόδους για κάθε νέο σύνολο εισόδων που θα εισέρχονται σε αυτό. Η μέθοδος της Παλινδρόμησης περιλαμβάνει μεθόδους γραμμικής παλινδρόμησης (όπου η συνάρτηση **f** παριστάνεται στο καρτεσιανό επίπεδο με μία ευθεία), μη γραμμικής παλινδρόμησης (όπου η συνάρτηση **f** παριστάνεται στο καρτεσιανό επίπεδο με μία καμπύλη) ή ακόμη και μεθόδους όπου σχηματίζονται και υπερεπίπεδα (Maulud and Abdulazeez 2020).

Ως προς το πλήθος των μεταβλητών στα δεδομένα εισόδου, η Παλινδρόμηση χωρίζεται σε δύο υποκατηγορίες: την απλή και την πολλαπλή. Η απλή Παλινδρόμηση χρησιμοποιεί μία μόνο ανεξάρτητη μεταβλητή εισόδου για να προβλέψει την εξαρτημένη μεταβλητή εξόδου, ενώ στην πολλαπλή Παλινδρόμηση, οι ανεξάρτητες μεταβλητές είναι περισσότερες από μία.

Οι κυριότεροι τύποι Παλινδρόμησης, είναι η Γραμμική Παλινδρόμηση (**Εικόνα 2.1α**), η Πολυωνυμική (**Εικόνα 2.1β**) και η Λογιστική[1] (**Εικόνα 2.1γ**). Καθένας εξ αυτών είναι κατάλληλος για την επίλυση διαφορετικών προβλημάτων.



Εικόνα 2.1: *Ενδεικτικοί τύποι Παλινδρόμησης*

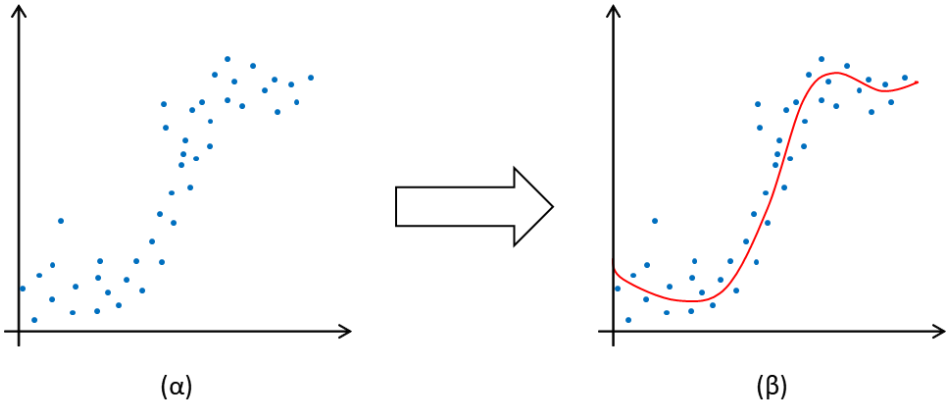
Η επιλογή του καταλληλότερου τύπου Παλινδρόμησης για την εκπαίδευση ενός μοντέλου προβλέψεων που θα επιστρέφει αποτελέσματα με τη μέγιστη δυνατή ακρίβεια, απαιτεί την πρότερη αποτύπωση ενός διαγράμματος διασποράς (*μτφρ. scatter plot*) στο οποίο θα εμφανίζονται όλες οι εξαρτημένες μεταβλητές συναρτήσει όλων των ανεξάρτητων. Κατόπιν, μπορεί να γίνει εμπειρική επιλογή του τύπου Παλινδρόμησης που φαίνεται να ανταποκρίνεται καλύτερα στα αποτυπωμένα δεδομένα. Εναλλακτικά, ο εκπαιδευτής του μοντέλου μπορεί να προβεί σε δοκιμές διαφορετικών τύπων μέχρις ότου να βρεθεί ο καταλληλότερος. Σε οποιαδήποτε εκ των ανωτέρω δύο περιπτώσεων, την επιλογή του τύπου Παλινδρόμησης ακολουθεί η παραμετροποίησή ώστε το τελικό μοντέλο να είναι κατά το δυνατόν βελτιστοποιημένο. Για να προσδιοριστεί η τελική εξίσωση που θα χαράσσει την αποτελεσματικότερη καμπύλη προβλέψεων, ο αλγόριθμος εκπαίδευσης θα πρέπει να δημιουργήσει και να συγκρίνει πλήθος μοντέλων, κάνοντας χρήση διαφορετικών μαθηματικών μεθόδων. Δύο εκ των δημοφιλέστερων είναι η μέθοδος ελαχίστων τετραγώνων και το άθροισμα απόλυτων αποκλίσεων (Maulud and Abdulazeez 2020).

Έστω ότι το σύνολο δεδομένων που είναι διαθέσιμο για την εκπαίδευση ενός μοντέλου παλινδρόμησης απεικονίζεται σε ένα διάγραμμα διασποράς όπως αυτό στην **Εικόνα 2.2α**. Εκ πρώτης όψεως, η πολυωνυμική και η λογιστική παλινδρόμηση φαίνονται να είναι οι δύο καταλληλότερες. Εν τέλει, μετά από δοκιμές και παραμετροποίηση, επαληθεύεται ότι ο καταλληλότερος είναι ήταν ο τύπος πολυωνυμικής παλινδρόμησης (Maulud and Abdulazeez 2020).

Η Παλινδρόμηση αποτελεί ιδανική επιλογή για την πραγματοποίηση ακριβών προβλέψεων τιμών βάσει συσχετισμών με συγκεκριμένες παραμέτρους εισόδου και, μεταξύ άλλων, μπορεί να εφαρμοστεί στους τομείς της οικονομίας (π.χ. για την πρόβλεψη της πορείας χρηματιστηριακών μετοχών), την κτηματομεσιτική (π.χ. για την εκτίμηση της τιμής ακινήτων), την ιατρική (π.χ. για την εκτίμηση της πορείας ασθενών), το εμπόριο (π.χ. για την πρόβλεψη της αγοραστικής κίνησης), την

[1] Η λογιστική παλινδρόμηση χρησιμοποιεί μία λογιστική συνάρτηση που καλείται *σιγμοειδής* (sigmoid) για τον υπολογισμό των προβλέψεων και των πιθανοτήτων τους Η σιγμοειδής συνάρτηση είναι μία συνάρτηση της οποίας η γραφική παράσταση έχει τη μορφή του Αγγλικού γράμματος "S" και έχει ως πεδίο τιμών το διάστημα [0, 1].

αγορά πρώτων υλών (π.χ. για την πρόβλεψη της τιμής πολύτιμων ή ημιπολύτιμων λίθων, μεταλλευμάτων, ορυκτών καυσίμων), κ.λπ (Maulud and Abdulazeez 2020).



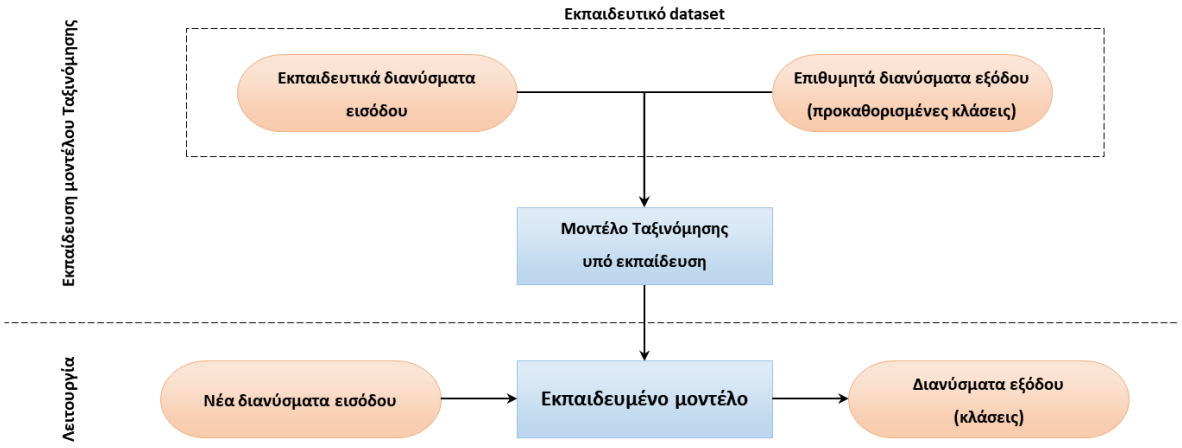
Εικόνα 2.2: *Παράδειγμα υλοποίησης μοντέλου πολυωνυμικής παλινδρόμησης*

2.2.2 Ταξινόμηση (Classification)

Μία άλλη μέθοδος Μηχανικής Μάθησης με επίβλεψη είναι η Ταξινόμηση (*μτφρ. Classification*), η οποία χρησιμοποιείται όταν χρειάζεται να αναδειχθούν μοτίβα για την αναγνώριση αντικειμένων και την κατηγοριοποίησή τους σε προκαθορισμένα σύνολα ή υποσύνολα.

Το μοντέλο τροφοδοτείται με ένα σύνολο δεδομένων το οποίο διαθέτει εξ αρχής διανύσματα εξόδου (Κλάσεις) στις οποίες ταξινομούνται τα διανύσματα εισόδου και καλείται να ανακαλύψει τα κοινά γνωρίσματα τους ώστε μετά το πέρας της εκπαίδευσης να τα κατατάσσει ορθώς (βλ. **Εικόνα 2.3**).

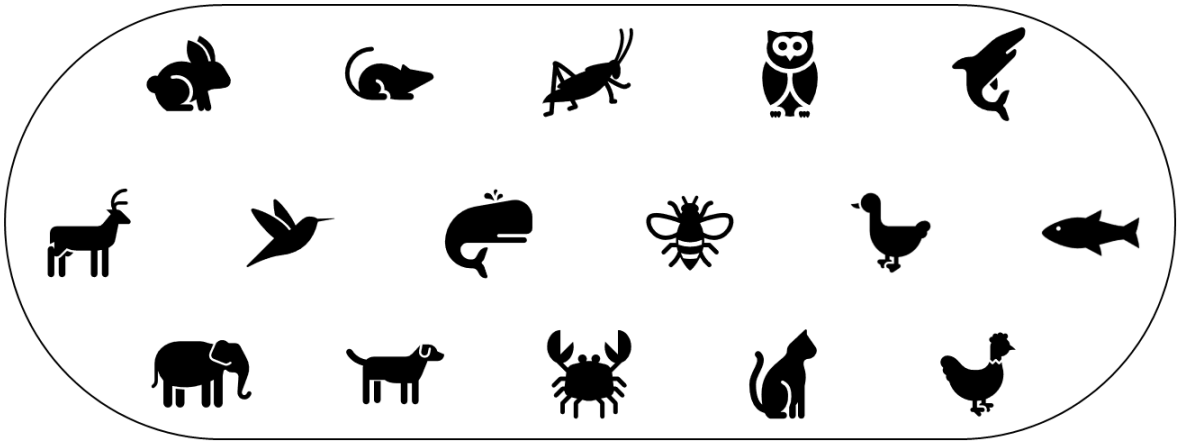
Η λειτουργία του εκπαιδευμένου μοντέλου επιδίδεται σε ταξινομήσεις δυαδικής ή πολλαπλής φύσεως. Στη δυαδική ταξινόμηση το μοντέλο κατηγοριοποιεί τα δεδομένα εισόδου με απαντήσεις τύπου ΝΑΙ/ΟΧΙ, ενώ στην πολλαπλή τα δεδομένα μπορούν να ταξινομηθούν σε περισσότερες κλάσεις (Kotsiantis, Zaharakis and Pintelas 2007).



Εικόνα 2.3: *Διάγραμμα ροής για την εκπαίδευση και τη λειτουργίας μοντέλου Ταξινόμησης*

Για την καλύτερη κατανόηση της λειτουργίας ενός μοντέλου Ταξινόμησης, ας υποθέσουμε ότι θέλουμε να υλοποιήσουμε έναν αλγόριθμο ο οποίος θα κατηγοριοποιεί αυτόματα εισερχόμενες φωτογραφίες που απεικονίζουν συγκεκριμένα είδη ζώων. Αρχικά, ο αλγόριθμος εκπαιδεύεται με ένα

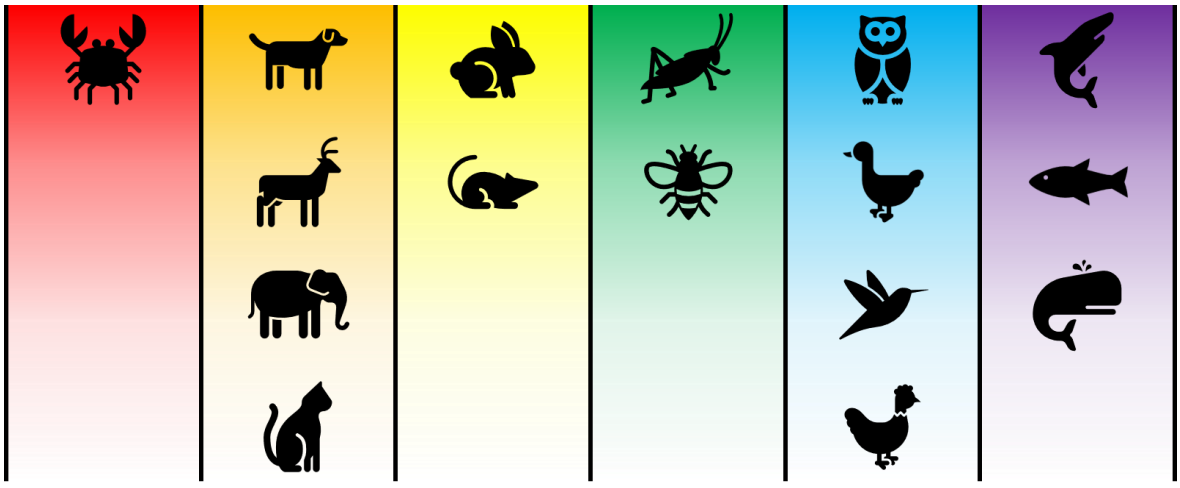
σύνολο δεδομένων φωτογραφιών με τα είδη ζώων που επιθυμούμε να κατηγοριοποιούμε. Ένα παράδειγμα παρουσιάζεται στην **Εικόνα 2.4**.



Εικόνα 2.4: *Γραφική αναπαράσταση ενδεικτικού εκπαιδευτικού συνόλου δεδομένων με ζώα*

Για τον σκοπό αυτό, κάθε φωτογραφία η οποία τροφοδοτεί το υπό εκπαίδευση μοντέλο, συνοδεύεται από επιπρόσθετα δεδομένα τα οποία είναι σεσημασμένα με ετικέτες (*μτφρ. labels*) οι οποίες μπορούν να αναφέρουν οτιδήποτε σχετικό με τα χαρακτηριστικά του εικονιζόμενου ζώου, π.χ. εάν είναι θηλαστικό, πτηνό, αμφίβιο ή έντομο, εάν είναι σαρκοφάγο, φυτοφάγο ή παμφάγο, κ.λπ. Εν συνεχεία, μέσα από το σύνολο δεδομένων επιλέγεται η ετικέτα με τις επιθυμητές Κλάσεις, έστω εκείνη που αναφέρει ποιο είδος ζώου απεικονίζεται (διάνυσμα εξόδου). Προαιρετικά, είναι καλό να προβλεφθεί και μία ακόμα Κλάση όπου θα κατατάσσονται οι μη ταξινομήσιμες είσοδοι (non-classified) όπου εκεί θα καταχωρούνται οι φωτογραφίες με ζώα που ο αλγόριθμός δεν θα καταφέρνει να αντιστοιχήσει σε κάποια από τις προκαθορισμένες Κλάσεις (Kotsiantis, Zaharakis and Pintelas 2007).

Με την ολοκλήρωση της εκπαίδευσης του μοντέλου, θα μπορεί αυτό να τροφοδοτείται είτε με νέα σύνολα δεδομένων, είτε με μεμονωμένες εικόνες, και θα είναι στη θέση να ταξινομεί με τη μέγιστη δυνατή ακρίβεια τα εισερχόμενα διανύσματα εισόδου, όπως για παράδειγμα στην **Εικόνα 2.5**.



Εικόνα 2.5: *Γραφική αναπαράσταση ταξινόμησης των δεδομένων*

Οι αλγόριθμοι Ταξινόμησης εφαρμόζονται σε περιπτώσεις χρήσης με πολυπαραγοντικά δεδομένα που χρήζουν ταχείας και ακριβούς αξιολόγησης. Μερικές ενδεικτικές περιπτώσεις χρήσης είναι η αναγνώριση ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (spam e-mail), η αναγνώριση της

αγοραστικής συμπεριφοράς πελατών, η αναγνώριση γραφικών χαρακτήρων, η ικανότητα αποπληρωμής αιτούμενων δανείων, κ.λπ. (Kotsiantis, Zaharakis and Pintelas 2007).

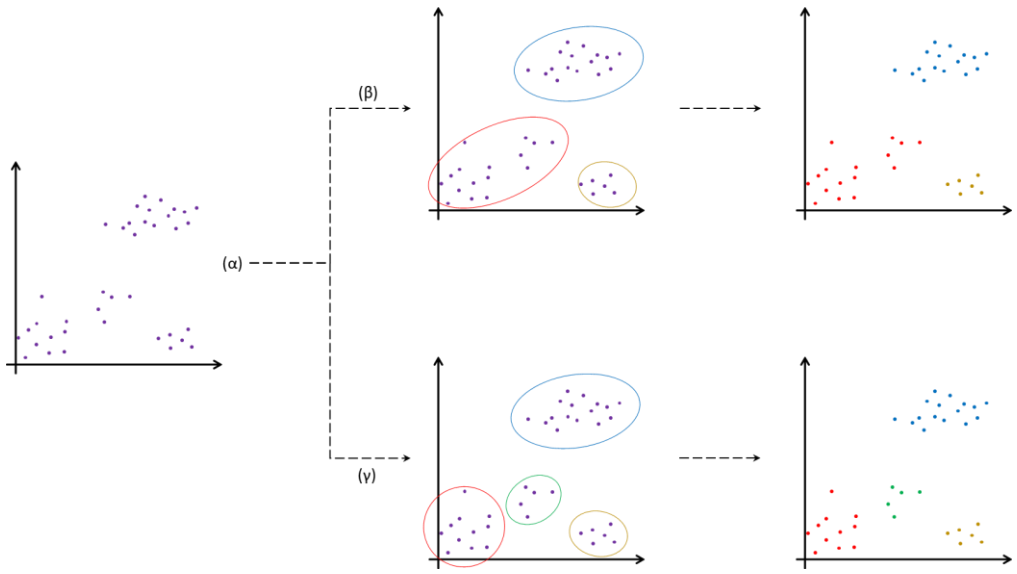
2.2.3 Συσταδοποίηση (Clustering)

Η Συσταδοποίηση ή Ομαδοποίηση (*μτφρ. Clustering*), αποτελεί μέθοδο της μη επιτηρούμενης Μηχανικής Μάθησης όπου το μοντέλο καλείται να εντοπίσει κοινά γνωρίσματα μεταξύ οντοτήτων (data points) και κατόπιν να τις ομαδοποιήσει με βάση αυτά. Έστω το σύνολο δεδομένων εκπαίδευσης με τα δεδομένα που φαίνονται στην **Εικόνα 2.6**. Μία δυνητική ομαδοποίηση τους θα μπορούσε να αφορά τον διαχωρισμό των εικονιζόμενων ζώων με βάση το περιβάλλον στο οποίο εμφανίζουν εξελικτικό πλεονέκτημα, και πιο συγκεκριμένα σε χερσαία, υδρόβια και ιπτάμενα:

Εικόνα 2.6: *Παράδειγμα Συσταδοποίησης*

Η κύρια παράμετρος για την βέλτιστη υλοποίηση ενός μοντέλου Συσταδοποίησης είναι ο αριθμός των Συστάδων (*μτφρ. Clusters*) στις οποίες ο εκπαιδευτής θα ορίσει να διαχωριστούν οι οντότητες των εκπαιδευτικών δεδομένων. Εν συνεχεία, ο αλγόριθμος θα ανατρέξει στα δεδομένα εκπαίδευσης, θα αναγνωρίσει κοινά χαρακτηριστικά και στο τέλος θα δημιουργήσει Συστάδες ίσες με το αριθμό που όρισε ο εκπαιδευτής. Εκεί, θα καταχωρήσει βάσει κοινών γνωρισμάτων τα εκπαιδευτικά διανύσματα εισόδου. Οι Συστάδες που προκύπτουν θα αποτελούν σημεία αναφοράς για νέα διανύσματα εισόδου, εκτός του συνόλου δεδομένων εκπαίδευσης, τα οποία το μοντέλο θα κληθεί να κατατάξει σε αυτές. Κάθε νέο διάνυσμα θα τοποθετείται στη συστάδα που κρίνεται ως πιο σχετική, βάσει των γνωρισμάτων του. Οι αντιστοιχίσεις των νέων διανυσμάτων πραγματοποιούνται μέσω διαφόρων προσεγγίσεων, και η βέλτιστη επιλογή εξαρτάται πάντα από πρόβλημα που τίθεται προς επίλυση. Δύο εκ των χαρακτηριστικότερων είναι (i) η μέθοδος κατηγοριοποίησης βάσει του κέντρου βάρους των Συστάδων και (ii) η μέθοδος κατηγοριοποίησης βάσει της εγγύτερης γειτνιάζουσας οντότητας (*μτφρ. nearest neighbour*). Στην πρώτη περίπτωση ορίζεται ένα κεντρικό σημείο σε κάθε Συστάδα ως σημείο αναφοράς, ενώ στη δεύτερη ως σημείο αναφοράς μπορεί να εκληφθεί το αντικείμενο της εκάστοτε συστάδας το βρίσκεται πιο κοντά (γείτονας) στο νέο διάνυσμα εισόδου. Συνηθέστερα, χρησιμοποιείται ένας αριθμός **K** εγγύτερων γειτόνων (K nearest neighbors, KNN) και όχι μόνο σε ένας (McGregor, et al. 2004), προκειμένου να αποφευχθούν στρεβλώσεις που τυχόν δημιουργούν έκτοπα δεδομένα (outliers).

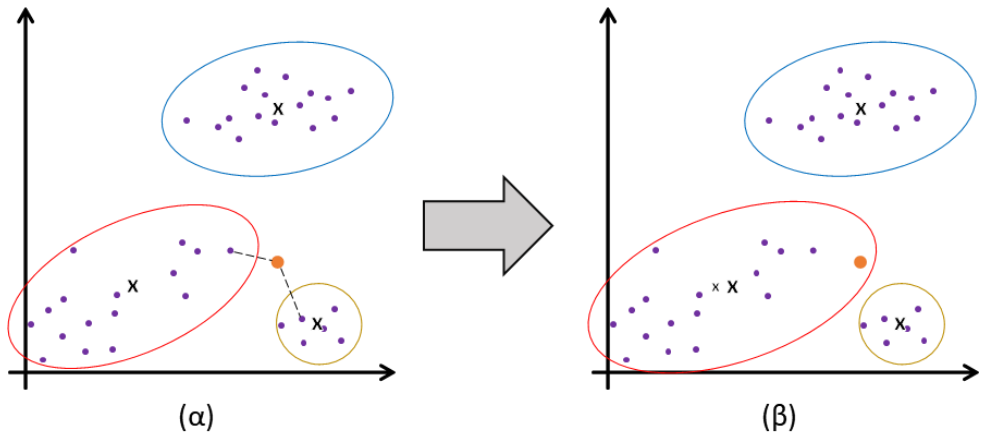
Για παράδειγμα, στην **Εικόνα 2.7α** απεικονίζεται ένα διάγραμμα διασποράς με τα διανύσματα εισόδου (οντότητες) ενός συνόλου δεδομένων. Μολονότι μπορεί να γίνει επιλογή οποιουδήποτε αριθμού συστάδων για την ομαδοποίηση των οντοτήτων κατά την παραμετροποίηση του αλγορίθμου εκπαίδευσης, από το διάγραμμα διασποράς διαφαίνεται ότι το σύνολο δεδομένων θα μπορούσε να χωριστεί σε τρεις (3) ή τέσσερις (4) Συστάδες.



Εικόνα 2.7: *Συσταδοποίηση με 3 (β) και 4 (γ) Συστάδες*

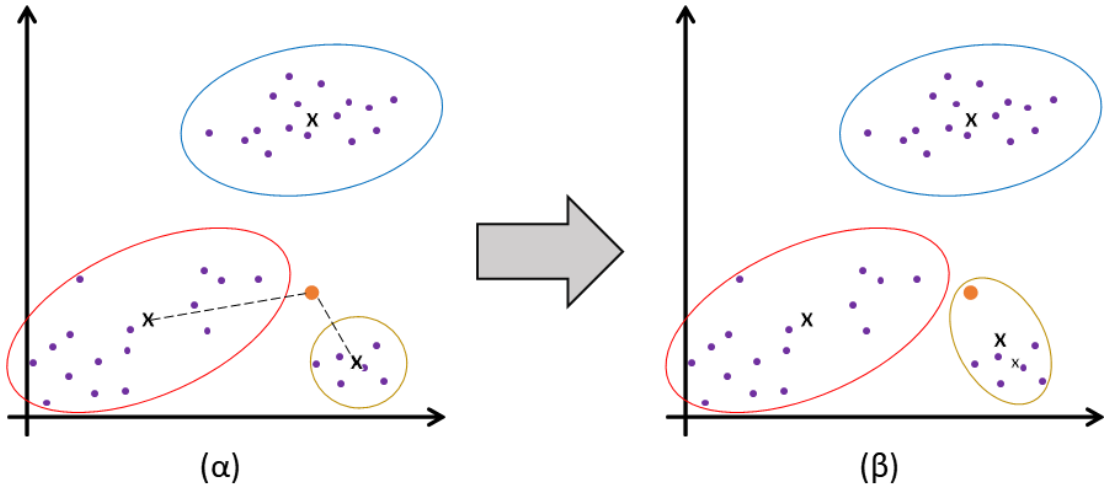
Αρχικά, ο αλγόριθμος εκπαίδευσης παραμετροποιείται ώστε να δημιουργήσει 3 συστάδες και κατόπιν να ομαδοποιήσει τις οντότητες. Το αποτέλεσμα που προκύπτει αποτυπώνεται στην **Εικόνα 2.7β**. Στη συνέχεια, παραμετροποιείται εκ νέου αλλά με τον αλγόριθμο να καλείται αυτή τη φορά να δημιουργήσει 4 συστάδες και να ομαδοποιήσει και πάλι τις οντότητες, με τη νέα παράμετρο. Το αποτέλεσμα αποτυπώνεται στην **Εικόνα 2.7γ**. Έχοντας πλέον στη διάθεσή μας δύο λειτουργικά μοντέλα, εισάγουμε σε καθένα από αυτά μία νέα οντότητα ώστε να εξετάσουμε πώς αυτή θα ομαδοποιείται υπό διαφορετικές συνθήκες . Για το κάθε μοντέλο (3 ή 4 Συστάδων), η ομαδοποίηση θα πραγματοποιείται τόσο με τη μέθοδο του εγγύτερου γείτονος όσο και με το κέντρο βάρους κάθε συστάδας. Στα παραδείγματα που ακολουθούν, το νέο διάνυσμα εισόδου απεικονίζεται με πορτοκαλί χρώμα ενώ τα κέντρα βάρους των συστάδων με ένα **X** μαύρου χρώματος.

Στην **Εικόνα 2.8** διαφαίνεται που τοποθετείται η νέα οντότητα επί του διαγράμματος διασποράς, και πιο συγκεκριμένα σε σχέση με το μοντέλο τριών (3) Συστάδων. Για να αποφασιστεί που θα ενταχθεί με χρήση της μεθόδου εγγύτερου γείτονος, χαράσσονται ευθείες προς τις κοντινότερες οντότητες των συστάδων. Στο παράδειγμα της εικόνας παρουσιάζονται μόνο οι δύο κοντινότερες, και δη, από την κόκκινη και κίτρινη Συστάδα (**Εικόνα 2.8α**). Παρατηρείται και αποδεικνύεται ότι η νέα οντότητα βρίσκεται εγγύτερα στην κόκκινη Συστάδα και κατά συνέπεια θα ενταχθεί εκεί. Παράλληλα, τα όριά της κόκκινης Συστάδας θα αναπροσαρμοστούν με βάση το νέο μέλος της (**Εικόνα 2.8β**).



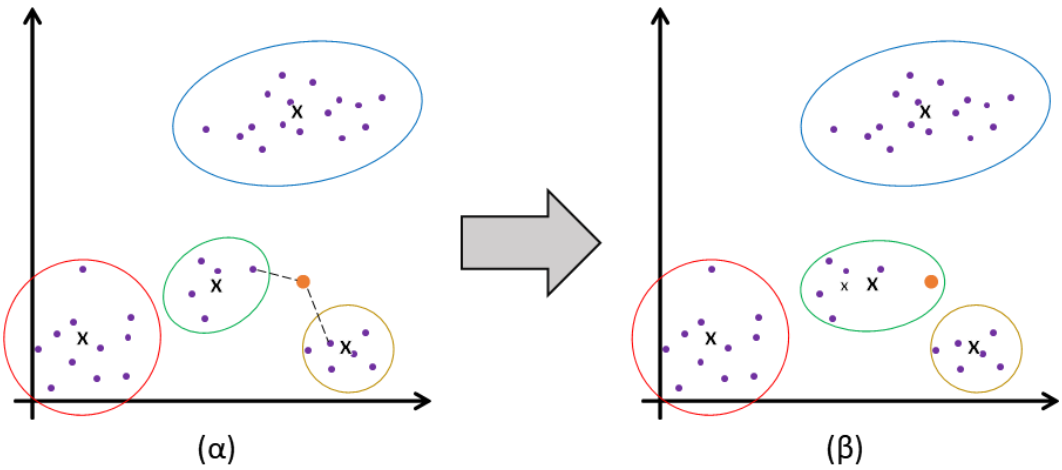
Εικόνα 2.8: *Ομαδοποίηση νέας οντότητας με τη μέθοδο του εγγύτερου γείτονος σε 3 Συστάδες*

Ωστόσο, δεν συμβαίνει το ίδιο όταν για το ίδιο μοντέλο χρησιμοποιείται η μέθοδος των κέντρων βάρους (**Εικόνα 2.9**). Και πάλι χαράσσονται ευθείες, αυτή τη φορά όμως προς τα κέντρα βάρους κάθε μίας Συστάδας. Και πάλι διαφαίνεται ότι η νέα οντότητα βρίσκεται πολύ μακρύτερα από την μπλε Συστάδα. Παρατηρείται και αποδεικνύεται ότι η βρίσκεται εγγύτερα στο κέντρο βάρους της κίτρινης Συστάδας (**Εικόνα 2.9α**), και κατά συνέπεια θα ενταχθεί εκεί. Ως εκ τούτου, τα όριά της κίτρινης Συστάδας θα αναπροσαρμοστούν με βάση το νέο μέλος της (**Εικόνα 2.9β**) όπως επίσης θα πραγματοποιηθεί και επανυπολογισμός του κέντρου βάρους. Πιο συγκεκριμένα, στην **Εικόνα 2.9β** παρατηρείται το νέο κέντρο βάρους, σημειωμένο με ένα μαύρο **X** ενώ το προηγούμενο κέντρο βάρους σημειώνεται με ένα αχνότερο **x,** μικρότερου μεγέθους, ώστε να διακρίνεται η μετατόπισή που υπέστη (McGregor, et al. 2004).



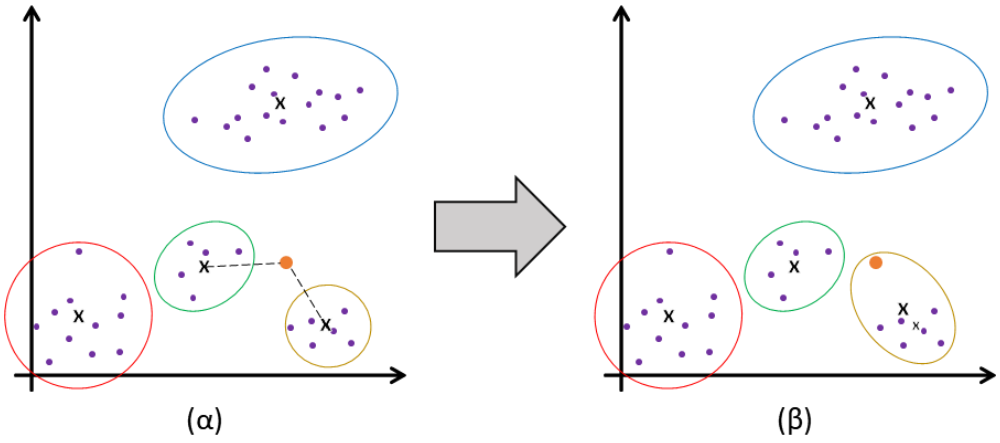
Εικόνα 2.9: *Ομαδοποίηση νέας οντότητας με τη μέθοδο κέντρων βάρους σε 3 Συστάδες*

Η προαναφερθείσα διαδικασία επαναλαμβάνεται αντίστοιχα και για το μοντέλο των τεσσάρων (4) Συστάδων.



Εικόνα 2.10: *Ομαδοποίηση νέας οντότητας με τη μέθοδο του εγγύτερου γείτονος σε 4 Συστάδες*

Στην **Εικόνα 2.10** παρουσιάζεται η ένταξη της νέας οντότητας σε συστάδα με χρήση της μεθόδου του εγγύτερου γείτονος ενώ στην **Εικόνα 2.11** που ακολουθεί, με χρήση της μεθόδου των κέντρων βάρους.



Εικόνα 2.11: *Ομαδοποίηση νέας οντότητας με τη μέθοδο κέντρων βάρους σε 4 Συστάδες*

Στην πρώτη περίπτωση η νέα οντότητα τοποθετήθηκε στην πράσινη συστάδα (σε αντίθεση με το μοντέλο των τριών 3 συστάδων όπου τοποθετήθηκε στην κόκκινη), ενώ στη δεύτερη τοποθετήθηκε οριακά στην κίτρινη, με τη διαφορά των αποστάσεων της από τα κέντρα βάρους της πράσινης και της κίτρινης συστάδας να είναι πολύ μικρή και όχι ευδιάκριτη όπως στην **Εικόνα 2.11**.

Με βάση τα ανωτέρω παραδείγματα γίνεται σαφές ότι τόσο ο αριθμός των Συστάδων που θα οριστεί μέσω της παραμετροποίησης του εκπαιδευόμενου μοντέλου, όσο και η μέθοδος που θα χρησιμοποιηθεί για την τοποθέτηση των νέων οντοτήτων, παίζουν σημαντικό ρόλο στην λειτουργία και την απόδοση του μοντέλου όταν αυτό τεθεί σε επιχειρησιακή λειτουργία (McGregor, et al. 2004).

Μοντέλα συσταδοποίησης μπορούν να εφαρμοστούν σε περιπτώσεις χρήσης πολυπαραγοντικών δεδομένων όπως η κατηγοριοποίηση ηλεκτρονικής αλληλογραφίας (π.χ. διαφημιστική, ενοχλητική, επιβλαβής, κ.λπ.), για τον χαρακτηρισμό άρθρων ή δημοσιεύσεων ως ψευδείς ειδήσεις (fake news), την αναγνώριση παράνομων δραστηριοτήτων, την κατηγοριοποίηση χρηστών για βελτιστοποίηση στοχευμένων προωθητικών ενεργειών, κ.λπ. (McGregor, et al. 2004).

2.2.4 Εξελικτικοί Αλγόριθμοι

Οι Εξελικτικοί Αλγόριθμοι (μτφρ. Evolutionary Algorithms) είναι ένας ιδιαίτερος τρόπος επίλυσης προβλημάτων επειδή δεν προσπαθούν να προσεγγίσουν τη λειτουργία της ανθρώπινη σκέψης, αλλά την εξελικτική λειτουργία της ίδιας της φύσης. Πρόκειται για ένα ευρύ σύνολο συστημάτων επίλυσης προβλημάτων, που συμπεριλαμβάνει μεθόδους όπως οι γενετικοί αλγόριθμοι που χρησιμοποιούν γενετικό προγραμματισμό, τα συστήματα ταξινόμησης, οι εξελικτικές στρατηγικές κ.ά. (Gobeyn, et al. 2019).

Για την εκπαίδευσή τους, οι εξελικτικοί αλγόριθμοι χρησιμοποιούν μεθόδους ενισχυμένης μάθησης ενώ υλοποιούνται μέσω τεχνικών που έχουν εμπνευστεί από τη βιολογική εξέλιξη των ειδών. Για τον λόγο αυτό, δανείζονται όρους από την επιστήμη της Βιολογίας και τους χρησιμοποιούν με αφαιρετικό τρόπο. Στόχος τους είναι να αναπαράξουν αλγοριθμικά, στο ελάχιστα αποδεκτό επίπεδο, τις σχετικές φυσικές διεργασίες που θα χρησιμοποιηθούν για την επίλυση προβλημάτων αναζήτησης και βελτιστοποίησης. Η ορολογία τους περιλαμβάνει όρους που έχουν υιοθετηθεί από την επιστήμη της Βιολογίας και χρησιμοποιούνται για να περιγράψουν τις ανάλογες διαδικασίες των Εξελικτικών Αλγορίθμων (Gobeyn, et al. 2019):

- **Πληθυσμός** (*μτφρ. population*) ονομάζεται ένα σύνολο ομοειδών οντοτήτων που αναπαράγονται μεταξύ τους.
- **Γενεά** (*μτφρ. generation*) ονομάζεται κάθε νέο σύνολο οντοτήτων (απόγονοι) που προκύπτει από προηγούμενες (πρόγονοι) που αναπαράχθηκαν.
- **Γενότυπος** (*μτφρ. genotype*) ονομάζεται το γονιδιακό σύνολο μιας οντότητας. Για λόγους απλότητας, κυρίως όταν θέλουμε να περιγράψουμε στοιχεία του πληθυσμού, ο γενότυπος αναφέρεται ως "**οντότητα**" (*μτφρ. entity*) ή "**άτομο**" (*μτφρ. individual*).
- **Χρωμόσωμα** (*μτφρ. chromosome*) είναι μια οργανωμένη δομή πληροφοριών (γονίδια).
- **Γονίδιο** (*μτφρ. gene*) ονομάζεται κάθε κληροδοτούμενο χαρακτηριστικό γνώρισμα (ιδιότητα) το οποίο κατέχει συγκεκριμένη θέση μέσα σε ένα χρωμόσωμα.
- **Γενετικός Τόπος** ή **Γονιδιακή Θέση** (*μτφρ. locus*) ονομάζεται η θέση ενός γονιδίου μέσα σε ένα χρωμόσωμα.
- **Γονιδιακή Δεξαμενή** (*μτφρ. gene pool*) είναι η διαθέσιμη συνολική γενετική ποικιλομορφία του υπό εξέταση πληθυσμού.
- **Αλληλόμορφα** (*μτφρ. allele*): ονομάζονται οι διαφορετικές παραλλαγές ενός γονιδίου που βρίσκονται σε συγκεκριμένο γενετικό τόπο και συναντώνται σε διαφορετικά άτομα του ίδιου είδους. Για παράδειγμα, το γονίδιο που καθορίζει το χρώμα των ματιών έχει δύο αλληλόμορφα: το αλληλόμορφο για τα καστανά μάτια και το αλληλόμορφο για τα μπλε μάτια. Ένα άτομο μπορεί να έχει δύο αλληλόμορφα του ίδιου γονιδίου (ομόζυγο) ή ένα αλληλόμορφο από κάθε γονέα (ετερόζυγο). Σε περίπτωση ομόζυγου, το άτομο θα εκφράσει το χαρακτηριστικό που καθορίζεται από το επικρατές αλληλόμορφο. Σε περίπτωση ετερόζυγου, το άτομο θα εκφράσει ένα μείγμα των δύο χαρακτηριστικών. Τα αλληλόμορφα είναι υπεύθυνα για την ποικιλομορφία των οργανισμών και χωρίς αυτά όλοι οι οργανισμοί του ίδιου είδους θα ήταν πανομοιότυποι.

Οι εξελικτικοί αλγόριθμοι είναι πιθανοτικές μέθοδοι που αναζητούν τη βέλτιστη λύση μέσα από το σύνολο όλων των πιθανών λύσεων ενός συγκεκριμένου προβλήματος. Ένας εξελικτικός αλγόριθμος λαμβάνει ως σημείο εκκίνησης ένα σύνολο πιθανών λύσεων και τις αξιολογεί. Κατόπιν, λειτουργώντας παρόμοια με βιολογικούς εξελικτικούς μηχανισμούς (διασταύρωση, μετάλλαξη

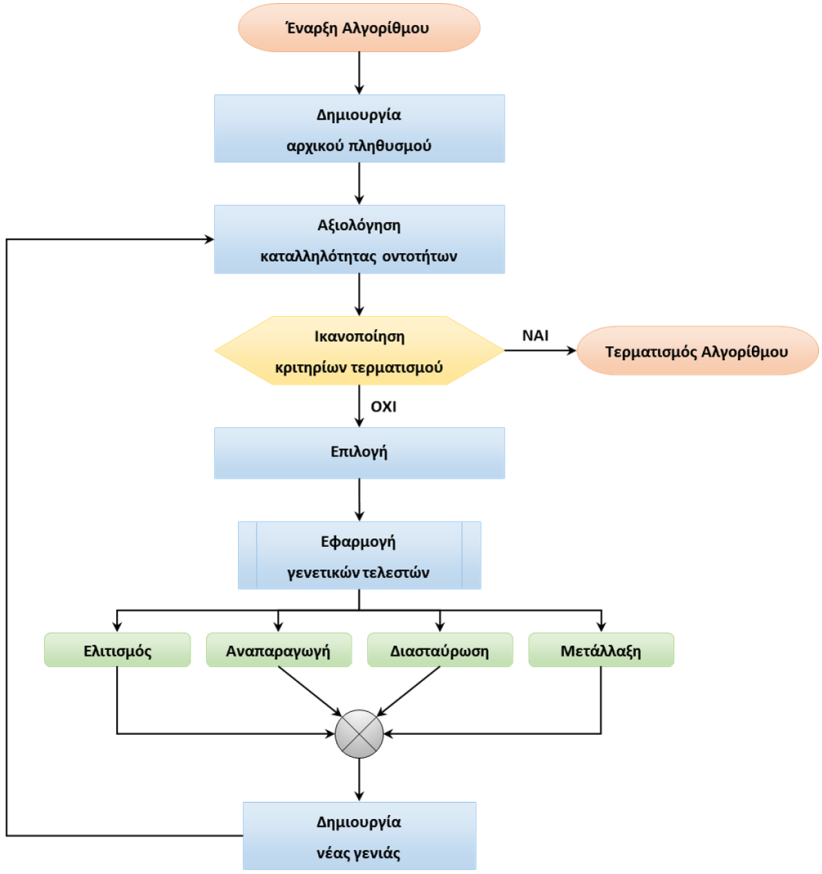
κ.λπ.), δημιουργούνται νέες λύσεις (απόγονοι) και επιλέγονται οι καταλληλότερες βάσει βαθμολογικών κριτηρίων, οι οποίες θα χρησιμοποιηθούν για τη δημιουργία νέων γενεών. Η διαδικασία αυτή επαναλαμβάνεται έως ότου βρεθεί η καλύτερη λύση σύμφωνα με τελικά κριτήρια-στόχους ή έως ότου ο αλγόριθμος τερματίσει μετά από έναν προκαθορισμένο αριθμό επαναλήψεων. Η τυπική διαδικασία προσδιορισμού της βέλτιστης λύσης που ακολουθείται από έναν εξελικτικό αλγόριθμο έχει ως ακολούθως (Gobeyn et al., 2019):

1. **Αρχικοποίηση** (*μτφρ. initialization*): Είναι η διαδικασία δημιουργίας του πρώτου πληθυσμού. Από αυτήν τη γενεά (έστω: ***g***) θα δημιουργηθούν νέες γενεές οντοτήτων. Η δημιουργία μιας αρχικής γενεάς πραγματοποιείται είτε με τυχαίο τρόπο είτε με αξιοποιώντας προϋπάρχουσα γνώση.
2. **Αξιολόγηση** (*μτφρ. evaluation*): Πρόκειται για τη διαδικασία αξιολόγησης των οντοτήτων με βάση το κατά πόσο προσεγγίζουν το επιθυμητό αποτέλεσμα. Κάθε οντότητα λαμβάνει μια τιμή καταλληλότητας (*fitness score*) της οποίας το μέγεθος εξαρτάται από το πόσο κοντά βρίσκεται η εκάστοτε οντότητα στην επιθυμητή ή βέλτιστη λύση.
3. **Επιλογή** (*μτφρ. selection*): Μετά την ολοκλήρωση της διαδικασίας αξιολόγησης, ακολουθεί η επιλογή των οντοτήτων που θα διασταυρωθούν μεταξύ τους, οι οποίες με τη σειρά τους θα αποδώσουν νέους απογόνους. Η πιθανότητα επιλογής μίας οντότητας είναι ανάλογη της βαθμολογίας που της αποδόθηκε κατά την αξιολόγηση.
4. **Δημιουργία νέας γενεάς:** Μετά το πέρας της αξιολόγησης (βαθμολόγησης) των οντοτήτων του τελευταίου (τρέχοντος) πληθυσμού, ο Γενετικός Αλγόριθμος θα προχωρήσει στη δημιουργία της νέας γενεάς. Έστω **g** η πρώτη γενεά. Η επόμενή της θα είναι η ***g+1***, θα ακολουθήσει η ***g+2,*** κοκ. Κάθε γενεά απαρτίζεται από έναν προκαθορισμένο αριθμό οντοτήτων ο οποίος συνηθίζεται να είναι ίσος με εκείνον του αρχικού πληθυσμού. Η επιλογή του αριθμού αυτού πραγματοποιείται με διάφορα κριτήρια, όπως για παράδειγμα πόσο κοστοβόρος είναι σε σχέση με τις υπολογιστικές δυνατότητες του συστήματος στο οποίο εκτελείται ο αλγόριθμος. Οι μέθοδοι που ακολουθούνται για τη δημιουργία μια νέας γενεάς ονομάζονται “γενετικοί τελεστές” και οι πιο ευρέως χρησιμοποιούμενες, είναι (Gobeyn, et al. 2019):

    i. **Ελιτισμός** (*μτφρ. elitism*)**:** όταν ο εξελικτικός αλγόριθμος εντοπίσει μια οντότητα που ανταποκρίνεται σε αυστηρά καθορισμένα κριτήρια (ως, για παράδειγμα, να επιτυγχάνει υψηλή βαθμολογία σε σύγκριση με τις υπόλοιπες του ίδιου πληθυσμού) τότε δύναται να επιλεγεί ώστε να μεταφερθεί άμεσα στην επόμενη γενεά.
    ii. **Αναπαραγωγή** (*μτφρ. replication*)**:** η αναπαραγωγή αφορά μία μέθοδο όπου μια οντότητα αντιγράφεται ως έχει στην επόμενη γενεά μέσω τυχαίας επιλογής. Η μέθοδος αυτή συχνά ονομάζεται "ρουλέτα επιλογής". Η πιθανότητα να επιλεγεί μία οντότητα εξαρτάται από το μέγεθος της βαθμολογίας που έλαβε κατά τη διαδικασία της αξιολόγησης.
    iii. **Διασταύρωση** (*μτφρ. crossover*)**:** αναφέρεται στη διαδικασία μέσω της οποίας ανταλλάσσεται γενετική πληροφορία μεταξύ δύο οντοτήτων του ίδιου πληθυσμού. Όμοια με τη βιολογική αναπαραγωγή των ειδών, όπου ο απόγονος παίρνει γονίδια και από τους δύο γονείς, η διαδικασία αυτή πραγματοποιείται όταν δύο οντότητες προσφέρουν διαφορετικά γονίδια σε μία οντότητα-απόγονό τους.
    iv. **Μετάλλαξη** (*μτφρ. mutation*)**:** η διαδικασία της μετάλλαξης αφορά την απρόβλεπτη μεταβολή της τιμής ενός τυχαίου γονιδίου το οποίο μεταβιβάζεται από έναν πρόγονο σε

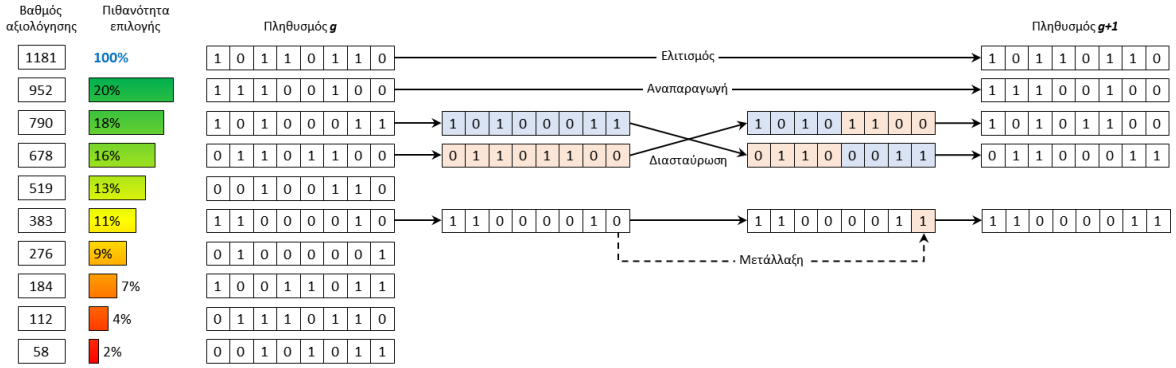
έναν απόγονο. Η ρυθμός εμφάνισης των μεταλλάξεων (mutation rate) καθορίζεται στη φάση παραμετροποίησης του αλγορίθμου.

Ακολουθεί Διάγραμμα Ροής (**Εικόνα 2.12**) που παρουσιάζει τη γενική λειτουργία ενός Εξελικτικού Αλγόριθμου:



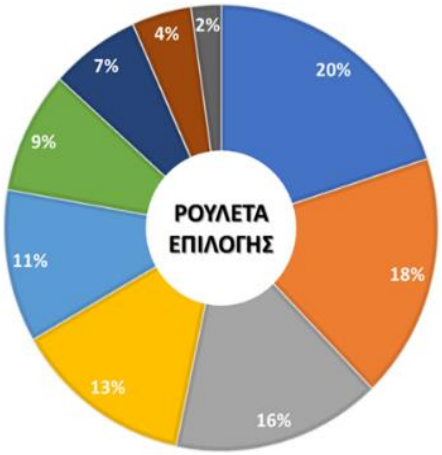
Εικόνα 2.12: *Διάγραμμα Ροής ενός τυπικού Εξελικτικού Αλγόριθμου*

Στο παρακάτω σχήμα (**Εικόνα 2.13**) παρουσιάζεται η λειτουργία των 4 προαναφερθέντων γενετικών τελεστών. Στο παράδειγμα, και για την καλύτερη κατανόησή του, χρησιμοποιούνται συμβολοσειρές των 8 bit, με κάθε γενετικό τελεστή να εφαρμόζεται μία φορά. Οι οντότητες έχουν ταξινομηθεί με φθίνουσα σειρά και βάσει του βαθμού καταλληλότητάς τους. Ακολούθως, προκύπτει και η πιθανότητα επιλογής μιας οντότητας για συμμετοχή σε στις διαδικασίες των Γενετικών Τελεστών (πλην του ελιτισμού) (Gobeyn, et al. 2019).



Εικόνα 2.13: *Παράδειγμα λειτουργίας Γενετικών Τελεστών*

- Στην κορυφή της λίστας εφαρμόζεται **ελιτισμός** επί της πρώτης οντότητας, καθότι αυτή συγκεντρώνει υψηλή βαθμολογία καταλληλότητας, καθιστώντας την αναμφίβολα ως τον καλύτερο υποψήφιο για την επόμενη γενεά.
- Στη συνέχεια, γίνεται εφαρμογή της διαδικασίας της **αναπαραγωγής**, όπου κατά την παραμετροποίησή της καθορίζεται ο αριθμός οντοτήτων που θα επιλεγούν για να μεταφερθούν αυτούσιες στην επόμενη γενεά. Όλες οι υποψήφιες οντότητες συμμετέχουν σε μια ψηφιακή ρουλέτα (**Εικόνα 2.14**) όπου οι πιθανότητες της κάθε μίας για να επιλεγεί εξαρτώνται από το βαθμό καταλληλότητας (fitness score) που της αποδόθηκε κατά τη διαδικασία της Αξιολόγησης. Οι οντότητες που τελικά επιλέγονται, μεταφέρονται ως έχουν στην επόμενη γενιά.
- Κατά τη **διασταύρωση**, επιλέγονται δύο οντότητες οι οποίες ανταλλάσσουν μεταξύ τους γονίδια (bits) μεταξύ των ίδιων γονιδιακών θέσεων (θέσεις πίνακα).
- Σύμφωνα με την παραμετροποίησή της, η **μετάλλαξη** μπορεί να εμφανιστεί σε οποιοδήποτε γονίδιο, σε οποιαδήποτε γονιδιακή θέση, εντός οντοτήτων που επιλέχθηκαν τυχαία.



Εικόνα 2.14: *Γραφική αναπαράσταση "ρουλέτας γονικής επιλογής"*

Με βάση τα παραπάνω, υπάρχει πιθανότητα να προκύψει η εμφάνιση της ίδιας οντότητας δύο φορές σε μια προκύπτουσα γενεά ή να επανεμφανιστεί στο «μέλλον» (σε μεταγενέστερη δηλαδή γενεά), ακόμα κι αν είχε εξαφανιστεί για μερικές γενεές. Σε όλες τις περιπτώσεις, η διαδικασία επιστρέφει στο βήμα της αξιολόγησης και επαναλαμβάνεται διαρκώς μέχρι να βρεθεί η βέλτιστη δυνατή λύση ή έως ότου ολοκληρωθεί ο αλγόριθμος βάσει προκαθορισμένων κριτηρίων.

Υπάρχουν διάφορες προσεγγίσεις για τη βελτιστοποίηση ενός εξελικτικού αλγορίθμου, οι οποίες εφαρμόζονται κατά περίπτωση, ανάλογα με τον τύπο του προς επίλυση προβλήματος, τους διαθέσιμους υπολογιστικούς πόρους, και άλλους παράγοντες. Για παράδειγμα, μπορεί να επιλεγεί να ξεκινήσει ο αλγόριθμος με έναν αρχικό πληθυσμό που αριθμεί πολλές οντότητες, με τη δυνατότητα να μειωθεί κατά το ήμισυ αργότερα. Μια τέτοια προσέγγιση μπορεί να εφαρμοστεί όταν στοχεύουμε σε μεγαλύτερη αρχική εξερεύνηση του χώρου αναζήτησης και εν συνεχεία σε μία πιο εστιασμένη αναζήτηση βάσει κριτηρίων αξιολόγησης. Σε κάθε περίπτωση, οι γενετικοί τελεστές προσαρμόζονται σύμφωνα με τις απαιτήσεις του εκάστοτε προβλήματος ενώ δεν καθίσταται απαραίτητη η χρήση όλων των διαθέσιμων τελεστών (Gobeyn, et al. 2019)

Ο τρόπος προσέγγισης που επιλέγουν οι εξελικτικοί αλγόριθμοι είναι απλός και ιδιαίτερα ευέλικτος. Αυτό τους παρέχει τη δυνατότητα να χρησιμοποιούνται τόσο αυτόνομα ως ανεξάρτητες λύσεις, όσο και σε συνδυασμό με άλλες μεθόδους, δημιουργώντας πιο εξειδικευμένες υβριδικές μορφές εξελικτικών αλγορίθμων. Ένα αξιοσημείωτο χαρακτηριστικό τους είναι ότι δεν λειτουργούν απευθείας με τις μεταβλητές του προβλήματος, αλλά με μια κωδικοποιημένη αναπαράσταση του συνόλου των δυνατών λύσεων. Είναι εφαρμόσιμοι ακόμα και σε δυναμικά συστήματα, όπου ο στόχος και οι περιορισμοί του προβλήματος μπορεί να είναι χρονικά μεταβαλλόμενοι. Επιπλέον, αποδεικνύουν την αποτελεσματικότητά τους και σε περίπλοκες περιπτώσεις, όπως όταν ο χώρος

αναζήτησης είναι ασυνεχής, με πολλαπλά ακρότατα, χαοτικός, και γενικά όταν οι παραδοσιακές μέθοδοι δεν μπορούν να αποδώσουν ικανοποιητικά αποτελέσματα (Gobeyn, et al. 2019).

Ας υποθέσουμε, για παράδειγμα, ότι πρέπει να εντοπίσουμε τη μέγιστη δυνατή τιμή εξόδου μιας άγνωστης διεργασίας που διαθέτει τέσσερις εισόδους. Καθεμία από αυτές τις εισόδους μπορεί να πάρει τιμές από το 0 έως το 100. Συνεπώς, έχουμε συνολικά 100^4 = 100.000.000 πιθανούς συνδυασμούς για τις τιμές εισόδου. Μία συμβατική προσέγγιση για την επίλυση αυτού του προβλήματος θα απαιτούσε τον εξαντλητικό έλεγχο κάθε πιθανού συνδυασμού τιμών εισόδου ξεχωριστά, καταγράφοντας την αντίστοιχη έξοδο. Αφού δοκιμαζόταν κάθε συνδυασμός, ο αλγόριθμος θα επέστρεφε τη μέγιστη τιμή εξόδου. Αντίθετα, μια προσέγγιση που βασίζεται σε εξελικτικούς αλγόριθμους αναζητά πολλές πιθανές λύσεις ταυτόχρονα, αντί να τις εξετάζει μία προς μία. Στο συγκεκριμένο παράδειγμα, ένας εξελικτικός αλγόριθμος θα κωδικοποιούσε την είσοδο ως μια συμβολοσειρά (χρωμόσωμα) με 12 ψηφία, δηλαδή 3 για κάθε μία από τις 4 εισόδους (γονίδια) του συστήματος. Έπειτα, θα ξεκινούσε με έναν αρχικό πληθυσμό (**g**), συγκεκριμένου πλήθους οντοτήτων, τις οποίες θα αξιολογούσε βάσει της εξόδου που παρήγαγε καθεμία. Στη συνέχεια, θα εφάρμοζε τις καθορισμένες διαδικασίες για τη δημιουργία μιας νέας γενιάς οντοτήτων (**g+1**). Οι απόγονοι θα αξιολογούνταν με τη σειρά τους και, βάσει γενετικών τελεστών που εφαρμόζονται, θα δημιουργηθεί η επόμενη γενιά. Αυτή η διαδικασία θα επαναλαμβανόταν μέχρις ότου εκπληρωθούν τα κριτήρια τερματισμού του αλγορίθμου.

Παρατηρείται ένα σημαντικό χαρακτηριστικό των εξελικτικών αλγορίθμων οι οποίοι διατηρούν καθ' όλη τη διάρκεια της λειτουργίας τους έναν πληθυσμό λύσεων για το πρόβλημα που αντιμετωπίζουν, ενώ παράλληλα προσπαθούν να εντοπίσουν τη βέλτιστη λύση σε πολλά σημεία του χώρου αναζήτησης ταυτοχρόνως.

Οι εξελικτικοί αλγόριθμοι εφαρμόζονται κυρίως όταν αντιμετωπίζονται προκλήσεις βελτιστοποίησης και κατορθώνουν να εξυπηρετούν πολλούς τομείς, μεταξύ των οποίων και οι εξής (Gobeyn, et al. 2019):

- **Γενικές Εφαρμογές:** έλεγχος ποιότητας, σχεδιασμός χρονοδιαγραμμάτων, κ.λπ.
- **Μετεωρολογία:** μοντελοποίηση των θερμοκρασιακών αλλαγών σε τοπικό ή παγκόσμιο επίπεδο, κ.λπ.
- **Βιολογία:** πρόβλεψη δομής RNA, κατασκευή φυλογενετικών δέντρων ,ανάλυση προφίλ γονιδιακών εκφράσεων, κ.λπ.
- **Κοινωνικές Επιστήμες:** γλωσσικές αναλύσεις, σχεδιασμός αντιτρομοκρατικών συστημάτων, κ.λπ.
- **Οικονομικές Επιστήμες:** εντοπισμός απάτης, βελτιστοποίηση χαρτοφυλακίου, σχεδιασμός αυτοματοποιημένων χρηματοπιστωτικών συστημάτων συναλλαγών, κ.λπ.
- **Μεταφορές:** δρομολογήσεις οχημάτων, βελτιστοποίηση φόρτωσης κοντέινερ, κ.λπ.
- **Τηλεπικοινωνίες:** βελτιστοποίηση υποδομής τηλεπικοινωνιακών δικτύων, κ.λπ.
- **Σχεδιασμός Συστημάτων:** αυτοματοποιημένος σχεδιασμός βιομηχανικού εξοπλισμού, αυτοματοποιημένος σχεδιασμός μηχατρονικών συστημάτων, δίκτυα παρακολούθησης υπόγειων υδάτων, σχεδιασμός συστημάτων παροχής νερού, αυτοματοποιημένος σχεδιασμός σύνθετων υλικών, κ.λπ.

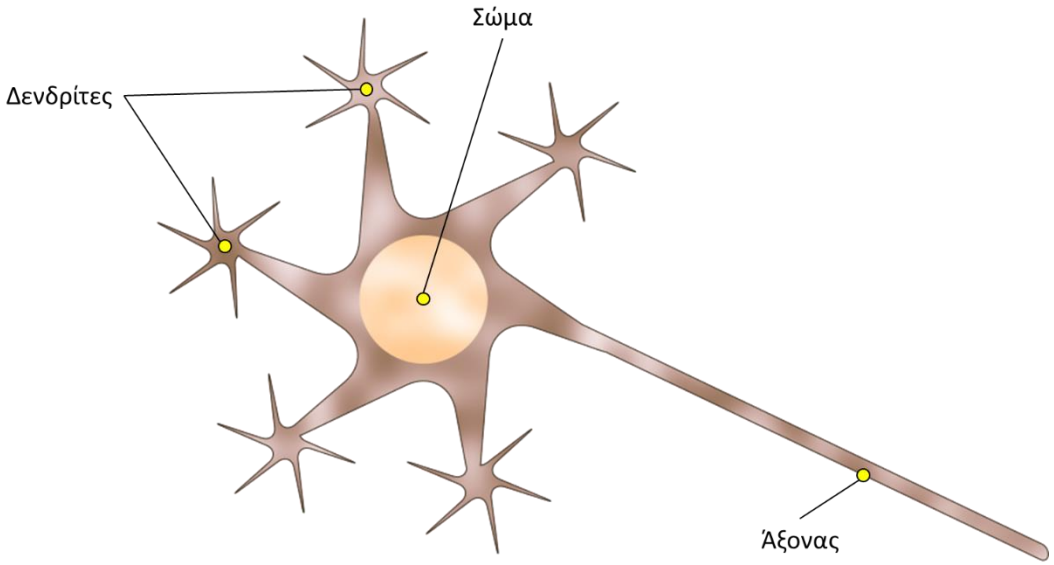
2.2.5 Τεχνητά Νευρωνικά Δίκτυα

Ο όρος “Τεχνητό Νευρωνικό Δίκτυο” (ΤΝΔ) αναφέρεται σε ένα δίκτυο συνδεδεμένων τεχνητών νευρώνων, απευθείας εμπνευσμένο από τη δομή των βιολογικών νευρωνικών δικτύων που συναντώνται στο νευρικό σύστημα των οργανισμών. Στο πλαίσιο της Τεχνητής Νοημοσύνης, τα τεχνητά νευρωνικά δίκτυα αναπτύσσονται με σκοπό να προσομοιώσουν τη λειτουργία των βιολογικών νευρώνων μέσω υπολογιστικών αλγορίθμων. Ο στόχος αυτών των δικτύων είναι να αντιμετωπίσουν πολύπλοκα προβλήματα μέσω της εφαρμογής αλγοριθμικών τεχνικών που εμπνέονται από τη λειτουργία του εγκεφάλου. Αυτό επιτυγχάνεται μέσω της μαθηματικής προσομοίωσης της λειτουργίας των βιολογικών νευρώνων, τους οποίους αντιμετωπίζουν ως λειτουργικές μονάδες και δικτυακές δομές [36]. Οι τεχνητοί νευρώνες είναι γνωστοί ως "αντιληπτήρες" (*μτφρ. perceptrons*) (Chen, et al. 2019).

Τα τεχνητά νευρωνικά δίκτυα διαθέτουν τη δυνατότητα να παράγουν ασφαλή συμπεράσματα με εξαιρετική ακρίβεια, ακόμα και σε περιπτώσεις όπου στην είσοδό τους λαμβάνουν περιορισμένες πληροφορίες. Στόχος τους είναι η ανάκληση ή/και η αντιστοίχιση πληροφοριών μετά από την αξιολόγηση και επεξεργασία των πληροφοριών που έλαβαν ως είσοδο. Παρόμοια με τα βιολογικά νευρωνικά δίκτυα και τους νευρώνες τους, τα τεχνητά νευρωνικά δίκτυα διακινούν πληροφορίες στο εσωτερικό τους, ανταλλάσσοντας πληροφορίες μέσω των συνάψεων που συνδέουν τους αντιληπτήρες μεταξύ τους. Στην ψηφιακή τους μορφή, σε κάθε σύναψη αντιστοιχεί ένα *συναπτικό βάρος* (Chen, et al. 2019).

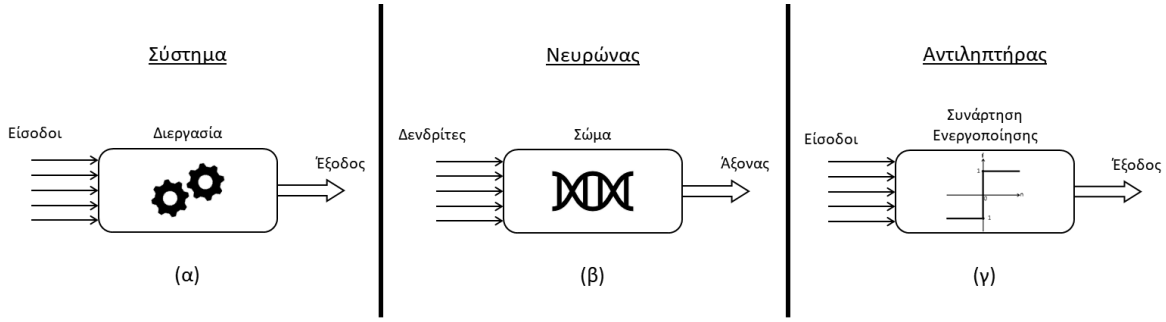
Καθώς τα τεχνητά νευρωνικά δίκτυα προσομοιώνουν τη δομή και λειτουργία των βιολογικών νευρωνικών δικτύων, είναι σημαντικό να αναδειχθεί η σχετική αναλογία, προκειμένου να διευκολυνθεί η κατανόηση της λειτουργίας των συγκεκριμένων αλγορίθμων. Ένας νευρώνας αποτελεί μία βιολογική επεξεργαστική μονάδα πληροφοριών. Παρά την πολυπλοκότητα του, μπορούμε να ξεχωρίσουμε τρία βασικά τμήματα που τον απαρτίζουν (Chen, et al. 2019)(**Εικόνα 2.15**):

- τους **δενδρίτες**, οι οποίοι αποτελούν δέκτες των εισερχόμενων πληροφοριών,
- το κυρίως **σώμα** που περιέχει τον **πυρήνα**, ο οποίος αποτελεί μια μονάδα επεξεργασίας των παραμέτρων του κάθε εισερχόμενης πληροφορίας, και
- τον **άξονα**, ο οποίος λειτουργεί ως δίαυλος επικοινωνίας, μεταφέροντας τα παραγόμενα αποτελέσματα προς άλλους δενδρίτες, μέσω των ενδιάμεσων συνάψεων του νευρικού δικτύου που τους συνδέουν μεταξύ τους.



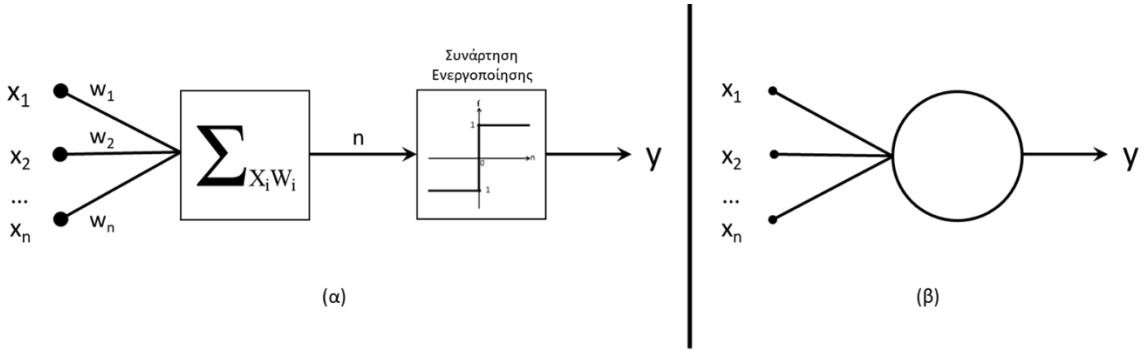
Εικόνα 2.15: *Αναπαράσταση βιολογικού νευρώνα*

Στο πεδίο των τεχνητών νευρωνικών δικτύων, ο αντιληπτήρας, ως οντότητα, αποτελεί την απλούστερη δομή ΤΝΔ (**Εικόνα 2.16**). Όπως προκύπτει, τόσο οι βιολογικοί νευρώνες όσο και οι τεχνητοί (αντιληπτήρες) είναι συστήματα πολλών εισόδων - μίας εξόδου (multiple inputs/single output - MISO).



Εικόνα 2.16: *Αναλογία τυπικού συστήματος με βιολογικό νευρώνα και αντιληπτήρα*

Όσον αφορά τη λειτουργία ενός αντιληπτήρα, αυτή είναι απλή: κάθε σήμα εισόδου x_i πολλαπλασιάζεται με ένα αντίστοιχο συναπτικό βάρος w_i. Στη συνέχεια οδηγούνται σε έναν αθροιστή, το αποτέλεσμα του οποίου ονομάζεται *σταθμισμένο άθροισμα* (net input) και οδηγείται σε επόμενη βαθμίδα όπου βρίσκεται μια συνάρτηση ενεργοποίησης. Η συνάρτηση αυτή είναι εκείνη που θα καθορίσει την τελική έξοδο του αντιληπτήρα, βάσει της εισόδου που δέχθηκε (Chen, et al. 2019) (**Εικόνα 2.17**).



Εικόνα 2.17: *Απεικόνιση λειτουργίας αντιληπτήρα και τυπικό σχήμα του*

Ο σκοπός ενός αντιληπτήρα είναι να επιλύει ζητήματα ταξινόμησης, προσφέροντας εξόδους εντός αποδεκτών ορίων για κάθε δυνατό συνδυασμό εισερχομένων διανυσμάτων. Ο Frank Rosenblatt απέδειξε ότι όταν ένας αντιληπτήρας καταφέρνει να διαχωρίζει κλάσεις, τότε ο αλγόριθμος εκπαίδευσης συγκλίνει και επιστρέφει ορθά αποτελέσματα μέσα σε πεπερασμένο αριθμό βημάτων. Αυτό το θεώρημα είναι γνωστό ως «Θεώρημα Σύγκλισης του Αντιληπτήρα» και αποτελεί κανόνα διόρθωσης σφαλμάτων. Τα δε συναπτικά βάρη διαδραματίζουν σημαντικό ρόλο στην αποτελεσματικότητα ενός αντιληπτήρα. Οι τιμές αυτών των βαρών καθορίζουν τον βαθμό συμμετοχής κάθε μίας εισόδου στο σταθμισμένο άθροισμα. Προς επίτευξη της μέγιστης δυνατής ακρίβειας στα αποτελέσματα ενός αντιληπτήρα, και κατά συνέπεια ενός τεχνητού νευρωνικού δικτύου, είναι απαραίτητο να προσδιοριστούν με ακρίβεια όλα τα συναπτικά βάρη. Σε ένα τεχνητό νευρωνικό δίκτυο, το οποίο αποτελείται από μεγάλο αριθμό αντιληπτήρων, αυτό επιτυγχάνεται μέσω κατάλληλων μεθόδων μηχανικής μάθησης (Chen, et al. 2019).

Ως προς την αρχιτεκτονική τους, τα Τεχνητά Νευρωνικά Δίκτυα απαρτίζονται αρχικά από το *επίπεδο* ή *στρώμα* (*μτφρ. layer*) *εισόδων* και ακολούθως από ένα ή περισσότερα επίπεδα αντιληπτήρων. Ως επίπεδο ορίζεται κάθε ιεραρχική "στρώση" από νευρώνες που εργάζονται μαζί για να επεξεργαστούν δεδομένα. Το τελευταίο ιεραρχικό επίπεδο αντιληπτήρων ονομάζεται *επίπεδο εξόδων*. Ανάλογα με τον αριθμό των επιπέδων που περιέχουν αντιληπτήρες, τα τεχνητά νευρωνικά δίκτυα διακρίνονται σε μονοστρωματικά και πολυστρωματικά. Τονίζεται εδώ ότι το επίπεδο εισόδων εξαιρείται της καταμέτρησης καθότι δεν απαρτίζεται από αντιληπτήρες. Στα πολυστρωματικά τεχνητά νευρωνικά δίκτυα, κάθε επίπεδο αντιληπτήρων μεταξύ του επιπέδου εισόδου και του επιπέδου εξόδου θεωρείται ως *κρυφό επίπεδο*. Τα τεχνητά νευρωνικά δίκτυα, κατηγοριοποιούνται βάσει ροής της πληροφορίας εντός τους ως εξής (Chen, et al. 2019):

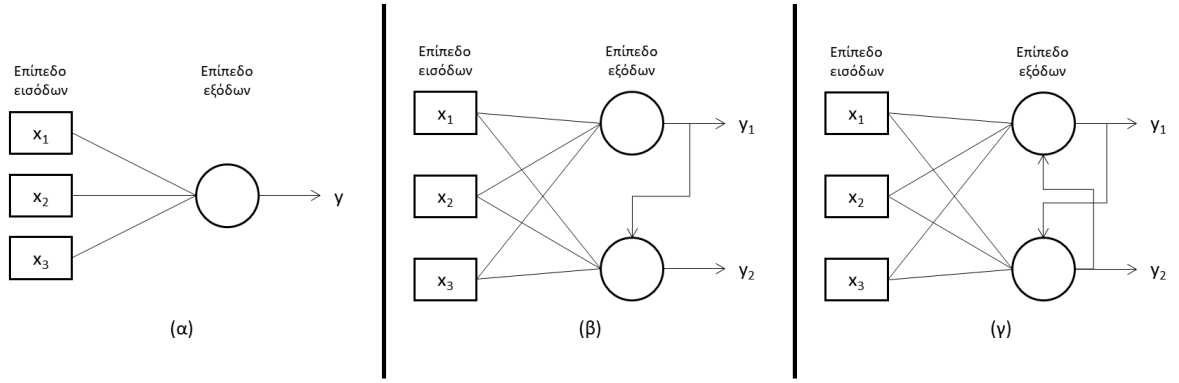
1. Πρόσθιας τροφοδότησης (*μτφρ. feed forward*): η ροή της πληροφορίας γίνεται από τις εξόδους των αντιληπτήρων ενός επιπέδου προς τις εισόδους των αντιληπτήρων του επόμενου.
2. Οπισθοδιάδοσης (*μτφρ. feedback*): η ροή της πληροφορίας γίνεται από τις εξόδους των αντιληπτήρων ενός επιπέδου προς τις εισόδους των αντιληπτήρων του επόμενου αλλά και προς εισόδους αντιληπτήρων μη-επόμενου επιπέδου. Εάν οι έξοδοι των αντιληπτήρων κάθε επιπέδου συνδέονται με μερικές μόνο εισόδους των μη επόμενων επιπέδων τότε έχουμε ένα *μερικώς συνδεδεμένο νευρωνικό δίκτυο* (partially connected neural network). Αντιθέτως, εάν όλοι οι έξοδοι των αντιληπτήρων κάθε επιπέδου συνδέονται με όλες τις εισόδους αντιληπτήρων κάθε μη-επόμενου επιπέδου, τότε έχουμε ένα *πλήρως συνδεδεμένο νευρωνικό δίκτυο* (fully connected neural network).

Στην **Εικόνα 2.18** παρουσιάζονται τρεις αντιληπτήρες ως μονοστρωματικά ΤΝΔ, τα οποία διαθέτουν μόνο 3 εισόδους προς χάριν απλούστευσης:

α. Μονοστρωματικό ΤΝΔ με πρόσθια τροφοδότηση.

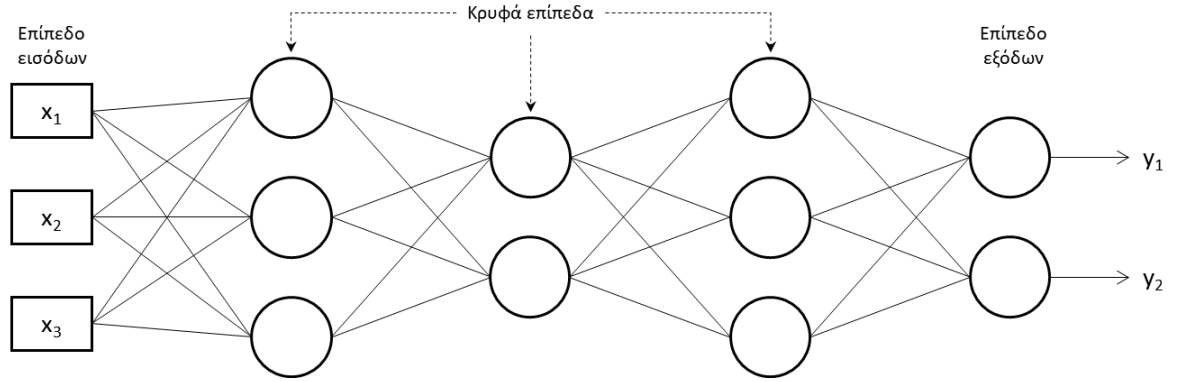
β. Μονοστρωματικό ΤΝΔ με μερική οπισθοδιάδοση .

γ. Μονοστρωματικό ΤΝΔ με πλήρη οπισθοδιάδοση.



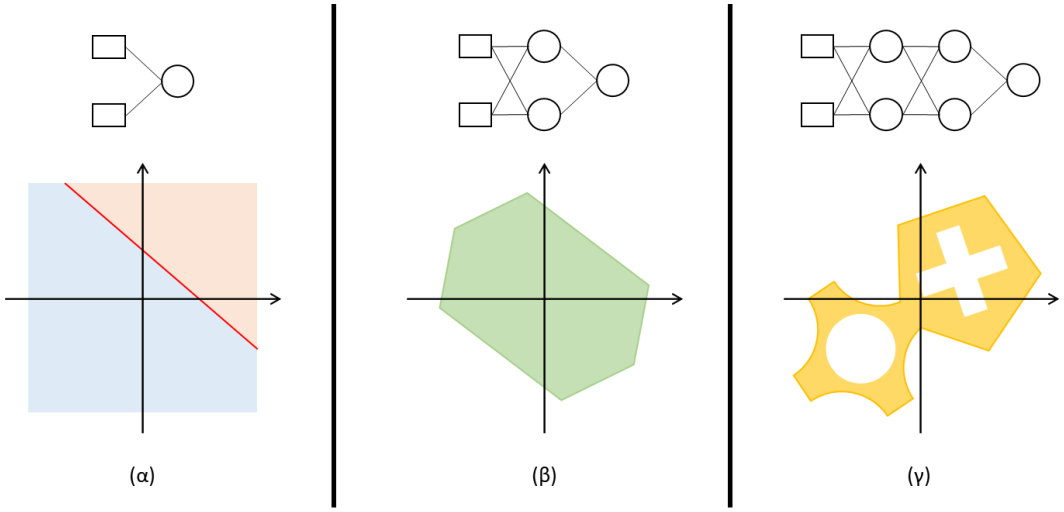
Εικόνα 2.18: *Παραδείγματα μονοστρωματικών ΤΝΔ*

Στην **Εικόνα 2.19** απεικονίζεται σχηματικά ένα πολυστρωματικό ΤΝΔ με πρόσθια τροφοδότηση, που αποτελείται από τέσσερα επίπεδα: τρία "κρυφά" και ένα για τις εξόδους.



Εικόνα 2.19: *Παράδειγμα πολυστρωματικού ΤΝΔ*

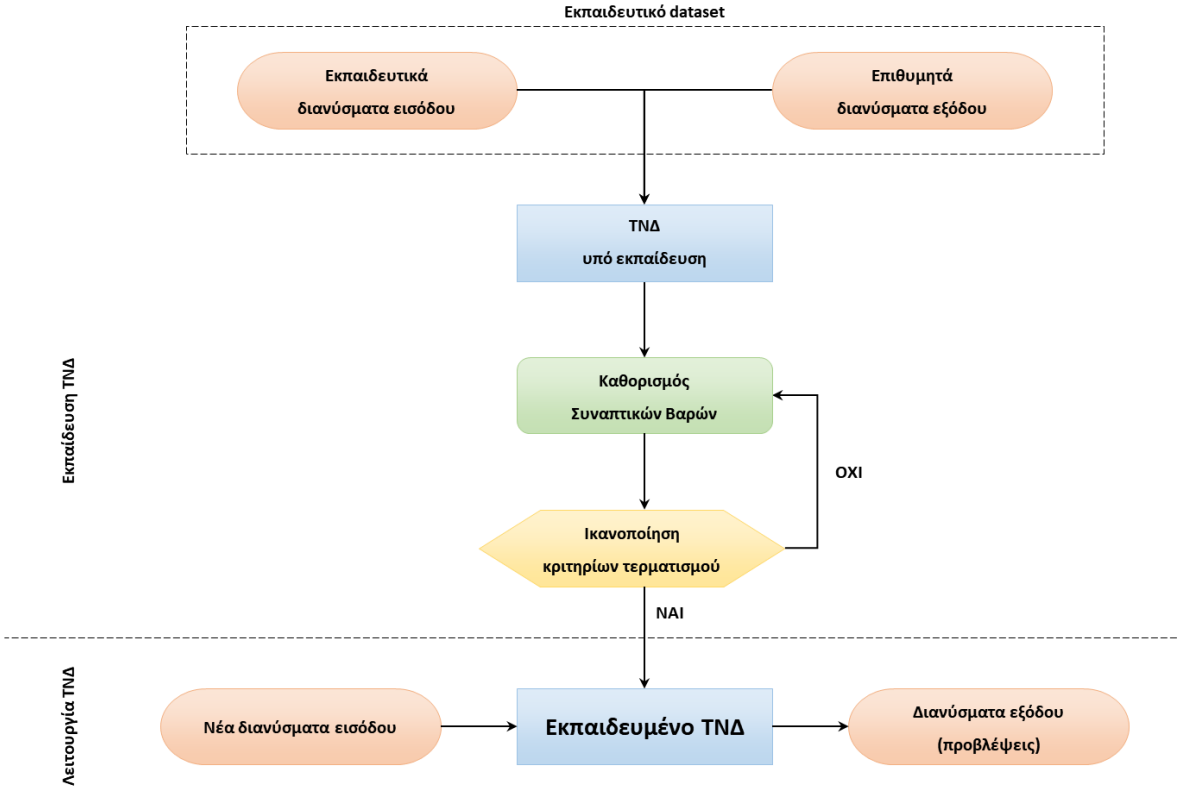
Τα μονοστρωματικά νευρωνικά δίκτυα δημιουργούν γραμμικά όρια, γι' αυτό και αξιοποιούνται σε απλούστερες σχετικά εφαρμογές, όπως η ταξινόμηση (classification). Τα τεχνητά νευρωνικά δίκτυα που αποτελούνται από περισσότερα επίπεδα μπορούν να συνδυάζουν γραμμικά όρια και να επιλύουν μη-γραμμικά προβλήματα ταξινόμησης. Όπως παρατηρείται στα σχήματα που παρουσιάζονται στην **Εικόνα 2.20**, το μονοστρωματικό ΤΝΔ (αντιληπτήρας) δημιουργεί ένα γραμμικό όριο (α), ενώ ένα πολυστρωματικό νευρωνικό δίκτυο δύο επιπέδων μπορεί να συνδυάσει γραμμικά όρια (β) σχηματίζοντας περιοχές ορίων. Από τα παραπάνω συμπεραίνουμε ότι όσο αυξάνονται τα κρυφά επίπεδα ενός ΤΝΔ, τόσο αυξάνεται η πολυπλοκότητα των σχημάτων που δημιουργούνται, όχι μόνο σε δύο αλλά σε πολύ περισσότερες διαστάσεις (γ). Σημειώνεται εδώ ότι τα σχήματα (β) και (γ) είναι ενδεικτικά για λόγους κατανόησης των ανωτέρω και το πλήθος των επιπέδων κάθε παραδείγματος δεν ανταποκρίνονται απαραίτητα στα αντίστοιχα σχήματα που παρατίθενται.



Εικόνα 2.20: *Ενδεικτικές αναπαραστάσεις εξόδων βάσει αρχιτεκτονικής ΤΝΔ*

Ανεξάρτητα από το είδος ενός τεχνητού νευρωνικού δικτύου, είτε η δομή του είναι μονοστρωματική είτε πολυστρωματική, στη θεωρία δεν υπάρχει ανώτατο όριο στον αριθμό των επιπέδων ή/και των νευρώνων που απαρτίζουν το καθένα από αυτά. Το ίδιο και για τον αριθμό των εισόδων και εξόδων του συστήματος. Ωστόσο, στην πράξη, αυτοί οι αριθμοί υπόκεινται σε περιορισμούς, τόσο λόγω της ανάγκης βελτιστοποίησης του σχεδιαζόμενου τεχνητού νευρωνικού δικτύου όσο και λόγω των περιορισμών στην επεξεργαστική ισχύ και τον χρόνο εκπαίδευσης που απαιτούνται για την εκπαίδευση και λειτουργία του (Chen, et al. 2019).

Η εκπαίδευση ενός τεχνητού νευρωνικού δικτύου εστιάζει στη διαδικασία καθορισμού των τιμών των συναπτικών του βαρών (*μτφρ. synaptic weights*), έτσι ώστε όταν εισάγεται ένα διάνυσμα εισόδου στο σύστημα να παράγεται ένα ακριβές αποτέλεσμα στην έξοδό του. Η εκπαίδευση μπορεί να πραγματοποιηθεί τόσο με μεθόδους επιτηρούμενης μάθησης όσο και με μη-επιτηρούμενης. Τα συναπτικά βάρη, ή αλλιώς *συντελεστές βάρους* (*μτφρ. weight coefficients*), αποτελούν την κωδικοποιημένη γνώση που αποκτά το νευρωνικό δίκτυο ως εμπειρία. Αυτή η γνώση αποκτάται μέσω της εκπαίδευσης αλλά και της αλληλεπίδρασης του συστήματος με το περιβάλλον κατά την επιχειρησιακή του λειτουργία. Τα συναπτικά βάρη αποτελούν το χαρακτηριστικό που προσδίδει σε ένα νευρωνικό δίκτυο την ικανότητα να αναπροσαρμόζεται και να εξελίσσεται. Η διαδικασία εκπαίδευσης κάνει χρήση εξειδικευμένων αλγορίθμων οι οποίοι ονομάζονται "*κανόνες μάθησης*" και οι οποίοι εργάζονται επαναληπτικά για τη βελτίωση της τελικής απόδοσης του συστήματος. Μετά από κάθε επανάληψη, αξιολογείται η ακρίβεια της εξόδους και τα συναπτικά βάρη αναπροσαρμόζονται ώστε στην επόμενη να προσεγγίσουν ακόμα περισσότερο τις επιθυμητές τιμές εξόδου. Με αυτόν τον τρόπο το εκπαιδευόμενο σύστημα ενισχύει και εμπλουτίζει την αποκτηθείσα γνώση του και την αποθηκεύει εσωτερικά. Η διαδικασία εκπαίδευσης ολοκληρώνεται όταν δεν προκύπτει η περαιτέρω ανάγκη για αναπροσαρμογή των συναπτικών βαρών ή αφού παρέλθει ένας προκαθορισμένος αριθμός επαναλήψεων. Η μέθοδος εκπαίδευσης που θα επιλεγεί εξαρτάται από την αρχιτεκτονική του νευρωνικού δικτύου αλλά και από την εφαρμογή την οποία θα κληθεί να εξυπηρετήσει κατά την επιχειρησιακή του λειτουργία (Chen, et al. 2019).



Εικόνα 2.21: *Τυπικό διάγραμμα εκπαίδευσης και λειτουργίας ΤΝΔ*

Αφού ολοκληρωθεί η διαδικασία της εκπαίδευσης, το τεχνητό νευρωνικό δίκτυο είναι έτοιμο να τεθεί σε λειτουργία και να παράξει ακριβείς εξόδους, αξιοποιώντας την ικανότητά του να ανακτά πληροφορίες από τη μνήμη του. Η διαδικασία αυτή ονομάζεται "*ανάκληση*" (*μτφρ. recall*) και πιο συγκεκριμένα αφορά τον υπολογισμό του διανύσματος εξόδου για ένα συγκεκριμένο διάνυσμα εισόδου (**Εικόνα 2.21**).

Τα τεχνητά νευρωνικά δίκτυα έχουν τη δυνατότητα να γενικεύουν, κυρίως όταν δεν λαμβάνουν στην είσοδό τους διανύσματα τιμών τα οποία ούτε «διδάχτηκαν» κατά την εκπαίδευσή τους, ούτε ενσωματώθηκαν ως αποκτηθείσα εμπειρία κατά την επιχειρησιακή τους λειτουργία. Συνεπώς, η ικανότητα της γενίκευσης ενός ΤΝΔ αφορά την επιτυχή παραγωγή εξόδων όχι μόνο για τα συγκεκριμένα διανύσματα εισόδου που έχει «κατανοήσει», αλλά και για διανύσματα εισόδου που δεν έχει «συναντήσει» προηγουμένως. Η ικανότητα αυτή επηρεάζεται από διάφορους παράγοντες, μεταξύ των οποίων είναι η πολυπλοκότητα του προβλήματος, το μέγεθος και η αρχιτεκτονική του ΤΝΔ, όπως επίσης και τα ποιοτικά και ποσοτικά χαρακτηριστικά των δεδομένων που χρησιμοποιήθηκαν ως υλικό εκπαίδευσης.

Πολλά συστήματα, τίθενται εκτός λειτουργίας εάν υποστούν βλάβη έστω και σε ένα μικρό εξάρτημά τους. Τα ΤΝΔ ωστόσο επιδεικνύουν ανοχή, όχι μόνο σε βλάβες που μπορεί να παρουσιαστούν αλλά ακόμα και σε θόρυβο. Αυτό οφείλεται στο γεγονός ότι η πληροφορία βρίσκεται κατανεμημένη σε διάφορα σημεία του Δικτύου. Εάν ένας νευρώνας υποστεί βλάβη, η απόδοση του συστήματος πράγματι επηρεάζεται αρνητικά, αλλά σε βαθμό που θεωρείται αμελητέος. Για να θεωρήσουμε ότι ένα ΤΝΔ έχει υποστεί βλάβη, αυτή θα πρέπει να είναι εξαιρετικά εκτεταμένη, σε βαθμό που η ακρίβεια των αποτελεσμάτων να έχει μειωθεί σημαντικά και να βρίσκονται εκτός αποδεκτών ορίων (Chen, et al. 2019).

Οι δυνατότητες των ΤΝΔ τα καθιστούν ένα αξιόπιστο αλλά και ευέλικτο εργαλείο το οποίο βρίσκει εφαρμογή σε ένα ευρύτατο σύνολο περιπτώσεων χρήσης. Ενδεικτικά:

- **Αεροδιαστημική:** προσομοιωτές πτήσεων, έλεγχος αεροσκάφους, ανίχνευση βλαβών, κ.λπ.
- **Βιομηχανία:** διάγνωση βλαβών, ποιοτικός έλεγχος, έλεγχος διεργασιών, κ.λπ.
- **Ηλεκτρονική:** τεχνητή όραση, πρόβλεψη ακολουθίας κωδικών, κ.λπ.
- **Ιατρική:** πρόβλεψη ή εκτίμηση της αντίδρασης έμβιων οργανισμών σε νέες φαρμακευτικές ουσίες, ανάλυση συμπτωμάτων, κ.λπ.
- **Οικονομικά:** αξιολόγηση αιτήσεων τραπεζικών δανείων, πρόβλεψη δεικτών χρηματιστηρίου, κ.λπ.
- **Τυχερά παίγνια («τζόγος»):** πρόβλεψη ενδιάμεσων και τελικών αποτελεσμάτων αγώνων, κ.λπ.

3 Κρυπτογραφία

Η κρυπτογραφία αποτελεί μια ιδιαίτερα σημαντική περιοχή της επιστήμης της πληροφορικής και της κυβερνοασφάλειας, η οποία στοχεύει στην εξασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων και των πληροφοριών[2], αλλά και τη δυνατότητα λογοδοσίας/καταλογισμού ευθυνών μέσω της διάστασης της μη-αποποίησης (non-repudiation). Στην κορυφή της υπάρχει η αρχή της ασφαλούς επικοινωνίας μεταξύ δύο ή περισσότερων φορέων, οι οποίοι επιθυμούν να ανταλλάξουν πληροφορίες σε ένα περιβάλλον που μπορεί να είναι εχθρικό ως προς τη διακίνηση των διακινούμενων πληροφοριών, συμπεριλαμβάνοντας υποκλοπή ή παρεμπόδιση της επικοινωνίας, αλλοίωση των δεδομένων ή έγχυση πλαστών δεδομένων, αντιποίηση ταυτότητας κ.λπ. (Sharma and Gupta 2017).

Για την επίτευξη αυτού του σκοπού, η κρυπτογραφία αξιοποιεί μια σειρά από μαθηματικές μεθόδους και αλγόριθμους που επιτρέπουν τη μετατροπή των αρχικών, «ανοιχτών» (μη κρυπτογραφημένων) κειμένων σε κρυπτογραφημένη μορφή, μη κατανοητή για τους μη εξουσιοδοτημένους παραλήπτες. Από την άλλη, ο εκάστοτε εξουσιοδοτημένος παραλήπτης, διαθέτοντας το κατάλληλο κρυπτογραφικό κλειδί, μπορεί στη συνέχεια να αποκωδικοποιήσει τα δεδομένα και να τα επιστρέψει στην αρχική τους μορφή (Sharma and Gupta 2017).

Η κρυπτογραφία δεν είναι σημαντική μόνο για την εγγύηση της ασφαλούς επικοινωνίας στα δίκτυα, αλλά είναι ουσιαστική και για πολλές άλλες εφαρμογές στον ψηφιακό κόσμο, όπως η ηλεκτρονική συναλλαγή, η ασφαλής αποθήκευση δεδομένων, οι ψηφιακές υπογραφές και η προστασία της ιδιωτικότητας. Επίσης, παίζει κεντρικό ρόλο σε σύγχρονες τεχνολογίες όπως τα Blockchain, τα κρυπτονομίσματα και τα συστήματα ομομορφικής κρυπτογράφησης, που επιτρέπουν πιο προχωρημένες μορφές ασφαλούς και απρόσκοπτης υπολογιστικής διαδικασίας. Έτσι, η κρυπτογραφία αποτελεί έναν απαραίτητο πυλώνα για την ανάπτυξη και τη διάδοση των ψηφιακών τεχνολογιών και εξυπηρετεί ως ένα από τα βασικά εργαλεία για την ενίσχυση της κυβερνοασφάλειας στον σύγχρονο κόσμο (Sharma and Gupta 2017).

3.1 Βασικές έννοιες

Κρυπτανάλυση: Η κρυπτανάλυση είναι η διαδικασία αποκρυπτογράφησης ή αποκωδικοποίησης ενός κρυπτογραφημένου μηνύματος χωρίς τη γνώση του κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση ή και του αλγορίθμου (Schaefer 2009). Αυτό συνήθως επιτυγχάνεται μέσω της ανάλυσης των συστατικών στοιχείων του κρυπτογραφημένου μηνύματος, της εφαρμογής μαθηματικών αλγορίθμων και της εκμετάλλευσης πιθανών αδυναμιών στο σύστημα κρυπτογράφησης.

Κρυπτολογία: Η κρυπτολογία είναι η επιστήμη που μελετά την ασφαλή επικοινωνία σε περιβάλλοντα όπου υπάρχουν αντίπαλοι. Περιλαμβάνει την κρυπτογραφία, που είναι η τέχνη της δημιουργίας κρυπτογραφημάτων, και την κρυπτανάλυση, που είναι η τέχνη της αποκρυπτογράφησης κρυπτογραφημάτων χωρίς την κατοχή γνώσης για τους αλγόριθμους κρυπτογράφησης ή τα κλειδιά. Η κρυπτολογία είναι ζωτικής σημασίας για την προστασία των δεδομένων στον ψηφιακό κόσμο (Schaefer 2009).

[2] Η διάσταση της διαθεσιμότητας υποστηρίζεται μέσω της παροχής εγγυήσεων ότι όσοι διαθέτουν την κατάλληλη εξουσιοδότηση μπορούν να χρησιμοποιήσουν συστήματα και να ανακτήσουν δεδομένα αξιόπιστα και έγκαιρα.

Συμμετρική κρυπτογράφηση: Η συμμετρική κρυπτογράφηση είναι μια μέθοδος κρυπτογράφησης που χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων (Schaefer 2009). Αυτό σημαίνει ότι το κλειδί πρέπει να είναι γνωστό και από τις δύο πλευρές: τον αποστολέα και τον παραλήπτη. Είναι γρήγορη και αποτελεσματική, αλλά εγείρονται ζητήματα για τον τρόπο διανομής του κλειδιού στα εμπλεκόμενα μέρη ή τη συμφωνία πάνω σε αυτό, ενώ δεν μπορεί να υποστηρίξει και τη διάσταση της λογοδοσίας/καταλογισμού.

Ασύμμετρη κρυπτογράφηση: Η ασύμμετρη κρυπτογράφηση είναι μια μέθοδος κρυπτογράφησης που χρησιμοποιεί δύο διαφορετικά κλειδιά: ένα δημόσιο κλειδί για την κρυπτογράφηση των δεδομένων και ένα ιδιωτικό κλειδί για την αποκρυπτογράφησή τους. Αυτό επιτρέπει στα δεδομένα να μεταδίδονται με ασφάλεια, ακόμη και σε μη ασφαλή δίκτυα, καθώς δεδομένα που έχουν κρυπτογραφηθεί με το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν μόνον από τον κάτοχο του δημόσιου κλειδιού.

Κατακερματισμός (*μτφρ. hashing*)**:** ονομάζεται η διαδικασία παραγωγής μιας συμβολοσειράς συγκεκριμένου μήκους (hash) που προκύπτει από υπολογιστικές κρυπτογραφικές συναρτήσεις οι οποίες χρειάζεται να λάβουν στην είσοδό τους ένα σύνολο δεδομένων. Η διαφοροποίηση στα δεδομένα εισόδου, έχει ως αποτέλεσμα μία διαφορετική έξοδο, ενώ είναι επιθυμητό μικρές "τοπικές" διαφοροποιήσεις στα δεδομένα να οδηγούν σε εκτεταμένες καθολικές διαφοροποιήσεις στο αποτέλεσμα, προκειμένου να μειώνεται η ικανότητα κρυπτανάλυσης. Η τεχνολογία Blockchain αξιοποιεί τέτοιες συναρτήσεις για την ασφαλή αποθήκευση και την επαλήθευση των δεδομένων. Το παραγόμενο hash συνοδεύει τα δεδομένα από τα οποία προέκυψε και μπορεί να χαρακτηριστεί ως το «δακτυλικό αποτύπωμά τους.

Ακεραιότητα (*μτφρ. integrity*)**:** αναφέρεται στη διασφάλιση ότι τα δεδομένα δεν έχουν τροποποιηθεί κατά τη μεταφορά τους ή την αποθήκευσή τους.

Αυθεντικοποίηση (*μτφρ. authentication*)**:** αναφέρεται στη διασφάλιση ότι τα μηνύματα προέρχονται όντως από τον φερόμενο ως αποστολέα, ο οποίος τυπικά αντιστοιχεί σε μια έγκυρη/νόμιμη πηγή.

Ψηφιακή υπογραφή (*μτφρ. Digital signature*)**:** Η ψηφιακή υπογραφή είναι μια τεχνική που συνδυάζει τις δύο προηγούμενες έννοιες, επιτρέποντας την αυθεντικοποίηση του αποστολέα και τη διασφάλιση της ακεραιότητας του μηνύματος.

Ανωνυμία (*μτφρ. anonymity*): αναφέρεται στη διασφάλιση ότι οι εμπλεκόμενοι σε μια επικοινωνία μπορούν να παραμείνουν ανώνυμοι, προστατεύοντας την προσωπική τους ταυτότητα.

3.2 Ιστορική παρουσία

Η κρυπτογραφία, η τέχνη της προστασίας των μυστικών με τη χρήση τεχνικών, κωδικών και κρυπτογραφημάτων, ξεκίνησε πριν από χιλιάδες χρόνια. Οι πρώτες μορφές κρυπτογραφίας μπορούν να εντοπιστούν στην αρχαία Αίγυπτο, όπως φαίνεται από ιερογλυφικές επιγραφές σε τάφο της Παλαιάς Βασιλείας περίπου το 1900 π.Χ., στις οποίες χρησιμοποιούνταν μη τυποποιημένα ιερογλυφικά σύμβολα, των οποίων η σημασία ήταν γνωστή μόνο σε ένα στενό κύκλο μυημένων. Αν και αυτές οι επιγραφές δεν θεωρούνται σύνθετες κρυπτογραφικές τεχνικές με στόχο την ασφαλή επικοινωνία, παρέχουν σημαντική ένδειξη για το πώς η ανθρωπότητα άρχισε να εξερευνά τις δυνατότητες της τήρησης μυστικών και της χρήσης συμβόλων. Οι ιερογλυφικές αυτές επιγραφές θεωρούνται συχνά ως προσπάθειες για δημιουργία μυστηρίου, ενδιαφέροντος, ή ακόμη και

διασκέδασης για τους γραμματισμένους παρατηρητές. Οι ιστορικοί και οι επιστήμονες των κρυπτογραφικών συστημάτων σημειώνουν ότι αυτές οι αρχαίες μορφές "κρυπτογραφίας" ήταν περισσότερο καλλιτεχνικές ή ρητορικές, παρά πρακτικές τεχνικές για την ασφάλεια της επικοινωνίας. Είναι πιθανό να χρησιμοποιούνταν για λόγους που σχετίζονται με τις θρησκευτικές ή κοινωνικές τελετουργίες της εποχής. Επιπροσθέτως, τα ιερογλυφικά συστήματα της αρχαίας Αιγύπτου ήταν αυστηρά δομημένα και γνωστά μόνο σε μια ελίτ εκπαιδευμένων γραμματέων, πράγμα που τα καθιστούσε ιδανικά για την εισαγωγή εσωτερικών συμβόλων ή εναλλακτικών ερμηνειών (Dooley, 2018).

Στην αρχαία Ελλάδα, συναντάμε πλήθος επικοινωνιακών συστημάτων μετάδοσης κρυφών μηνυμάτων. Η φρυκτωρίες (1100 - 500 π.Χ.), για παράδειγμα, ήταν ένα αρχαίο σύστημα οπτικής επικοινωνίας που χρησιμοποιούσε φλεγόμενους πυρσούς ή δαυλούς για τη μετάδοση μηνυμάτων σε μακρινές αποστάσεις. Η εφεύρεση της φρυκτωρίας αποδίδεται στον μυθικό ήρωα Παλαμήδη, κατά την περίοδο του Τρωικού Πολέμου. Κατασκευασμένο κυρίως για στρατιωτικούς σκοπούς, το δίκτυο φρυκτωριών αποτελούσε από σταθμούς που τοποθετούνταν σε υψηλά σημεία, όπως βουνοκορυφές, ώστε να είναι ορατοί μεταξύ τους. Ο φύλακας του φρυκτωρίου, ο «φρυκτωρός», ήταν υπεύθυνος για την ανάφλεξη του πυρσού και τη μετάδοση του σήματος. Παρόμοια συστήματα χρησιμοποιήθηκαν από τους Πέρσες, τους Ρωμαίους, και τους Βυζαντινούς. Στη Βυζαντινή Αυτοκρατορία, για παράδειγμα, το σύστημα ονομαζόταν «καμινοβίγλιο» και είχε τη δυνατότητα να μεταδώσει μηνύματα σε αποστάσεις περίπου 700 χιλιομέτρων μέσα σε μία ώρα, χάρη σε έναν εξελιγμένο κώδικα που επινοήθηκε από τον Λέοντα τον Φιλόσοφο (Dooley 2018).

Ως μετεξέλιξη των φρυκτωριών, δημιουργήθηκαν τα «πυρσεία», ένα σύστημα που δημιουργήθηκε από τους Αλεξανδρινούς μηχανικούς Κλεόξενο και Δημόκλειτο τον 2ο αιώνα π.Χ. Το σύστημα επέτρεπε τη μετάδοση πληροφοριών γράμμα-γράμμα μεταξύ αποστολέα και παραλήπτη μέσω οπτικών σημάτων. Στηρίχτηκε στην τεχνική αντιστοίχισης πυρσών με γράμματα του ελληνικού αλφαβήτου, χρησιμοποιώντας το Τετράγωνο του Πολύβιου για την κωδικοποίηση των μηνυμάτων. Κάθε σταθμός της πυρσείας είχε δύο τοίχους που φιλοξενούσαν πέντε πυρσούς ο καθένας, και το σύστημα χρησιμοποιούσε φωτεινά σήματα για τη μετάδοση των μηνυμάτων. Θεωρείται ο πρόδρομος του τηλέγραφου και αποτελεί ένα πρωτοποριακό βήμα στην ιστορία των τηλεπικοινωνιών (Dooley 2018).

Η «Κρυπτεία σκυτάλη» ή «Λακεδαιμονική σκυτάλη» αναφέρεται πρώτη φορά από τον λυρικό ποιητή Αρχίλοχο τον 7ο π.Χ. αιώνα και έχει τις ρίζες της στην αρχαία Σπάρτη. Χρησιμοποιούσε τη μέθοδο της μετάθεσης, όπου το κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση αποτελούσε το σχήμα και η περιφέρεια της σκυτάλης, που θα μπορούσε να έχει διάφορες γεωμετρικές μορφές (κυκλική, εξαγωνική κ.λπ.). Στην πράξη, η σκυτάλη κόβονταν σε δύο μέρη. Το ένα μέρος το φύλαγαν οι έφοροι της Σπάρτης και το άλλο το έπαιρνε ο αρχηγός του στρατεύματος. Για την επικοινωνία, τυλίγονταν μια λωρίδα υφάσματος γύρω από το κομμάτι της σκυτάλης και γράφονταν μηνύματα με προκαθορισμένο τρόπο, όπως για παράδειγμα με την βοήθεια ενός καθρέφτη. Ο παραλήπτης, μπορούσε να αποκρυπτογραφήσει το μήνυμα εύκολα τυλίγοντας τη λωρίδα υφάσματος που λάμβανε στο δικό του κομμάτι της σκυτάλης (Dooley 2018).

Η μέθοδος του "Κωδικού Μοιρογνωμονίου" χρονολογείται από τον 4ο αιώνα π.Χ. και αποτελεί άλλη μία από τις πρώτες προσπάθειες για ασφαλή επικοινωνία. Η μέθοδος αυτή χρησιμοποιούσε έναν δίσκο διαμέτρου 8-10 εκατοστών, ο οποίος είχε μία οπή στο κέντρο και άλλες 24 περιφερειακές που αντιστοιχούσαν στα 24 γράμματα του αλφαβήτου. Ένα κορδόνι περνούσε διαδοχικά από τις οπές

που αντιστοιχούσαν στα γράμματα του κρυπτογραφημένου μηνύματος. Εάν ένα γράμμα επαναλαμβανόταν, το κορδόνι περνούσε δύο φορές από την ίδια οπή. Η ανάγνωση του μηνύματος γινόταν με το "ξετύλιγμα" του κορδονιού από το τέλος προς την αρχή. Αυτό το σύστημα κρυπτογράφησης ήταν ευέλικτο, καθώς τα αρχικά γράμματα για τη σειριακή ανάγνωση θα μπορούσαν να αλλάξουν μετά από μυστική προσυνεννόηση μεταξύ των επικοινωνούντων. Επομένως, επέτρεπε μια στοιχειώδη, αλλά αποτελεσματική, μορφή ασφαλούς επικοινωνίας (Bauer 2021).

Οι Ρωμαίοι, και ειδικότερα ο Ιούλιος Καίσαρας, αποτελούν μια από τις πρώιμες φιγούρες στην ιστορία της κρυπτογραφίας. Ο Καίσαρας χρησιμοποίησε μια πολύ απλή μορφή κρυπτογράφησης που σήμερα είναι γνωστή ως «Κρυπτοσύστημα του Καίσαρα». Συγκεκριμένα, αυτή η μέθοδος περιλάμβανε τη μετατόπιση κάθε γράμματος του αρχικού κειμένου κατά έναν συγκεκριμένο αριθμό θέσεων μέσα στο αλφάβητο. Η μέθοδος του Καίσαρα αποτελεί ένα από τα πιο πρώιμα γνωστά κρυπτογραφικά συστήματα και αναδεικνύει την αναγκαιότητα της ασφάλειας στην επικοινωνία, ιδίως σε πλαίσια στρατιωτικής ή πολιτικής σημασίας. Παρά την απλότητά της, η μέθοδος αυτή υπηρέτησε ως βάση για την ανάπτυξη πιο σύνθετων κρυπτογραφικών τεχνικών και προσέφερε μια πρώτη γεύση των δυνητικών εφαρμογών της κρυπτογραφίας. Συγκεκριμένα, η ανταλλαγή μηνυμάτων με αυξημένη εμπιστοσύνη και η προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση είναι κρίσιμης σημασίας. Η απλή τεχνική του Καίσαρα έδειξε ότι ακόμη και οι πιο βασικοί κρυπτογραφικοί μηχανισμοί μπορούν να προσφέρουν ένα επίπεδο ασφάλειας, ενώ ταυτόχρονα προώθησε την εξερεύνηση και την κατανόηση πιο περίπλοκων και ασφαλών μεθόδων. Αυτό το πρώιμο παράδειγμα έχει λειτουργήσει ως καταλύτης για την περαιτέρω έρευνα και ανάπτυξη στον τομέα της κρυπτογραφίας, τονίζοντας τη σημασία της διαρκούς προσαρμογής και εξέλιξης στον κόσμο της ασφάλειας των πληροφοριών (Bauer 2021).

Κατά τη μεσαιωνική εποχή, η κρυπτογραφία εξελίχθηκε περαιτέρω, με την ανάπτυξη πιο πολύπλοκων κωδικών και κρυπτογραφημάτων. Η κρυπτογραφία στην Ευρώπη ξεκίνησε κατά την μεσαιωνική εποχή, όταν αναπτύχθηκε από τα Παπικά Κράτη και τις ιταλικές πόλεις-κράτη. Το πρώτο ευρωπαϊκό εγχειρίδιο για την κρυπτογραφία (περίπου το 1379) ήταν μια συλλογή κωδικών από τον Gabriele de Lavinde της Πάρμας, ο οποίος υπηρετούσε τον Πάπα Κλήμη Z'. Αυτό το εγχειρίδιο, που βρίσκεται τώρα στα αρχεία του Βατικανού, περιέχει ένα σύνολο κλειδιών για 24 αλληλογράφους και περιλαμβάνει σύμβολα για γράμματα, κενά, και αρκετούς κωδικούς δύο μερών[3] (two-part codes) ισοδύναμους με λέξεις και ονόματα (Bauer 2021).

Η κρυπτογραφία συνέχισε να εξελίσσεται κατά την νεότερη εποχή, με την εφεύρεση πιο πολύπλοκων μηχανικών και ηλεκτρομηχανικών μηχανών, όπως η μηχανή Enigma (**Εικόνα 2.1**), που παρείχε πιο εξελιγμένα και αποτελεσματικά μέσα κρυπτογράφησης. Η μηχανή Enigma ήταν μια ηλεκτρομηχανική συσκευή που χρησιμοποιούσε ένα σύστημα περιστρεφόμενων δίσκων για να αλλάζει τις ηλεκτρικές συνδέσεις μεταξύ των πλήκτρων και των λαμπτήρων. Η μηχανή αυτή χρησιμοποιήθηκε εκτενώς από τη Ναζιστική Γερμανία κατά τον Β' Παγκόσμιο Πόλεμο, σε όλες τις μονάδες του γερμανικού στρατού. Ο κώδικας της μηχανής Enigma έγινε γνωστός από τους Πολωνούς στις αρχές της δεκαετίας του 1930 και από τους Βρετανούς κατά τη διάρκεια του πολέμου. Οι Βρετανοί δημιούργησαν μια ηλεκτρονική συσκευή, γνωστή ως Bombe, για να βοηθήσουν στην

[3] Οι κωδικοί δύο μερών αφορούν κωδικούς όπου το ένα μέρος χρησιμοποιείται για τη μετατροπή του κανονικού κειμένου σε κρυπτογραφημένο μήνυμα, ενώ το δεύτερο μέρος για το αντίστροφο.

αποκρυπτογράφηση των μηνυμάτων της Enigma. Η αποκρυπτογράφηση της Enigma παρείχε στους Συμμάχους πολύτιμες πληροφορίες για τις γερμανικές κινήσεις και σχέδια (Bauer 2021).

Εικόνα 3.1: *Η μηχανή Enigma*

Μένοντας στην εποχή του Δεύτερου Παγκόσμιου Πολέμου, συναντάμε επίσης τον «Κώδικα Navajo», μια μέθοδο κρυπτογράφησης που χρησιμοποιήθηκε από τις Ηνωμένες Πολιτείες κατά τη διάρκεια του πολέμου, προκειμένου να διαβιβάζονται στρατιωτικές εντολές με ασφάλεια. Η γλώσσα των Navajo, ενός αυτοχθόνος λαού των ΗΠΑ, χρησιμοποιήθηκε ως βάση για την κρυπτογράφηση επειδή ήταν πολύπλοκη και δύσκολο να κατανοηθεί από τις δυνάμεις του Άξονα. Αυτό ήταν ιδιαίτερα σημαντικό στον πολεμικό θέατρο επιχειρήσεων του Ειρηνικού Ωκεανού, όπου οι Ηνωμένες Πολιτείες ήταν ενεργά αντιμέτωπες με την Ιαπωνική Αυτοκρατορία. Οι «Navajo Code Talkers» όπως ήταν γνωστοί, ήταν Navajo που είχαν εκπαιδευτεί για να χρησιμοποιούν αυτήν τη γλώσσα αποκλειστικά για στρατιωτική επικοινωνία. Ο κώδικας Navajo απεδείχθη αποτελεσματικός και άφησε πίσω του μια επιτυχημένη ιστορία χρήσης. Ενώ άλλοι κώδικες και μέθοδοι κρυπτογράφησης είχαν σπάσει, ο κώδικας Navajo παρέμεινε απρόσβλητος καθ' όλη τη διάρκεια του πολέμου, συμβάλλοντας έτσι στην τελική νίκη των Συμμάχων επί του Άξονα. Η χρήση αυτής της μεθόδου κρυπτογράφησης αποδείχθηκε τόσο αποτελεσματική που οι Navajo Code Talkers, τιμήθηκαν με διάφορες βραβεύσεις και αναγνωρίσεις (Bauer 2021).

3.3 Σύγχρονη κρυπτογραφία

Η σύγχρονη κρυπτογραφία είναι ένας επιστημονικός τομέας που συνδυάζει τα μαθηματικά, την επιστήμη των υπολογιστών και την ασφάλεια των πληροφοριών. Διαδραματίζει ζωτικό ρόλο στην προστασία της ασφάλειας των πληροφοριών στην ψηφιακή εποχή, επιτρέποντας την ασφαλή μετάδοση, αποθήκευση και επεξεργασία των δεδομένων σε ένα περιβάλλον που είναι συχνά εχθρικό και αβέβαιο. Ο κύριος στόχος της είναι να παρέχει υπηρεσίες ασφάλειας, όπως η εμπιστευτικότητα, η ακεραιότητα, η ταυτοποίηση και η μη αμφισβήτηση των δεδομένων, προστατεύοντας τις πληροφορίες από την παραβίαση, την παραποίηση ή την κακόβουλη χρήση (Katz and Lindell 2007).

Η σύγχρονη κρυπτογραφία βασίζεται σε μαθηματικές θεωρίες, όπως η θεωρία αριθμών, η θεωρία πολυπλοκότητας και η θεωρία πιθανοτήτων. Αυτές οι θεωρίες παρέχουν τα εργαλεία που είναι απαραίτητα για τον σχεδιασμό και την ανάλυση ασφαλών κρυπτογραφικών αλγορίθμων (Katz and Lindell 2007).

Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν μαθηματικούς αλγόριθμους για να κωδικοποιήσουν τις πληροφορίες μέσω ενός μυστικού κλειδιού και στη συνέχεια να τις μεταδώσουν σε έναν ή περισσότερους παραλήπτες. Κατά τη λήψη του, το μήνυμα αποκωδικοποιείται με βάση το κλειδί που χρησιμοποιήθηκε για την κωδικοποίησή του. Η δυσκολία υπολογισμού των αλγορίθμων, η μη γνώση του μυστικού κλειδιού, καθώς και άλλοι παράγοντες, καθιστούν δυσχερή την απόκτηση των αρχικών

πληροφοριών, ακόμα και αν κάποιος γνωρίζει τον αλγόριθμο που χρησιμοποιήθηκε για την κωδικοποίηση. Μερικά από τα κύρια είδη των σύγχρονων κρυπτογραφικών αλγορίθμων είναι οι συμμετρικοί, οι ασύμμετροι και οι κρυπτογραφικές συναρτήσεις κατακερματισμού. Τα κρυπτοσυστήματα και οι συναρτήσεις κατακερματισμού είναι βασικά στοιχεία της κρυπτογραφίας που επιτρέπουν την ασφαλή μετάδοση, αποθήκευση και επεξεργασία δεδομένων. Κάθε τύπος κρυπτοσυστήματος και η τεχνολογία του κατακερματισμού έχουν διαφορετικές ιδιότητες, πλεονεκτήματα και περιορισμούς. Πιο συγκεκριμένα, σύμφωνα με την εργασία (Katz and Lindell 2007) έχουμε ότι:

- **Συμμετρικά Κρυπτοσυστήματα** (*μτφρ. symmetric cryptosystems*): Στα συμμετρικά κρυπτοσυστήματα, χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση του μηνύματος. Αυτό σημαίνει ότι τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να έχουν πρόσβαση στο ίδιο κλειδί και να το διατηρούν μυστικό. Οι συμμετρικές μέθοδοι είναι γενικά πιο γρήγορες σε σύγκριση με εκείνες των ασύμμετρων κρυπτοσυστημάτων και προσφέρουν μεγαλύτερη ευκολία στην εφαρμογή και τη διαχείριση. Επίσης, χρησιμοποιούν λιγότερους υπολογιστικούς πόρους, καθιστάμενες έτσι κατάλληλες για συσκευές με περιορισμένες δυνατότητες. Ωστόσο, η ανάγκη για ένα κοινό κλειδί που πρέπει να διατηρηθεί μυστικό αποτελεί περιορισμό, καθότι η ασφαλής διανομή του κλειδιού σε όλα τα ενδιαφερόμενα μέρη μπορεί είναι δυσχερής έως προβληματική. Κατά συνέπεια, αυτές οι μέθοδοι ενδέχεται να είναι πιο ευάλωτες σε επιθέσεις εάν το κλειδί παραβιαστεί. Επίσης, δεν έχουν τη δυνατότητα να εξασφαλίσουν πλήρως αυθεντικοποίηση και καταλογισμό, διότι το κλειδί είναι γνωστό σε πάνω από ένα μέρη.

- **Ασύμμετρα Κρυπτοσυστήματα** (*μτφρ. asymmetric cryptosystems*): Τα ασύμμετρα κρυπτοσυστήματα προσφέρουν υψηλό επίπεδο ασφάλειας μέσω της χρήσης δύο διαφορετικών κλειδιών: ενός δημόσιου και ενός ιδιωτικού. Το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση, ενώ το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση. Ένα σημαντικό πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι το δημόσιο κλειδί είναι ασφαλές για κοινοποίηση και μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση μηνυμάτων που μόνο το αντίστοιχο ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει. Δηλαδή, το δημόσιο κλειδί μπορεί να κοινοποιηθεί ανοιχτά, και ως εκ τούτου, δεν απαιτείται κάποια εξειδικευμένη «ασφαλής» διαδικασία για να το φτάσει στον παραλήπτη. Παρόλα αυτά, οι ασύμμετρες μέθοδοι είναι συγκριτικά πιο αργές σε σχέση με τις συμμετρικές ενώ απαιτούν περισσότερους υπολογιστικούς πόρους, κάτι το οποίο μπορεί να αποτελεί ζήτημα για συσκευές με περιορισμένες δυνατότητες.

- **Συναρτήσεις Κατακερματισμού** (*μτφρ. hash functions*): Οι συναρτήσεις κατακερματισμού είναι μέθοδοι που παίρνουν είσοδό τους μια πληροφορία και επιστρέφουν μια σταθερού μήκους συμβολοσειρά, που φαίνεται τυχαία. Η έξοδος αυτή, που ονομάζεται "**hash**", πρέπει να είναι πάντα ίδια για την ίδια είσοδο και διαφορετική (στο μέτρο του δυνατού) για διαφορετικές εισόδους. Υπάρχει πάντα η θεωρητική πιθανότητα δύο διαφορετικών εισόδων να δημιουργούν το ίδιο hash, αν και οι καλά σχεδιασμένες συναρτήσεις κατακερματισμού καθιστούν αυτό εξαιρετικά απίθανο. Σε κάθε περίπτωση, η ανάκτηση των αρχικών δεδομένων από το hash δεν είναι εφικτή. Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται σε ποικίλες εφαρμογές, όπως η επαλήθευση δεδομένων, τα ψηφιακά πιστοποιητικά και οι αλγόριθμοι διαδικτυακής ασφάλειας. Γενικά είναι γρήγορες στον

υπολογισμό του hash και παρέχουν έναν γρήγορο τρόπο για την επαλήθευση της ακεραιότητας των δεδομένων.

Η σύγχρονη κρυπτογραφία χρησιμοποιεί διάφορες τεχνικές για να διασφαλίσει την αξιοπιστία των επικοινωνιών. Ειδικότερα όπως αναφέρει η εργασία (Katz and Lindell 2007) παρέχονται οι ακόλουθες μέθοδοι και τεχνικές:

- **Ψηφιακές Υπογραφές** (*μτφρ. digital signatures*): Οι ψηφιακές υπογραφές είναι μία τεχνολογία που επιτρέπει την επαλήθευση της προέλευσης και της ακεραιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Ένα μηχανισμός ψηφιακής υπογραφής χρησιμοποιεί ένα ζευγάρι κλειδιών: ένα ιδιωτικό και ένα δημόσιο. Ο κάτοχος του ιδιωτικού κλειδιού χρησιμοποιεί αυτό για να δημιουργήσει μια υπογραφή, ενώ οποιοσδήποτε με το δημόσιο κλειδί μπορεί να επαληθεύσει την υπογραφή.

- **Μέθοδοι Δέσμευσης** (*μτφρ. commitment schemes*): Αυτές οι μέθοδοι επιτρέπουν σε ένα εμπλεκόμενο μέρος να δεσμευτεί σε μία συγκεκριμένη τιμή (γενικά, ένα μήνυμα ή τιμή δεδομένων) με τέτοιο τρόπο ώστε αργότερα να μην μπορεί να αλλάξει την τιμή, αλλά χωρίς να την αποκαλύπτει αμέσως.

- **Ψηφιακά Συμβόλαια** (*μτφρ. digital contracts*): Τα ψηφιακά συμβόλαια είναι ηλεκτρονικές συμφωνίες που χρησιμοποιούν κρυπτογραφικές τεχνικές για να εξασφαλίσουν την αυθεντικότητα, την ακεραιότητα, και συχνά την εφαρμογή των συμφωνηθέντων όρων.

- **Πρωτόκολλα Εξουσιοδότησης** (*μτφρ. authorization protocols*): Αυτά είναι μέθοδοι και πρωτόκολλα που χρησιμοποιούνται για τον προσδιορισμό των δικαιωμάτων πρόσβασης ή των ενεργειών που μπορεί να εκτελέσει ένας χρήστης ή ένα σύστημα σε ένα ψηφιακό περιβάλλον.

- **Αποδεικτικά Μηδενικής Γνώσης** (*μτφρ. zero-knowledge proofs*): Τα αποδεικτικά μηδενικής γνώσης είναι μια τεχνική που επιτρέπει σε έναν χρήστη να αποδείξει σε έναν άλλο ότι γνωρίζει μια συγκεκριμένη πληροφορία, όπως έναν κωδικό πρόσβασης, χωρίς ποτέ να αποκαλύψει την πληροφορία αυτή.

Όλες αυτές οι τεχνικές και τα πρωτόκολλα ενσωματώνονται στη σύγχρονη κρυπτογραφία για την εξασφάλιση της ασφάλειας, της αξιοπιστίας και της ιδιωτικότητας σε ψηφιακές επικοινωνίες και συναλλαγές. Επίσης, χρησιμοποιεί μαθηματικές δομές, όπως (Katz and Lindell 2007):

- **Ομάδες** (*μτφρ. groups*): Στη μαθηματική θεωρία των ομάδων, ως ομάδα ορίζεται ένα ζεύγος (S, op) όπου S είναι ένα σύνολο στοιχείων και op ένας τελεστής για το οποίο ζεύγος ισχύουν τα ακόλουθα: (i) το S είναι κλειστό ως προς τον τελεστή op, (ii) ο τελεστής είναι προσεταιριστικός, (iii) υπάρχει ουδέτερο στοιχείο ως προς τον τελεστή op και (iv) για κάθε στοιχείο του S υπάρχει ο αντίστροφός του ως προς τον τελεστή op, ο οποίος ανήκει στο S. Οι ομάδες παίζουν σημαντικό ρόλο σε κρυπτοσυστήματα όπως το RSA και σε τεχνικές όπως το Diffie-Hellman key exchange.

- **Δακτύλιοι** (*μτφρ. rings*): Ένας δακτύλιος είναι μια αλγεβρική δομή που επεκτείνει την έννοια της ομάδας, προσθέτοντας μια δεύτερη πράξη που συνήθως ερμηνεύεται ως

πολλαπλασιασμός. Οι δακτύλιοι βρίσκουν εφαρμογές σε κρυπτογραφικά πρωτόκολλα και αλγορίθμους.

- **Πεδία** (*μτφρ. fields*): Ένα πεδίο είναι μια αλγεβρική δομή που περιλαμβάνει δύο πράξεις (συνήθως πρόσθεση και πολλαπλασιασμός) και επεκτείνει τη θεωρία των δακτυλίων. Πεδία χρησιμοποιούνται ευρέως σε κρυπτογραφικές μεθόδους, όπως τα κρυπτοσυστήματα βασισμένα σε ελλειπτικές καμπύλες.

- **Ελλειπτικές Καμπύλες** (*μτφρ. elliptic curves*): Οι ελλειπτικές καμπύλες είναι τύποι καμπυλών που παίζουν σημαντικό ρόλο στην ελλειπτική κρυπτογραφία, μια προχωρημένη μορφή ασύμμετρης κρυπτογραφίας. Η κρυπτογραφία βασισμένη σε ελλειπτικές καμπύλες θεωρείται ιδιαίτερα ασφαλής συγκριτικά με άλλες τεχνικές, χρησιμοποιώντας μικρότερα κλειδιά για παρόμοια επίπεδα ασφάλειας.

Αδιαμφισβήτητα, η σύγχρονη κρυπτογραφία αποτελεί έναν πολυδιάστατο και δυναμικό τομέα που ενσωματώνει πολύπλοκες μαθηματικές θεωρίες και τεχνικές για τη διασφάλιση των απανταχού ψηφιακών αλληλεπιδράσεων. Από τα απλά συμμετρικά κρυπτοσυστήματα έως τα πιο προχωρημένα πρωτόκολλα βασισμένα σε ελλειπτικές καμπύλες, η κρυπτογραφία εξελίσσεται συνεχώς για να ανταποκριθεί στις αυξανόμενες απαιτήσεις για ασφάλεια και προστασία της ιδιωτικότητας. Εν τέλει, τόσο η κατανόηση όσο και η πρακτική εφαρμογή της κρυπτογραφίας είναι εξίσου ουσιαστικές για τη διατήρηση της αξιοπιστίας και της ακεραιότητας του ψηφιακού κόσμου στον οποίο δραστηριοποιείται ο σύγχρονος άνθρωπος (Katz and Lindell 2007).

3.4 Κύριοι αλγόριθμοι κρυπτογράφησης

Η επιλογή του κατάλληλου αλγορίθμου κρυπτογράφησης είναι ζωτικής σημασίας για την εγγύηση της ασφάλειας και της εμπιστοσύνης στο πεδίο των ψηφιακών επικοινωνιών και των τεχνολογιών. Από τις πρώτες μορφές συμμετρικής κρυπτογράφησης μέχρι τις πιο σύνθετες μεθόδους ασύμμετρης κρυπτογράφησης και την κρυπτογραφία βασισμένη σε ελλειπτικές καμπύλες, οι αλγόριθμοι κρυπτογράφησης έχουν παρουσιάσει σημαντική εξέλιξη. Στην παρούσα ενότητα, παρουσιάζονται οι πιο βασικοί και διαδεδομένοι κρυπτογραφικοί αλγόριθμοι, επισημαίνοντας τα κύρια χαρακτηριστικά τους γνωρίσματα, τις δυνητικές εφαρμογές τους και τη σημασία του καθενός στο σύγχρονο κρυπτογραφικό τοπίο.

3.4.1 AES (Advanced Encryption Standard)

Ο Advanced Encryption Standard (AES) αποτελεί έναν συμμετρικό αλγόριθμο κρυπτογράφησης, που είναι ευρέως αποδεκτός στην παγκόσμια κοινότητα της κρυπτογραφίας και της ασφάλειας πληροφοριών. Διακρίνεται για την ικανότητά του να υποστηρίζει διάφορα μεγέθη κλειδιού - 128, 192, ή 256 bits - προσφέροντας ευελιξία και κλιμάκωση σε διάφορες εφαρμογές. Λόγω της υψηλής του απόδοσης και της ανθεκτικότητάς του σε είδη επιθέσεων όπως η παρεμβολή, ο αλγόριθμος AES χρησιμοποιείται ευρέως σε πολυάριθμες τεχνολογικές λύσεις (Heron 2009).

Είναι ο αλγόριθμος που συνηθέστατα επιλέγεται για την εφαρμογή ασφαλείας σε διαδικτυακές υπηρεσίες μέσω πρωτοκόλλων όπως το SSL/TLS, την ασφάλεια σε εταιρικά δίκτυα μέσω VPNs, και την προστασία των βάσεων δεδομένων. Στον χώρο των ηλεκτρονικών συναλλαγών και των κρυπτονομισμάτων, ο AES συνεχίζει να αποτελεί τον βασικό πυλώνα για την διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων. Είναι εγκεκριμένος από αξιόπιστους διεθνείς οργανισμούς, όπως το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) των ΗΠΑ, και

συχνά λειτουργεί ως αναφορά για την αξιολόγηση και την ανάπτυξη άλλων κρυπτογραφικών αλγορίθμων (Heron 2009).

Στην ουσία, ο Advanced Encryption Standard εξακολουθεί να παραμένει μία από τις πιο αξιόπιστες, ευρέως διαδεδομένες και καταξιωμένες λύσεις για την προστασία της ψηφιακής πληροφορίας στο σύγχρονο τεχνολογικό τοπίο. Η σημασία του υπερβαίνει τον τεχνικό χαρακτήρα, αφού ενισχύει την ηλεκτρονική εμπιστοσύνη και διευκολύνει την ασφαλή διακίνηση πληροφοριών σε παγκόσμιο επίπεδο (Heron 2009).

3.4.2 DES (Data Encryption Standard) και 3DES (Triple DES)

Ο Data Encryption Standard (DES) είναι ένας από τους παλαιότερους συμμετρικούς αλγορίθμους κρυπτογράφησης και ήταν για πολλά χρόνια το πρότυπο για την ασφάλεια δεδομένων σε πολλές εφαρμογές, από τις τραπεζικές συναλλαγές μέχρι τις κυβερνητικές επικοινωνίες. Με τη χρήση ενός μεγέθους κλειδιού 56 bits, ο DES ήταν κάποτε θεωρητικά ασφαλής, αλλά στη σημερινή εποχή έχει κριθεί ως ευάλωτος σε επιθέσεις λόγω των περιορισμένων μεγεθών κλειδιών και της αυξημένης υπολογιστικής ισχύος (Nicolaou 2017).

Για να αντιμετωπισθούν αυτές οι αδυναμίες, αναπτύχθηκε ο 3DES (Triple DES), ο οποίος εφαρμόζει τον αλγόριθμο DES τρεις φορές με διαφορετικά κλειδιά, αυξάνοντας έτσι το επίπεδο ασφάλειας. Παρά την αυξημένη ασφάλεια σε σύγκριση με τον απλό DES, ο 3DES υπολείπεται σε ταχύτητα και απόδοση σε σχέση με πιο σύγχρονους αλγορίθμους όπως το AES (Nicolaou 2017)

Ο DES και ο 3DES έχουν βρει εφαρμογές σε ποικίλες διαδικασίες, όπως η ασφάλεια σε ATM και άλλες τραπεζικές εφαρμογές, αλλά οι αδυναμίες τους και η εμφάνιση πιο ασφαλών αλγορίθμων, όπως το AES, έχουν περιορίσει τη σημερινή τους χρησιμότητα. Εντούτοις, η κατανόηση της λειτουργίας τους και των περιορισμών τους παραμένει σημαντική, καθώς επιτρέπει την καλύτερη αξιολόγηση των τρεχουσών και μελλοντικών τεχνολογιών ασφάλειας. Η χρήση τους σε παλαιότερες υποδομές και συστήματα επιβεβαιώνει τη σημασία της διαχείρισης και της ενημέρωσης των κρυπτογραφικών συστημάτων στην εποχή της ψηφιακής μετάβασης (Nicolaou 2017).

3.4.3 RSA (Rivest - Shamir - Adleman)

Ο αλγόριθμος RSA (Rivest-Shamir-Adleman) είναι ένας από τους πλέον διαδεδομένους και ευρέως αποδεκτούς αλγορίθμους ασύμμετρης κρυπτογραφίας. Εισήχθη το 1978 και αποτέλεσε έναν από τους πρώτους πρακτικά χρησιμοποιήσιμους αλγορίθμους για την ασφαλή διακίνηση δεδομένων και την ψηφιακή υπογραφή. Βασίζεται στην αριθμητική των πεδίων και εκμεταλλεύεται την δυσκολία του προβλήματος της παραγοντοποίησης ενός μεγάλου σύνθετου αριθμού (Muhammad, Chiroma και Mahmud 2014).

Ο RSA χρησιμοποιείται σε μια πληθώρα εφαρμογών, συμπεριλαμβανομένων των πρωτοκόλλων ασφαλούς περιήγησης στο Διαδίκτυο (π.χ., SSL/TLS), ψηφιακών υπογραφών, κρυπτονομισμάτων και πολλών άλλων. Ένα από τα κύρια χαρακτηριστικά του είναι η ικανότητα να προσφέρει και κρυπτογράφηση και ψηφιακή υπογραφή με την ίδια κρυπτογραφική σουίτα. Εντούτοις, ο RSA είναι συχνά πιο αργός σε σύγκριση με συμμετρικούς αλγορίθμους όπως το AES, ιδιαίτερα για μεγάλα μεγέθη κλειδιών, τα οποία είναι απαραίτητα για υψηλό επίπεδο ασφάλειας (Muhammad, Chiroma και Mahmud 2014).

Η σημασία του RSA είναι αδιαμφισβήτητη, καθώς προσφέρει έναν από τους πιο γενικά χρησιμοποιούμενους και αξιόπιστους μηχανισμούς για την ασφάλεια της ψηφιακής επικοινωνίας.

Ωστόσο, όπως και σε κάθε τεχνολογία, η συνεχής ανάπτυξη και τελειοποίηση των κρυπτογραφικών μεθόδων καθιστούν απαραίτητη την προσαρμογή και την ενημέρωση των προτύπων ασφάλειας, ειδικά στο πλαίσιο των κβαντικών υπολογιστών που θεωρητικά θα μπορούσαν να απειλήσουν την ασφάλεια αλγορίθμων όπως ο RSA (Muhammad, Chiroma και Mahmud 2014).

3.4.4 Diffie-Hellman

Ο αλγόριθμος Diffie-Hellman αποτελεί ένα από τα πιο πρωτοποριακά κρυπτογραφικά πρωτόκολλα και είναι πρωτίστως γνωστός για την υλοποίηση της ασύμμετρης κρυπτογραφίας μέσω της ασφαλούς ανταλλαγής κλειδιών. Εισήχθη το 1976 από τους Whitfield Diffie και Martin Hellman και ανοίγει τον δρόμο για την ασφαλή επικοινωνία μεταξύ δύο μερών που δεν έχουν προηγουμένως διαμοιραστεί κρυπτογραφικό υλικό (Joux και Nguyen 2003).

Μέσω του αλγορίθμου Diffie-Hellman, τα εμπλεκόμενα μέρη μπορούν να δημιουργήσουν ένα κοινό μυστικό κλειδί, το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Η διαδικασία είναι σχεδιασμένη έτσι ώστε, ακόμη και αν ένας τρίτος παρακολουθεί την επικοινωνία, να μην είναι εφικτό να υπολογίσει το κοινό κλειδί, λόγω της δυσκολίας του να επιλυθεί ο αντίστροφος υπολογισμός (Joux και Nguyen 2003).

Ο αλγόριθμος Diffie-Hellman έχει εφαρμογές σε πολλούς τομείς της ασφάλειας των πληροφοριών, από τα VPNs και τα ασφαλή πρωτόκολλα επικοινωνίας, μέχρι την ασφάλεια σε ιστοσελίδες και συστήματα ηλεκτρονικού εμπορίου. Παρόλο που έχουν εντοπιστεί περιπτώσεις όπου ο αλγόριθμος είναι ευάλωτος σε συγκεκριμένους τύπους επιθέσεων, όπως τις επιθέσεις "man-in-the-middle", η σημασία του παραμένει αναμφίλεκτη ως βάση για την ανάπτυξη πιο πολύπλοκων και ασφαλέστερων κρυπτογραφικών συστημάτων. Η κατανόηση της λειτουργίας και των περιορισμών του Diffie-Hellman είναι κομβικής σημασίας για την περαιτέρω εξέλιξη των τεχνολογιών ασφάλειας των πληροφοριών (Joux και Nguyen 2003).

3.4.5 ECC (Elliptic Curve Cryptography)

Η κρυπτογραφία με ελλειπτικές καμπύλες (Elliptic Curve Cryptography - ECC) αποτελεί μία σύγχρονη προσέγγιση στην κρυπτογραφία, η οποία βασίζεται στην αριθμητική επί ελλειπτικών καμπυλών πάνω σε πεδία. Ένα από τα κύρια πλεονεκτήματα της ECC είναι η ικανότητά της να παρέχει το ίδιο επίπεδο ασφάλειας με άλλους κρυπτογραφικούς αλγορίθμους, όπως το RSA, χρησιμοποιώντας όμως πολύ μικρότερα κλειδιά. Αυτό την καθιστά ιδανική για εφαρμογές όπου οι πόροι είναι περιορισμένοι, όπως συσκευές IoT, κινητά τηλέφωνα και ενσωματωμένα συστήματα (Kapoor, Abraham και Singh 2008).

Η ECC βρίσκει εφαρμογές σε μια πληθώρα τεχνολογικών τομέων. Ειδικότερα, στην ασφάλεια δικτυακών πρωτοκόλλων όπως το SSL/TLS για ασφαλείς συνδέσεις διαδικτύου, στην ηλεκτρονική υπογραφή δεδομένων, σε συστήματα εξουσιοδότησης και πιστοποίησης, αλλά και σε κρυπτονομίσματα όπως το Bitcoin. Επιπλέον, λόγω της αποδοτικότητας της ECC σε περιορισμένους πόρους, χρησιμοποιείται ευρέως σε εφαρμογές Internet of Things (IoT), όπου οι υπολογιστικοί πόροι αλλά και η ενέργεια είναι περιορισμένοι (Kapoor, Abraham και Singh 2008).

Η κατανόηση και η εφαρμογή της ECC απαιτούν εξειδικευμένες γνώσεις στην αριθμητική και τη μαθηματική λογική, καθώς και την κατανόηση των πρωτοκόλλων και των μαθηματικών αξιώσεων που διέπουν τις ελλειπτικές καμπύλες. Παρά την πολυπλοκότητά της, η ECC αποτελεί ένα από τα

πιο δυναμικά εργαλεία της κρυπτογραφίας για τη διασφάλιση των ψηφιακών μας δεδομένων στον σύγχρονο κυβερνοχώρο (Kapoor, Abraham και Singh 2008).

3.4.6 DSA (Digital Signature Algorithm)

Ο Digital Signature Algorithm (DSA) είναι ένας κρυπτογραφικός αλγόριθμος που χρησιμοποιείται κυρίως για τη δημιουργία ψηφιακών υπογραφών. Εισήχθη από το ινστιτούτο NIST (National Institute of Standards and Technology) των ΗΠΑ και βασίζεται σε μαθηματικές θεωρίες όπως το πρόβλημα του διακριτού λογαρίθμου, αλλά και σχετιζόμενες τεχνικές. Η χρήση του DSA περιλαμβάνει τη δημιουργία ενός κλειδιού ζεύγους, ενός ιδιωτικού και ενός δημόσιου, και τη διαδικασία της υπογραφής και της επαλήθευσης (NIST 1992).

Η εφαρμογή του DSA είναι ευρεία και εκτείνεται από την ασφάλεια των ηλεκτρονικών μηνυμάτων και των εγγράφων, μέχρι την εξασφάλιση των δικτυακών συνδέσεων. Παρά το γεγονός ότι πρόκειται για έναν αποδεδειγμένα ασφαλή αλγόριθμο, η εμφάνιση νέων και πιο αποδοτικών αλγορίθμων για ψηφιακές υπογραφές, όπως το ECDSA (Elliptic Curve Digital Signature Algorithm), έχει οδηγήσει σε μια προοδευτική μείωση της χρήσης του DSA.

Συνοψίζοντας, ο DSA παραμένει ένας σημαντικός αλγόριθμος για την κρυπτογραφική προστασία μέσω ψηφιακών υπογραφών, αλλά η εξέλιξη των κρυπτογραφικών τεχνολογιών και η ανάγκη για υψηλότερα επίπεδα ασφάλειας και αποδοτικότητας έχουν οδηγήσει στην ανάπτυξη και υιοθέτηση νεότερων αλγορίθμων. Η κατανόηση της λειτουργίας και των χαρακτηριστικών του DSA είναι σημαντική για την αξιολόγηση της συνολικής ασφάλειας ενός κρυπτογραφικού συστήματος (NIST 1992).

3.4.7 Blowfish και Twofish

Ο Blowfish είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης που αναπτύχθηκε από τον Bruce Schneier το 1993. Διαθέτει μικρό μέγεθος κώδικα, είναι πολύ γρήγορος και εφαρμόζεται συχνά σε εφαρμογές και πρωτόκολλα όπου η ταχύτητα και η απλότητα είναι αυξημένης σημασίας. Παρόλο που ο αλγόριθμος είναι ισχυρός, η χρήση μικρών μεγεθών κλειδιών καθιστά το Blowfish λιγότερο ασφαλής από πιο σύγχρονους αλγορίθμους, όπως ο AES (Bhanot και Hans 2015).

Ο Twofish είναι ο διάδοχος του Blowfish και αναπτύχθηκε επίσης από τον Bruce Schneier το 1998. Προσφέρει βελτιωμένη ασφάλεια και ευελιξία, καθώς υποστηρίζει μεγέθη κλειδιών έως 256 bits. Ο Twofish είναι σχεδιασμένος για να προσφέρει υψηλό επίπεδο ασφάλειας, διατηρώντας την ταχύτητα και την αποδοτικότητα του προκατόχου του (Bhanot και Hans 2015).

Και οι δύο αλγόριθμοι έχουν εφαρμογές σε διάφορους τομείς, όπως τα VPN, οι συνδέσεις μέσω SSH, τα εμπορικά λογισμικά ασφαλείας, και άλλες εφαρμογές όπου η κρυπτογράφηση δεδομένων είναι απαραίτητη. Παρά το γεγονός ότι οι νεότεροι αλγόριθμοι όπως ο AES έχουν πάρει τη θέση τους σε πολλές περιπτώσεις, η κατανόηση των Blowfish και Twofish είναι σημαντική για την ιστορική και τεχνική εξέλιξη της κρυπτογραφίας. Αυτοί οι αλγόριθμοι αποτελούν μέρος της ευρύτερης εικόνας της εξέλιξης της κρυπτογραφικής τεχνολογίας και εξακολουθούν να είναι σημαντικοί για την κατανόηση των τρεχουσών αλλά και των μελλοντικών τάσεων στον τομέα της ασφάλειας των πληροφοριών (Bhanot και Hans 2015).

3.4.8 ElGamal

Ο αλγόριθμος ElGamal είναι ένα ασύμμετρο κρυπτογραφικό σύστημα που δημιουργήθηκε από τον Taher ElGamal το 1985. Βασίζεται σε μαθηματικές ιδέες από τη θεωρία των ομάδων και είναι

γνωστός για το ικανοποιητικό επίπεδο ασφάλειας που προσφέρει, ωστόσο είναι σχετικά πιο αργός σε σύγκριση με άλλους αλγορίθμους όπως ο RSA ή ο AES (Meier 2005).

Ο ElGamal χρησιμοποιείται συχνά για την ασφάλεια της ηλεκτρονικής αλληλογραφίας, των ψηφιακών υπογραφών και άλλων εφαρμογών που απαιτούν ανώνυμη επικοινωνία ή ελεγχόμενη αποκάλυψη πληροφοριών. Ένα από τα κύρια πλεονεκτήματα του ElGamal είναι η δυνατότητα προσφοράς «forward secrecy», δηλαδή τη δυνατότητα για ασφαλείς επικοινωνίες ακόμα και αν κάποιος καταφέρει να αποκτήσει πρόσβαση σε μυστικά μακράς διάρκειας που ενέχονται στην επικοινωνία. Αυτό, τον καθιστά εξαιρετικά ανθεκτικό σε πολλούς τύπους επιθέσεων (Meier 2005).

Η κατανόηση του ElGamal και των μαθηματικών αρχών πάνω στις οποίες βασίζεται είναι σημαντική για την κατανόηση της σύγχρονης κρυπτογραφίας, ειδικά σε περιβάλλοντα όπου η εμπιστευτικότητα και η ασφάλεια των δεδομένων είναι κρίσιμης σημασίας (Meier 2005).

3.4.9 SHA (Secure Hash Algorithm)

Αν και δεν πρόκειται ακριβώς αλγόριθμος κρυπτογράφησης, χρησιμοποιείται ευρέως για τη δημιουργία ασφαλών «αποτυπωμάτων» δεδομένων. Πιο συγκεκριμένα, ο Secure Hash Algorithm (SHA) αποτελεί μια σειρά από κρυπτογραφικούς αλγορίθμους hash, που χρησιμοποιούνται για τη δημιουργία τιμών κερματισμού (hashes) από δεδομένα διαφορετικού μεγέθους. Οι πιο συνηθισμένες εκδόσεις είναι οι SHA-1, SHA-3 και SHA-256. Ο SHA-1 χρησιμοποιήθηκε ευρέως για πολλά χρόνια, αλλά είναι πλέον ευάλωτος σε επιθέσεις, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, εξαιτίας των αδυναμιών στον αλγοριθμικό σχεδιασμό του αλλά και στο μικρό μέγεθος κλειδιού (Penard and van Werkhoven 2008).

Οι πιο σύγχρονες εκδόσεις, όπως ο SHA-3 και ο SHA-256, προσφέρουν υψηλότερα επίπεδα ασφάλειας και χρησιμοποιούνται ευρέως σε διάφορες εφαρμογές, από την ασφάλεια των δικτύων και την ταυτοποίηση δεδομένων μέχρι τη δημιουργία ψηφιακών υπογραφών και την εξασφάλιση της ακεραιότητας δεδομένων. Οι αλγόριθμοι SHA είναι καίριας σημασίας στην εφαρμογή πρωτοκόλλων ασφάλειας, όπως το TLS/SSL, αλλά και στην ασφάλεια των κρυπτονομισμάτων, όπως το Bitcoin (Penard and van Werkhoven 2008).

Η κατανόηση της λειτουργίας των αλγορίθμων SHA, των χαρακτηριστικών τους και των περιορισμών τους είναι ουσιαστική για την αξιολόγηση των τρεχόντων αλλά και μελλοντικών τεχνολογιών ασφάλειας. Ενώ οι παλαιότερες εκδόσεις όπως ο SHA-1 πρέπει να αποφεύγονται σε νέες εφαρμογές, οι νεότερες εκδόσεις συνεχίζουν να προσφέρουν μια αξιόπιστη βάση για την ασφάλεια των δικτυακών και ψηφιακών συστημάτων (Penard and van Werkhoven 2008).

3.4.10 MD5 (Message Digest Method 5 ή Message Digest Algorithm 5)

Ο αλγόριθμος MD5 (Message Digest Algorithm 5) είναι ένας ευρέως χρησιμοποιημένος αλγόριθμος κρυπτογραφικής σύνοψης (*hash*) που παράγει μία τιμή μεγέθους 128-bit (16-byte) από ένα δεδομένο κείμενο. Κατασκευάστηκε αρχικά με σκοπό την εξασφάλιση της ακεραιότητας των δεδομένων και χρησιμοποιήθηκε ευρέως σε πληθώρα εφαρμογών, όπως η επαλήθευση αρχείων, η αποθήκευση κωδικών πρόσβασης και η ψηφιακή υπογραφή εγγράφων (Varatharajan and Bhuvaneshwari 2022).

Ωστόσο, με την πάροδο του χρόνου, αποκαλύφθηκαν σοβαρές ευπάθειες στον MD5, καθιστώντας τον αναποτελεσματικό για κρυπτογραφικές εφαρμογές που απαιτούν υψηλά επίπεδα ασφάλειας. Είναι πλέον πολύ ευκολότερο να πραγματοποιηθεί μια «επίθεση σύγκρουσης» (*collision attack*),

όπου δύο διαφορετικά μηνύματα παράγουν το ίδιο hash, διακινδυνεύοντας έτσι την ακεραιότητα του αλγορίθμου (Varatharajan and Bhuvaneshwari 2022).

Παρά τις ευπάθειές του, ο MD5 συνεχίζει να χρησιμοποιείται σε ορισμένες εφαρμογές που δεν απαιτούν υψηλά επίπεδα κρυπτογραφικής ασφάλειας, όπως η επαλήθευση αρχείων. Εντούτοις, οι ειδικοί συστήνουν τη χρήση πιο ασφαλών αλγορίθμων συνάψεων, όπως το SHA-256, για κρίσιμες εφαρμογές. Η κατανόηση των περιορισμών και των ευπαθειών του MD5 είναι ζωτικής σημασίας για την επιλογή του κατάλληλου αλγορίθμου στην εποχή της ραγδαίας τεχνολογικής εξέλιξης (Varatharajan and Bhuvaneshwari 2022).

3.4.11 HMAC (Hash-based Message Authentication Code)

Ο αλγόριθμος HMAC (Hash-based Message Authentication Code) είναι μια ειδική κατηγορία των αλγορίθμων επαλήθευσης μηνυμάτων που χρησιμοποιούν κρυπτογραφικές συναρτήσεις hash σε συνδυασμό με ένα κρυπτογραφικό κλειδί. Αυτή η προσέγγιση διασφαλίζει ταυτόχρονα την ακεραιότητα και την αυθεντικότητα ενός μηνύματος. Ο HMAC είναι ευέλικτος ως προς την επιλογή της υποκείμενης συνάρτησης hash, όπως SHA-256, MD5, ή SHA-1, παρόλο που ορισμένες από αυτές έχουν κριθεί ως μη ασφαλείς στο πέρασμα του χρόνου (Hussain, Farooq and Ustun 2019).

Οι προδιαγραφές του HMAC τον καθιστούν κατάλληλο για εφαρμογές όπως η ηλεκτρονική υπογραφή δεδομένων, τα συστήματα εξασφάλισης της επικοινωνίας μέσω API, το ηλεκτρονικό εμπόριο, και άλλες διαδικασίες όπου είναι απαραίτητη η επαλήθευση της προέλευσης και της ακεραιότητας των δεδομένων (Hussain, Farooq and Ustun 2019).

Σε σύγκριση με άλλους αλγορίθμους κρυπτογραφικής επαλήθευσης, ο HMAC προσφέρει ένα καλό συμβιβασμό ανάμεσα σε ασφάλεια, ταχύτητα και ευελιξία. Επιπλέον, η δυνατότητα επιλογής της υποκείμενης συνάρτησης hash τον καθιστά προσαρμόσιμο σε διάφορες απαιτήσεις ασφάλειας. Ως εκ τούτου, ο HMAC παραμένει μια από τις πιο διαδεδομένες μεθόδους για την επαλήθευση μηνυμάτων σε πολλές εφαρμογές ασφάλειας δικτύου και συστημάτων (Hussain, Farooq and Ustun 2019).

4 Ομομορφική Κρυπτογραφία

Η κρυπτογραφία αποτελεί έναν σημαντικό τομέα της πληροφορικής και των μαθηματικών, ο οποίος επικεντρώνεται στην ασφάλεια των πληροφοριών. Σε ένα περιβάλλον όπου η εμπιστευτικότητα και η ακεραιότητα των δεδομένων είναι απαραίτητη, η κρυπτογραφία προσφέρει μεθόδους για την προστασία των μηνυμάτων από μη εξουσιοδοτημένες προσβάσεις ή αλλοιώσεις, μετατρέποντας το αρχικό (C. Moore, M. O'Neill, et al. 2014) μήνυμα σε μια μορφή που είναι καταληπτή μόνο από τον προοριζόμενο παραλήπτη, χρησιμοποιώντας κατάλληλους αλγορίθμους και κρυπτογραφικά κλειδιά. Επιπρόσθετα, η κρυπτογραφία μπορεί να υποστηρίξει τη διακρίβωση ταυτότητας και τον καταλογισμό/τη μη δυνατότητα αποποίησης.

Εν συντομία, η κρυπτογραφία παρέχει εγγυήσεις για την επικοινωνία μεταξύ δύο ή περισσότερων μερών, αποκρύπτοντας το περιεχόμενο από τρίτους και προφυλάσσοντας έναντι της αλλοίωσής τους. Αυτό γίνεται με τη χρήση κρυπτογραφικών κλειδιών, τα οποία μπορούν να είναι διαμοιραζόμενα μεταξύ των ενεχομένων μερών ή να εντάσσονται στο σχήμα ιδιωτικά/δημόσια, ανάλογα με το σύστημα κρυπτογραφίας που χρησιμοποιείται. Παρότι η αρχική προσέγγιση της κρυπτογραφίας μπορεί να φαίνεται γραμμική, οι αλγόριθμοι και οι τεχνικές που εφαρμόζονται στην ψηφιακή εποχή είναι εξαιρετικά σύνθετοι και διαρκώς εξελίσσονται. Έτσι, στα πλαίσια της σύγχρονης κρυπτογραφίας, έχουμε την ασύμμετρη κρυπτογραφία, όπου χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση, και τη συμμετρική, όπου χρησιμοποιείται το ίδιο κλειδί για και τις δύο διαδικασίες (Henry 2008).

Η συνεχής εξέλιξη στον τομέα αυτόν είναι απαραίτητη, καθώς οι απειλές και οι τεχνολογίες εξελίσσονται, δημιουργώντας την ανάγκη για πιο σύνθετες και ασφαλείς μεθόδους προστασίας των πληροφοριών. Έτσι, εισερχόμενοι βαθύτερα στον τομέα της κρυπτογραφίας, ανακαλύπτουμε εξειδικευμένες μεθόδους όπως η «ομομορφική κρυπτογραφία». Αυτή η τεχνολογία επιτρέπει την εκτέλεση υπολογισμών πάνω σε κρυπτογραφημένα δεδομένα, χωρίς την ανάγκη αποκρυπτογράφησης τους. Στο αυτό το κεφάλαιο, θα εξετάσουμε λεπτομερέστερα αυτή την προηγμένη μέθοδο κρυπτογραφίας.

Η ομομορφική κρυπτογράφηση αποτελεί ένα κεντρικό θεμέλιο στον κόσμο των κρυπτογραφικών τεχνικών, προαναγγέλλοντας μια νέα εποχή για την ασφάλεια και την ιδιωτικότητα των δεδομένων. Στον πυρήνα της παρέχει τη συναρπαστική δυνατότητα να εκτελεί υπολογισμούς απευθείας σε κρυπτογραφημένα δεδομένα, καταργώντας την ανάγκη πρώτα να αποκρυπτογραφεί τα δεδομένα για να τα επεξεργαστεί. Αυτή η φαινομενικά αντιφατική δυνατότητα αντιπροσωπεύει μια βαθιά αλλαγή από τις παραδοσιακές κρυπτογραφικές μεθόδους, και οι επιπτώσεις της για διάφορους τομείς, από την υγεία μέχρι τα οικονομικά, είναι τεράστιες (Henry 2008).

Η γέννηση της ομομορφικής κρυπτογράφησης επιστρέφει στις πρώτες προσπάθειες να αυξηθεί η ευελιξία των σχημάτων κρυπτογράφησης. Καθώς η τεχνολογία εξελίχθηκε και τα δεδομένα έγιναν πολύτιμο στοιχείο, προέκυψε μια επείγουσα ανάγκη να μην ασφαλίζουμε απλώς τα δεδομένα, αλλά να αλληλεπιδρούμε με αυτά στην ασφαλισμένη τους μορφή. Η ομομορφική κρυπτογράφηση ξεκίνησε με ακαδημαϊκή έρευνα, ενώ ακολούθως δημιουργήθηκαν και εξελίχθηκαν μέθοδοι για την εφαρμογή της και διεξήχθησαν διαπραγματεύσεις και συζητήσεις σε οργανισμούς τυποποίησης που καθόρισαν την τρέχουσα πορεία της. (Henry 2008).

Στη συνέχεια θα παραθέσουμε σχήματα κατηγοριοποίησης τύπων ομομορφικής κρυπτογράφησης, καθώς και σχετικές αναλύσεις. Κάθε τύπος έχει διακριτές δυνατότητες, περιορισμούς και

προσήκουσες περιπτώσεις χρήσης. Η κατανόηση των διαφορών ανάμεσα σε αυτούς τους τύπους είναι σημαντική για την εκτίμηση του φάσματος των δυνατοτήτων που παρέχουν (Henry 2008).

Εμβαθύνοντας στα χαρακτηριστικά της ομομορφικής κρυπτογράφησης, θα καταγράψουμε τις βασικές της αρχές και τις περίπλοκες μαθηματικές βάσεις που υποστηρίζουν τις λειτουργίες της. Η λειτουργικότητά της, παρόλο που είναι περίπλοκη, μπορεί να συνοψιστεί σε μια σειρά βημάτων και πρωτοκόλλων που επιτρέπουν τον ασφαλή χειρισμό των δεδομένων. Κάθε βήμα, από την κρυπτογράφηση έως τον υπολογισμό και την τελική αποκρυπτογράφηση, διατηρεί την ακεραιότητα των δεδομένων ενώ επιτρέπει σημαντικές λειτουργίες σε αυτά (Henry 2008).

Η ομομορφική κρυπτογράφηση, όπως κάθε προηγμένη τεχνολογία, παρουσιάζει πλεονεκτήματα και αδυναμίες. Από τη μια πλευρά, δύναται να παρέχει υψηλά επίπεδα ασφάλειας δεδομένων και να χρησιμοποιηθεί σε μεγάλο εύρος τομέων, επιτρέποντας την επεξεργασία ευαίσθητων πληροφοριών σε πραγματικό χρόνο χωρίς ποτέ να εκθέτει την ακατέργαστη τους μορφή. Από την άλλη πλευρά, ορισμένες προκλήσεις, ιδιαίτερα σχετιζόμενες με την αύξηση του υπολογιστικού κόστους και την αποδοτικότητα, μετριάζουν την υιοθέτησή της σε ευρεία κλίμακα (Henry 2008).

Τέλος, εξετάζονται δημοφιλείς αλγόριθμοι που αποτελούν το θεμέλιο της ομομορφικής κρυπτογράφησης. Κάθε αλγόριθμος, είτε πρόκειται για το πρωτοποριακό έργο του RSA είτε για πιο πρόσφατες προόδους όπως τα σχήματα BGV και CKKS, προσφέρει μια μοναδική προοπτική και ένα σύνολο εργαλείων για τον χειρισμό των κρυπτογραφημένων υπολογισμών. Με τη μελέτη των αλγορίθμων είναι δυνατό να σχηματοποιηθούν νέοι τρόποι με τους οποίους η κρυπτογραφική έρευνα διαμορφώνει και επαναπροσδιορίζει τα όρια της ασφάλειας των δεδομένων (Henry 2008).

4.1 Σύντομη ιστορική αναδρομή

Η έννοια της ομομορφικής κρυπτογράφησης έχει τις ρίζες της στα αρχικά στάδια της σύγχρονης έρευνας στην περιοχή της κρυπτογραφίας στη δεκαετία του 1970. Κατά τη διάρκεια αυτής της δεκαετίας, καθώς το ευρύτερο πεδίο της κρυπτογραφίας βίωνε ταχείες προόδους λόγω της ανάδυσης της ψηφιακής επικοινωνίας, ένα σύνολο πρωτοπόρων ερευνητών άρχισε να εμβαθύνει στην ενδιαφέρουσα ιδέα της εκτέλεσης υπολογισμών σε δεδομένα που παρέμεναν κρυπτογραφημένα. Αυτή ήταν μια βαθιά αλλαγή στη σκέψη, καθώς παραδοσιακά, τα δεδομένα χρειαζόταν να αποκρυπτογραφηθούν προτού μπορούσαν να εκτελεστούν σημαντικές λειτουργίες πάνω τους, εκθέτοντας ευαίσθητες πληροφορίες στη διαδικασία (Sharma, et al. 2021).

Το κίνητρο πίσω από την ομομορφική κρυπτογράφηση προέρχεται από την επιθυμία να διασφαλιστεί η ιδιωτικότητα και η ασφάλεια σε μια ολοένα και πιο ψηφιακή εποχή. Καθώς επιχειρήσεις, κυβερνήσεις και άτομα αντιμετώπιζαν τις προκλήσεις της αποθήκευσης και μετάδοσης δεδομένων με ασφάλεια, η δυνατότητα εκτέλεσης υπολογισμών σε κρυπτογραφημένα δεδομένα χωρίς ποτέ να εκτίθεται το πρωτότυπο δεδομένο ήταν μία προοπτική που θα πρόσφερε σημαντικά οφέλη, ειδικά σε σενάρια όπου η ιδιωτικότητα των δεδομένων ήταν αυξημένης σημασίας, αλλά οι υπολογισμοί πάνω στα δεδομένα ήταν απαραίτητοι. Ως ενδεικτικοί τομείς εφαρμογής αναφέρονται η ιατρική έρευνα (η οποία αφορά ευαίσθητα προσωπικά δεδομένα ασθενών), οι χρηματοοικονομικές συναλλαγές στα τραπεζικά συστήματα, καθώς και τα ασφαλή εκλογικά συστήματα (Sharma, et al. 2021).

Κατά τις επόμενες δεκαετίες, αυτή η αρχική έννοια ωρίμασε και εξελίχθηκε, οδηγώντας στη γέννηση διαφόρων τύπων σχημάτων ομομορφικής κρυπτογράφησης. Καθένα από αυτά τα σχήματα, ενώ μοιράζεται τη βασική ιδέα των υπολογισμών σε κρυπτογραφημένα δεδομένα, είχε διακριτές

μαθηματικές ιδιότητες, υπολογιστικές αποδόσεις και εγγυήσεις ασφάλειας. Αυτές οι διαφορές καθιστούσαν κάθε σχήμα πιο κατάλληλο για συγκεκριμένες εφαρμογές. Για παράδειγμα, κάποια σχήματα επέτρεπαν μόνο συγκεκριμένους τύπους λειτουργιών, όπως πρόσθεση ή πολλαπλασιασμό, ενώ άλλα ήταν σχεδιασμένα να χειρίζονται πιο περίπλοκους υπολογισμούς, με επιβάρυνση ωστόσο σε υπολογιστικό φόρτο (Sharma, et al. 2021).

Η έρευνα και ανάπτυξη των σχημάτων ομομορφικής κρυπτογράφησης έχουν ενισχυθεί από τη συνεργασία μεταξύ της ακαδημαϊκής κοινότητας και της βιομηχανίας, όπου κάθε συνεργαζόμενο μέρος εισφέρει τις δικές του προοπτικές και προκλήσεις. Οι ερευνητές του ακαδημαϊκού χώρου εξετάζουν τι είναι μαθηματικά δυνατό και διευρύνουν τα όρια των θεωριών και των αλγορίθμων, αναπτύσσοντας θεωρητικές δομές και αποδείξεις, ενώ οι επαγγελματίες της βιομηχανίας επικεντρώνονται στην πρακτική εφαρμογή, μεριμνώντας για την αποτελεσματική ενσωμάτωση των σχημάτων αυτών σε πραγματικά συστήματα (Sharma, et al. 2021)

4.2 Βασικές έννοιες

Η ομομορφική κρυπτογραφία είναι ένα σύνθετο πεδίο με πολλές υποκείμενες έννοιες. Οι ακόλουθες έννοιες θέτουν τις βάσεις για την κατανόηση της ομομορφικής κρυπτογραφίας και των πιθανών εφαρμογών της στον ασφαλή υπολογισμό και το απόρρητο δεδομένων:

Κρυπτογράφηση είναι η διαδικασία μετατροπής δεδομένων απλού κειμένου (plaintext) σε ακατάληπτη και μη αναγνώσιμη μορφή που ονομάζεται κρυπτογραφημένο κείμενο, χρησιμοποιώντας έναν συγκεκριμένο αλγόριθμο κρυπτογράφησης και ένα μυστικό κλειδί. Στην ομομορφική κρυπτογραφία, η κρυπτογράφηση επιτρέπει στα δεδομένα να παραμένουν εμπιστευτικά κατά την επεξεργασία (Henry 2008).

Κρυπτογραφικό κλειδί: Μια παράμετρος που χρησιμοποιείται στις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Πιο συγκεκριμένα, πρόκειται για μια ακολουθία από bits που χρησιμοποιείται από αλγόριθμους κρυπτογραφίας για την κρυπτογράφηση ή αποκρυπτογράφηση δεδομένων. Στην **συμμετρική κρυπτογραφία**, το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Στην **ασυμμετρική κρυπτογραφία**, υπάρχει ένα ζευγάρι κλειδιών: ένα δημόσιο κλειδί για κρυπτογράφηση και ένα ιδιωτικό κλειδί για αποκρυπτογράφηση (Henry 2008).

Αποκρυπτογράφηση είναι η αντίστροφη διαδικασία κρυπτογράφησης, όπου το κρυπτογραφημένο κείμενο μετατρέπεται ξανά σε απλό κείμενο χρησιμοποιώντας τον αντίστοιχο αλγόριθμο αποκρυπτογράφησης και το κατάλληλο κλειδί. Η αποκρυπτογράφηση σε σχήματα όπου χρησιμοποιείται ομομορφική κρυπτογράφηση πραγματοποιείται αφού ολοκληρωθεί ο υπολογισμός στα κρυπτογραφημένα δεδομένα (Henry 2008).

Μη εύπλαστη μορφή: Η μη εύπλαστη (non-malleable) μορφή δεδομένων στην κρυπτογραφία αναφέρεται σε μια κατάσταση όπου τα δεδομένα είναι κρυπτογραφημένα και δεν μπορούν να αποκρυπτογραφηθούν ή να διαβαστούν χωρίς το σωστό κλειδί (Henry 2008).

Ομομορφισμός είναι μια μαθηματική ιδιότητα που επιτρέπει στις πράξεις στα κρυπτογραφημένα δεδομένα να αντιστοιχούν σε πράξεις στα αρχικά δεδομένα απλού κειμένου. Στην ομομορφική κρυπτογραφία, αυτή η ιδιότητα επιτρέπει τον υπολογισμό σε κρυπτογραφημένα δεδομένα χωρίς να απαιτείται η πρότερη αποκρυπτογράφησή τους (Henry 2008).

Μερική Ομομορφική Κρυπτογράφηση (Partially Homomorphic Cryptography - PHE): Τα σχήματα PHE υποστηρίζουν έναν μόνο τύπο λειτουργίας σε κρυπτογραφημένα δεδομένα (π.χ. πρόσθεση ή πολλαπλασιασμό). Παραδείγματα περιλαμβάνουν τα κρυπτοσυστήματα RSA και ElGamal (Henry 2008).
Σχετικά Ομομορφική κρυπτογράφηση (Somewhat Homomorphic Cryptography – SHE): Τα σχήματα SHE επιτρέπουν περιορισμένο αριθμό λειτουργιών σε κρυπτογραφημένα δεδομένα, αλλά ο θόρυβος που εισάγεται κατά τη διάρκεια αυτών των λειτουργιών συσσωρεύεται και τελικά καθιστά την αποκρυπτογράφηση ανέφικτη (Henry 2008).
Πλήρης Ομομορφική κρυπτογράφηση (Fully Homomorphic Cryptography – FHE): Τα σχήματα FHE υποστηρίζουν απεριόριστο αριθμό λειτουργιών σε κρυπτογραφημένα δεδομένα, επιτρέποντας αυθαίρετους υπολογισμούς χωρίς απώλεια ασφάλειας ή πληροφορίας. Το FHE προτάθηκε για πρώτη φορά από τον Craig Gentry το 2009 .
Κρυπτογραφία βασισμένη σε πλέγμα (Lattice-based cryptography) είναι μια κατηγορία κρυπτογραφικών σχημάτων που βασίζονται στη μαθηματική δομή των πλεγμάτων, τα οποία είναι διακριτά, περιοδικά πλέγματα σημείων σε ένα χώρο υψηλών διαστάσεων. Πολλά σχήματα FHE, συμπεριλαμβανομένης της αρχικής κατασκευής του Gentry, βασίζονται στην κρυπτογραφία πλέγματος (Henry 2008).
Ψηφιακή Υπογραφή: Μια τεχνική που επιβεβαιώνει την αυθεντικότητα και την ακεραιότητα ενός μηνύματος ή ενός ηλεκτρονικού εγγράφου. Λειτουργεί ως ένα είδος ηλεκτρονικής "σφραγίδας" για τα δεδομένα, δηλώνοντας ότι προέρχονται από ένα συγκεκριμένο αποστολέα και ότι δεν έχουν τροποποιηθεί (Henry 2008).
Δυσκολία υπολογισμού (Computational hardness): Τα σχήματα ομομορφικής κρυπτογράφησης βασίζονται στην υπόθεση ότι ορισμένα μαθηματικά προβλήματα, όπως το πρόβλημα μάθησης με σφάλματα (learning with errors - LWE) ή το πρόβλημα μικρής ακέραιας λύσης (short integer solution - SIS), είναι υπολογιστικά δύσκολο να επιλυθούν. Η ασφάλεια των κρυπτογραφημένων δεδομένων εξαρτάται από αυτή τη δυσκολία υπολογισμού (Henry 2008).
Bootstrapping: Το bootstrapping είναι μια τεχνική που χρησιμοποιείται σε σχήματα FHE για την ανανέωση του κρυπτογραφημένου κειμένου μειώνοντας τον συσσωρευμένο θόρυβο, επιτρέποντας απεριόριστο αριθμό λειτουργιών σε κρυπτογραφημένα δεδομένα (Henry 2008).
Ομαδοποίηση: Η ομαδοποίηση είναι μια τεχνική που χρησιμοποιείται για τη βελτίωση της αποτελεσματικότητας της ομομορφικής κρυπτογράφησης με την κωδικοποίηση πολλαπλών στοιχείων δεδομένων απλού κειμένου σε ένα μόνο κρυπτογραφημένο κείμενο και την εκτέλεση λειτουργιών σε αυτά ταυτόχρονα (Henry 2008).

4.3 Χαρακτηριστικά και λειτουργία

Η ομομορφική κρυπτογράφηση προσφέρει ξεχωριστά χαρακτηριστικά που τη διαφοροποιούν από τις παραδοσιακές τεχνικές κρυπτογράφησης. Στον πυρήνα της, το κύριο αντικείμενό της αφορά τη διατήρηση της ιδιωτικότητας των δεδομένων. Η διατήρηση της ιδιωτικότητας στο πλαίσιο της ομομορφικής κρυπτογράφησης διασφαλίζει ότι οι πληροφορίες, μόλις κρυπτογραφηθούν, παραμένουν απροσπέλαστες σε μη εξουσιοδοτημένους χρήστες ή συστήματα, ακόμα και κατά τη διάρκεια υπολογιστικών λειτουργιών (C. Moore, M. O'Neill, et al. 2014).

Η εμπιστευτικότητα των δεδομένων είναι άλλο ένα προσόν της ομομορφικής κρυπτογράφησης. Σε αντίθεση με τις τυπικές μεθόδους κρυπτογράφησης, όπου τα δεδομένα πρέπει να αποκρυπτογραφηθούν πριν γίνει οποιαδήποτε έγκυρη λειτουργία πάνω τους, η ομομορφική

κρυπτογράφηση διασφαλίζει ότι τα δεδομένα παραμένουν κρυπτογραφημένα, και άρα διατηρείται ο βαθμός εμπιστευτικότητάς τους, καθ' όλη τη διάρκεια του κύκλου ζωής τους. Με τον τρόπο αυτό, προάγονται και οι ασφαλείς υπολογισμοί (C. Moore, M. O'Neill, et al. 2014).

Από πλευράς λειτουργικότητας, η ομομορφική κρυπτογράφηση αντιπροσωπεύει μια καινοτόμα προσέγγιση στη διασφάλιση της ασφάλειας και της ιδιωτικότητας των δεδομένων, ιδιαίτερα στον τομέα του cloud computing και των υπηρεσιών υπολογιστικής διά αναθέσεως (outsourcing computing). Αυτό σημαίνει ότι οι πάροχοι υπηρεσιών, όπως οι πλατφόρμες αποθήκευσης στο cloud ή οι υπηρεσίες υπολογισμού, μπορούν να επεξεργάζονται κρυπτογραφημένα δεδομένα χωρίς ποτέ να έχουν πρόσβαση στις ακατέργαστες, μη κρυπτογραφημένες πληροφορίες (C. Moore, M. O'Neill, et al. 2014).

Ένας από τους κύριους τομείς που αναμένεται να επωφεληθεί σημαντικά από αυτήν την τεχνολογία είναι ο υγειονομικός. Με την αυξανόμενη ψηφιοποίηση των ιατρικών αρχείων και την εισαγωγή της τηλεϊατρικής, υπάρχει μια εντεινόμενη ανάγκη για ασφάλεια των ευαίσθητων δεδομένων των ασθενών. Η ομομορφική κρυπτογράφηση εξασφαλίζει ότι τα ιατρικά αρχεία που αποθηκεύονται στο cloud, ή οι αναλύσεις που γίνονται σε αυτά τα αρχεία, παραμένουν ιδιωτικά και απρόσιτα σε μη εξουσιοδοτημένα μέρη. Αυτό όχι μόνο προσφέρει ασφάλεια στους ασθενείς, αλλά βοηθάει επίσης τους παρόχους υγειονομικής περίθαλψης να διατηρούν πλήρη συμμόρφωση με αυστηρούς κανονισμούς προστασίας δεδομένων, όπως τον κανονισμό HIPAA στις Ηνωμένες Πολιτείες αλλά και τον GDPR στην Ευρώπη (C. Moore, M. O'Neill, et al. 2014).

Ομοίως, ο χρηματοοικονομικός τομέας, που παραδοσιακά βασίζεται σε συναλλαγές και ανταλλαγές δεδομένων, μπορεί να χρησιμοποιήσει την ομομορφική κρυπτογράφηση για να ενισχύσει την ασφάλεια των δεδομένων. Οι τράπεζες, οι χρηματοπιστωτικές ιδρυματικές παροχές και οι fintech startups μπορούν να τελέσουν υπολογισμούς σε πλατφόρμες τρίτων χωρίς να διακυβεύεται η εμπιστευτικότητα των χρηματοοικονομικών δεδομένων των πελατών τους. Αυτό είναι σημαντικό, ιδίως λαμβάνοντας υπ’ όψιν τον αυξανόμενο αριθμό των κυβερνοεπιθέσεων που στοχεύουν τη χρηματοπιστωτική βιομηχανία (C. Moore, M. O'Neill, et al. 2014).

Η μηχανική μάθηση και η τεχνητή νοημοσύνη είναι άλλοι τομείς όπου η ομομορφική κρυπτογράφηση μπορεί να έχει εφαρμογή. Η εκπαίδευση των μοντέλων μηχανικής μάθησης συχνά απαιτεί πρόσβαση σε μεγάλες ποσότητες δεδομένων. Χρησιμοποιώντας ομομορφική κρυπτογράφηση, οι εταιρείες μπορούν να εκπαιδεύσουν αυτά τα μοντέλα σε κρυπτογραφημένα δεδομένα από διάφορες πηγές χωρίς ποτέ να βλέπουν τα πραγματικά ακατέργαστα δεδομένα. Αυτό εξασφαλίζει ότι τα προσωπικά ή ευαίσθητα δεδομένα που χρησιμοποιούνται στα σύνολα δεδομένων εκπαίδευσης παραμένουν ιδιωτικά, αντιμετωπίζοντας τις αυξανόμενες ανησυχίες σχετικά με την ιδιωτικότητα των δεδομένων στην εποχή της τεχνητής νοημοσύνης (C. Moore, M. O'Neill, et al. 2014).

Οι δυνατότητες της ομομορφικής κρυπτογράφησης αναδιαμορφώνουν τον τρόπο με τον οποίο οι βιομηχανίες προσεγγίζουν την ασφάλεια και την ιδιωτικότητα των δεδομένων. Σημειώνεται ότι οι πιθανές εφαρμογές της εκτείνονται πολύ πέρα από τους απλούς υπολογισμούς στο νέφος (cloud) και τον εξωτερικευμένο υπολογισμό, επιτρέποντας τον σχεδιασμό συστημάτων όπου η ιδιωτικότητα των δεδομένων δεν ενσωματώνεται ευκαιριακά, αλλά αποτελεί ένα βασικό αρχικό στοιχείο των απαιτήσεων και των προδιαγραφών, σύμφωνα με το πνεύμα του «security by design» (C. Moore, M. O'Neill, et al. 2014).

4.4 Πλεονεκτήματα και μειονεκτήματα

Ένα από τα πιο σημαντικά πλεονεκτήματα της χρήσης της ομομορφικής κρυπτογράφησης είναι το αυξημένο επίπεδο ασφάλειας που παρέχει. Αυτό οφείλεται κυρίως στο γεγονός ότι καταργεί την ανάγκη να εκτίθεται το απλό κείμενο, ή μη κρυπτογραφημένα δεδομένα, κατά τη διάρκεια των υπολογιστικών διαδικασιών. Διασφαλίζοντας ότι τα δεδομένα παραμένουν κρυπτογραφημένα καθ' όλη τη διάρκεια της ζωής τους, ακόμα και κατά την επεξεργασία ή ανάλυση, τα ρίσκα που σχετίζονται με τυχόν παραβιάσεις δεδομένων ή μη εξουσιοδοτημένη πρόσβαση μειώνονται σημαντικά (Zhang, Yan and Kantola 2016).

Ένα άλλο σημαντικό όφελος της ομομορφικής κρυπτογράφησης είναι ο βαθμός ευελιξίας που εισάγει, ιδιαίτερα σε συνεργατικά περιβάλλοντα ή σενάρια όπου τα δεδομένα κοινοποιούνται μεταξύ πολλαπλών οντοτήτων. Η τεχνική επιτρέπει σε διάφορα μέρη να εκτελούν μαθηματικούς υπολογισμούς σε κρυπτογραφημένα δεδομένα που κοινοποιούνται. Αυτή η δυνατότητα είναι ιδιαίτερα προνομιακή σε συνθήκες όπως το cloud computing, όπου πολλοί πελάτες ενδέχεται να χρειάζεται να αλληλεπιδρούν με ή να επεξεργάζονται κοινά δεδομένα. Με την ομομορφική κρυπτογράφηση, αυτά τα μέρη μπορούν να συμμετέχουν σε αυτές τις λειτουργίες χωρίς ποτέ να αποκαλύπτουν ή να θέτουν σε κίνδυνο τις ευαίσθητες πληροφορίες που περιέχονται στα δεδομένα. Μια τέτοια χαρακτηριστική ιδιότητα προάγει ένα περιβάλλον εμπιστοσύνης, καθώς οι ενδιαφερόμενοι μπορούν να είναι βέβαιοι ότι τα εμπιστευτικά τους δεδομένα παραμένουν προστατευμένα από άλλους συμμετέχοντες, ακόμα και καθώς γίνονται υπολογισμοί (Zhang, Yan and Kantola 2016).

Παρά τα σημαντικά αυτά πλεονεκτήματα, είναι ουσιώδες να προσεγγίζουμε την ομομορφική κρυπτογράφηση γνωρίζοντας και αναγνωρίζοντας τους πιθανούς περιορισμούς της. Ένα σημαντικό μειονέκτημα είναι το υπολογιστικό κόστος που σχετίζεται με αυτήν τη μορφή κρυπτογράφησης. Σε σύγκριση με τις παραδοσιακές κρυπτογραφικές μεθόδους, οι οποίες συχνά απαιτούν μόνο διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης στα τελικά σημεία αποθήκευσης ή μεταφοράς δεδομένων, η ομομορφική κρυπτογράφηση απαιτεί περισσότερους υπολογιστικούς πόρους. Αυτό οφείλεται στο γεγονός ότι επιτρέπει λειτουργίες σε κρυπτογραφημένα δεδομένα άμεσα. Ως αποτέλεσμα, μπορεί να απαιτήσει επιπλέον πόρους (overhead), πιθανώς επιβραδύνοντας τις διαδικασίες και απαιτώντας πιο ισχυρές υποδομές σε hardware (Zhang, Yan and Kantola 2016).

Επιπλέον, η περίπλοκη φύση της ομομορφικής κρυπτογράφησης σημαίνει ότι δεν είναι μια λύση άμεσης υλοποίησης και λειτουργίας. Η επιτυχής και ασφαλής υλοποίηση συχνά απαιτεί εξειδικευμένη γνώση στον τομέα της κρυπτογραφίας. Οι επαγγελματίες ή οι οργανισμοί που επιθυμούν να αξιοποιήσουν αυτήν την τεχνολογία πρέπει να διασφαλίσουν ότι έχουν πρόσβαση στην απαραίτητη γνώση αλλά και εμπειρία, είτε εσωτερικά, είτε μέσω εξωτερικών συμβούλων. Αυτή η εξειδικευμένη γνώση είναι απαραίτητη για να αντιμετωπίσουν τις πολυπλοκότητες της τεχνολογίας αυτής και να διασφαλιστεί ότι χρησιμοποιείται με τρόπο που διατηρεί πραγματικά την ακεραιότητα και την ασφάλεια των δεδομένων (Zhang, Yan and Kantola 2016).

4.5 Κατηγορίες ομομορφικών αλγορίθμων

Η ομομορφική κρυπτογράφηση, μπορεί να ταξινομηθεί σε τρεις κύριες κατηγορίες:

- Μερικώς Ομομορφική Κρυπτογράφηση (*μτφρ. Partially Homomorphic Encryption* - PHE),

- Σχετικώς Ομομορφική Κρυπτογράφηση (*μτφρ. Somewhat Homomorphic Encryption* - SHE) και
- Πλήρως Ομομορφική Κρυπτογράφηση (*μτφρ. Fully Homomorphic Encryption* - FHE).

Κάθε ένας από αυτές τις τύπους προσφέρει διαφορετικά επίπεδα υπολογιστικών δυνατοτήτων σε κρυπτογραφημένα δεδομένα, με διαφορετικά ισοζύγια μεταξύ ευελιξίας και υπολογιστικής αποτελεσματικότητας (Zhang, Yan and Kantola 2016).

Η Μερικώς Ομομορφική Κρυπτογράφηση (PHE) αντιπροσωπεύει την πιο απλή μορφή της ομομορφικής κρυπτογράφησης. Υποστηρίζει τη δυνατότητα να εκτελείται ένας μόνο τύπος λειτουργίας - είτε πρόσθεση είτε πολλαπλασιασμός - σε κρυπτογραφημένα δεδομένα, αλλά όχι και τα δύο ταυτόχρονα. Αν και αυτή η διευθέτηση μπορεί να φαίνεται ιδιαίτερα περιοριστική, το PHE έχει τις εφαρμογές του όταν χρειάζεται μόνο ένας συγκεκριμένος τύπος υπολογισμών στα κρυπτογραφημένα δεδομένα (Zhang, Yan and Kantola 2016).

Η Σχετικώς Ομομορφική Κρυπτογράφηση (SHE) μπορεί να θεωρηθεί ως μια επέκταση της PHE. Διευκολύνει ένα ευρύτερο φάσμα υπολογισμών σε κρυπτογραφημένα δεδομένα, αν και υπάρχει ακόμη ένα όριο στον αριθμό και στην πολυπλοκότητα των λειτουργιών που μπορεί να υποστηρίξει. Το «σχετικώς» υπονοεί ότι προσφέρει περισσότερη υπολογιστική ευελιξία από το PHE αλλά υπολείπεται της ευελιξίας και της λειτουργικότητας της FHE. Τα συστήματα SHE χρησιμοποιούνται συχνά σε σενάρια όπου οι υπολογιστικές ανάγκες υπερβαίνουν τις δυνατότητες της PHE αλλά δεν απαιτούν την πλήρη ισχύ της FHE (Zhang, Yan and Kantola 2016).

Στην άλλη άκρη του φάσματος βρίσκεται η Πλήρως Ομομορφική Κρυπτογράφηση (FHE), η οποία επιτρέπει την τέλεση τυχαίων υπολογισμών σε κρυπτογραφημένα δεδομένα, υπερβαίνοντας ουσιαστικά τους περιορισμούς που αντιμετωπίζουν οι PHE και SHE. Με την FHE, μπορεί κανείς να πραγματοποιεί τόσο προσθέσεις όσο και πολλαπλασιασμούς όσες φορές χρειάζεται χωρίς ποτέ να χρειάζεται να αποκρυπτογραφήσει τα δεδομένα. Αυτή η εξαιρετική ικανότητα διασφαλίζει ότι τα δεδομένα μπορούν να παραμείνουν εμπιστευτικά κατά την επεξεργασία τους, μια ιδιότητα που έχει τεράστιες επιπτώσεις για την ασφαλή υπολογιστική νέφους, την ιδιωτική ανάλυση δεδομένων και πολλές άλλες εφαρμογές. Ωστόσο, αυτή η ευελιξία συχνά έρχεται με ένα τίμημα: τα συστήματα FHE είναι γενικά πιο υπολογιστικά κοστοβόρα από τα αντίστοιχα PHE και SHE (Zhang, Yan and Kantola 2016).

Συμπερασματικά, η ομομορφική κρυπτογράφηση καλύπτει από την απλούστερη, μονής-λειτουργίας δυνατότητα της PHE έως την απεριόριστη υπολογιστική ελευθερία του FHE, με το SHE να εξυπηρετεί ως μια ενδιάμεση λύση. Η επιλογή μεταξύ αυτών των προσεγγίσεων εξαρτάται από τις συγκεκριμένες ανάγκες και περιορισμούς μιας δεδομένης εφαρμογής, ισοζυγίζοντας παράγοντες όπως η υπολογιστική αποτελεσματικότητα, οι απαιτήσεις ασφαλείας και το επιθυμητό εύρος λειτουργιών.

4.5.1 Μερική ομομορφική κρυπτογραφία (PHE)

Σε αντίθεση με την πλήρη ομομορφική κρυπτογραφία (FHE), που επιτρέπει ένα απεριόριστο αριθμό και είδος πράξεων πάνω σε κρυπτογραφημένα δεδομένα, η PHE περιορίζεται σε συγκεκριμένες πράξεις, όπως πρόσθεση ή πολλαπλασιασμό.

Η Μερικώς ομομορφική κρυπτογραφία είναι ένα πολύτιμο εργαλείο για την επεξεργασία κρυπτογραφημένων δεδομένων σε συγκεκριμένες περιπτώσεις, αλλά όπως κάθε εργαλείο, έχει τα δικά του πλεονεκτήματα και μειονεκτήματα. Σε σχέση με τις μεθόδους SHE και FHE, η PHE προσφέρει τα εξής πλεονεκτήματα: είναι συνήθως πιο αποδοτική σε ό,τι αφορά την ταχύτητα και τη χωρητικότητα, καθώς δεν απαιτεί τόσο περίπλοκες υπολογιστικές διαδικασίες, και μπορεί να είναι ιδανική για εφαρμογές που δεν απαιτούν πλήρη ομομορφία. Επίσης, η εκτέλεση πράξεων στη PHE είναι συχνά πιο άμεση και λιγότερο περίπλοκη (Acar, et al. 2018).

Ωστόσο, η PHE δεν είναι άτρωτη σε μειονεκτήματα. Παρόλο που είναι πιο αποδοτική, δεν προσφέρει την ίδια ευελιξία με τα άλλα συστήματα. Η έλλειψη ικανότητας για απεριόριστες πράξεις ή πράξεις αυξημένης πολυπλοκότητας μπορεί να περιορίζει τις εφαρμογές στις οποίες μπορεί να χρησιμοποιηθεί. Επιπλέον, όταν ένα σύστημα απαιτεί πράξεις πέρα από τις βασικές που προσφέρει η PHE, θα πρέπει να γίνεται επανειλημμένη αποκρυπτογράφηση και κρυπτογράφηση, πρακτική που μπορεί να μην είναι επιθυμητή από πολλές εφαρμογές (Acar, et al. 2018).

Παρακάτω ακολουθούν οι δημοφιλέστεροι ομομορφικοί αλγόριθμοι της PHE (Acar, et al. 2018):

Ο αλγόριθμος RSA

- Εισήχθη το 1977 από τους Ron Rivest, Adi Shamir, και Leonard Adleman.
- **Καινοτομία:** Ο RSA ήταν ένα από τα πρώτα κρυπτοσυστήματα δημοσίου κλειδιού και χρησιμοποιείται ευρέως για ασφαλή μετάδοση δεδομένων. Η ασφάλειά του βασίζεται στη δυσκολία του παραγοντοποίησης μεγάλων σύνθετων αριθμών.
- **Ομομορφική Ιδιότητα:** Το κρυπτοσύστημα RSA έχει ένα πολλαπλασιαστικό ομομορφικό χαρακτηριστικό. Δηλαδή, δεδομένων των κρυπτογραφήσεων δύο μηνυμάτων, κανείς μπορεί να παράγει την κρυπτογράφηση του γινομένου τους χωρίς να αποκρυπτογραφήσει τα μηνύματα.

Ο αλγόριθμος ElGamal

- Εισήχθη το 1985 από τον Taher ElGamal.
- **Καινοτομία:** Το ElGamal σχεδιάστηκε ως μια εναλλακτική λύση στο RSA. Σε αντίθεση με το RSA, το ElGamal βασίζει την ασφάλειά του στο Πρόβλημα Διακριτού Λογαρίθμου.
- **Ομομορφική Ιδιότητα:** Το σύστημα κρυπτογράφησης ElGamal έχει ένα πολλαπλασιαστικό ομομορφικό χαρακτηριστικό παρόμοιο με το RSA.

Ο αλγόριθμος Goldwasser-Micali (GM)

Εισήχθη το 1984 από τους Shafi Goldwasser και Silvio Micali.

- **Καινοτομία:** Το σύστημα GM ήταν από τα πρώτα που προσέφεραν σημασιολογική ασφάλεια, μια ισχυρότερη έννοια ασφάλειας από τα προηγούμενα συστήματα.
- **Ομομορφική Ιδιότητα**: Το σύστημα GM υποστηρίζει μια ομομορφική λειτουργία XOR.

Ο αλγόριθμος Benaloh

- Εισήχθη στα τέλη της δεκαετίας του 1980 από τον Josh Benaloh.
- **Καινοτομία:** Το κρυπτοσύστημα Benaloh επεκτείνει το σύστημα Goldwasser–Micali, επιτρέποντας την κρυπτογράφηση μεγαλύτερων μπλοκ δεδομένων.
- **Ομομορφική Ιδιότητα:** Το σύστημα Benaloh είναι γνωστό για την προσθετική του ομομορφική ιδιότητα.

Ο αλγόριθμος Paillier

- Εισήχθη το 1999 από τον Pascal Paillier.
- **Καινοτομία:** Το κρυπτοσύστημα Paillier διακρίνεται για τις ξεχωριστές ομομορφικές ιδιότητές του. Ενώ η πλειονότητα των προηγούμενων συστημάτων υποστήριζε πολλαπλασιαστική ομομορφία, το Paillier εισήγαγε ένα σύστημα με προσθετική ομομορφία.
- **Ομομορφική Ιδιότητα:** Συγκεκριμένα, με το σύστημα Paillier, αν πάρουμε την κρυπτογράφηση δύο μηνυμάτων, μπορούμε να παραγάγουμε την κρυπτογράφηση του αθροίσματός τους, χωρίς να αποκρυπτογραφήσουμε τα αρχικά μηνύματα.

4.5.2 Σχετική ομομορφική κρυπτογραφία (SHE)

Η SHE είναι μία ενδιάμεση κατηγορία ανάμεσα στη μερικώς (PHE) και την πλήρως ομομορφική κρυπτογραφία (FHE). Επιτρέπει την εκτέλεση ενός περιορισμένου αριθμού πράξεων σε κρυπτογραφημένα δεδομένα, πριν απαιτηθεί μια διαδικασία «αναδιάταξης» (relinearization) ή «εκκαθάρισης» (bootstrapping) (Acar, et al. 2018).

Οι περιπτώσεις όπου η SHE υπερτερεί έναντι των PHE και FHE είναι όταν χρειάζεται μια ισορροπία μεταξύ ταχύτητας και ευελιξίας. Δεδομένου ότι η SHE επιτρέπει περισσότερες πράξεις από την PHE, αλλά δεν απαιτεί τους υπολογιστικούς πόρους της FHE, είναι συχνά η προτιμώμενη επιλογή για σύνθετες εφαρμογές που δεν απαιτούν απεριόριστες πράξεις (Acar, et al. 2018).

Τα πλεονεκτήματα της SHE περιλαμβάνουν την ικανότητα να εκτελούνται σύνθετες πράξεις σε κρυπτογραφημένα δεδομένα, ενώ παράλληλα διατηρείται ένας αποδεκτός χρόνος υπολογισμού και η ευκολία χρήσης. Αυτό την καθιστά ιδανική για εφαρμογές όπου ο χρόνος και οι πόροι είναι περιορισμένοι, αλλά υπάρχει ανάγκη για περισσότερες από μία πράξεις (Acar, et al. 2018).

Ωστόσο, τα μειονεκτήματα της SHE περιλαμβάνουν την ανάγκη για τις διαδικασίες αναδιάταξης ή εκκαθάρισης μετά από έναν καθορισμένο αριθμό πράξεων. Αυτό μπορεί να προκαλέσει καθυστερήσεις και μπορεί να είναι υπολογιστικά δαπανηρό, καθιστώντας το σύστημα λιγότερο αποδοτικό για εφαρμογές που απαιτούν συνεχείς πράξεις. Πιο συγκεκριμένα σύμφωνα με την εργασία (Acar, et al. 2018):

- Στη διαδικασία αναδιάταξης, στόχος είναι η μείωση του μεγέθους των κρυπτογραφημένων δεδομένων μετά την εφαρμογή ορισμένων πράξεων, όπως ο πολλαπλασιασμός. Οι πράξεις αυτές μπορεί να αυξάνουν το μέγεθος του κρυπτογράφηματος, το οποίο σε τελική ανάλυση μπορεί να επηρεάσει την απόδοση των υπολογισμών. Μέσω της αναδιάταξης, το

κρυπτογράφημα «συμπιέζεται», επανερχόμενο πλήρως ή κατά προσέγγιση σε ένα πιο διαχειρίσιμο και αποδεκτό μέγεθος, περίπου ίσο με το αρχικό.

- Στη διαδικασία εκκαθάρισης, στόχος είναι η "ανανέωση" ενός κρυπτογραφήματος, μειώνοντας τον θόρυβο που προστίθεται κατά την εκτέλεση πράξεων στα κρυπτογραφημένα δεδομένα. Σε συστήματα όπως τα ομομορφικά συστήματα κρυπτογραφίας, ο θόρυβος αυξάνεται με κάθε πράξη και μετά από έναν ορισμένο αριθμό πράξεων, το κρυπτογράφημα μπορεί να γίνει αδύνατον να αποκρυπτογραφηθεί σωστά. Η εκκαθάριση επαναφέρει το κρυπτογράφημα σε μια κατάσταση όπου ο θόρυβος είναι ελεγχόμενος, επιτρέποντας περισσότερες πράξεις να εκτελεστούν πριν το κρυπτογράφημα καταστεί άχρηστο.

Αξίζει να σημειωθεί ότι οι διαδικασίες αναδιάταξης (relinearization) και εκκαθάρισης (bootstrapping) διαδραματίζουν σημαντικό ρόλο, αλλά δεν είναι πάντα απαραίτητο να εφαρμόζονται και οι δύο σε κάθε περίπτωση χρήσης (Acar, et al. 2018).

Παρακάτω ακολουθούν οι δημοφιλέστεροι ομομορφικοί αλγόριθμοι της SHE:

Ο αλγόριθμος NTRU

- Εισήχθη το 1996 από τους Jeffrey Hoffstein, Jill Pipher και Joseph H. Silverman.
- **Καινοτομία:** διαφέρει στο θεμέλιό του, βασίζεται στη θεωρία των δακτυλίων, συγκεκριμένα στην κρυπτογραφία βασισμένη σε πλέγματα, αντί για τη θεωρία των αριθμών που υποστηρίζει πολλά άλλα κρυπτοσυστήματα. Αυτή η διαφορά του δίνει πιθανές πλεονεκτήματα σε πλαίσια κρυπτογραφίας μετά τα κβαντικά, καθώς πολλοί ερευνητές πιστεύουν ότι τα συστήματα βασισμένα σε πλέγματα θα μπορούσαν να είναι πιο ανθεκτικά σε κβαντικές επιθέσεις.
- **Ομομορφική Ιδιότητα:** Παρόλο που το NTRU δεν κατατάσσεται πάντα ρητά ως SHE, διαθέτει εγγενείς ιδιότητες που υποστηρίζουν ορισμένες ομομορφικές λειτουργίες. Το κρυπτοσύστημα μπορεί να εκτελεί πολλαπλασιασμό πολυωνύμων σε κρυπτογραφημένα δεδομένα.

Ο αλγόριθμος BGN

- Εισήχθη το 2005 από τους Dan Boneh, Eu-Jin Goh και Kobbi Nissim.
- **Καινοτομία:** Το κρυπτοσύστημα BGN ήταν σημαντικό γιατί ήταν ένα από τα πρώτα συστήματα που υποστήριξε και προσθετικές και πολλαπλασιαστικές ομομορφικές λειτουργίες, αν και με τον περιορισμό μιας μόνο πολλαπλασιαστικής πράξης. Λειτουργεί ως γέφυρα μεταξύ των μερικώς και πλήρως ομομορφικών συστημάτων.
- **Ομομορφική Ιδιότητα:** Το BGN επιτρέπει απεριόριστες προσθήκες και μια πολλαπλασιαστική λειτουργία σε κρυπτογραφημένα δεδομένα, σημειώνοντας σημαντική πρόοδο αναφορικά με τις δυνατότητες σε σχέση με προγενέστερα συστήματα PHE.

Ο αλγόριθμος DGHV

- Εισήχθη γύρω στο 2010 από τους Marten van Dijk, Craig Gentry, Shai Halevi και Vinod Vaikuntanathan.

- **Καινοτομία:** Το σύστημα DGHV είναι γνωστό για την απλότητά του και την ασφάλειά του βασισμένη στο πρόβλημα του κατά-προσέγγιση-GCD. Αυτό το σύστημα βασίζεται σε προηγούμενη εργασία του Gentry για το bootstrapping, αλλά λειτουργεί χωρίς την κωδικοποίηση πρόσθετης δομής στα κρυπτογραφημένα.

- **Ομομορφική Ιδιότητα:** Το DGHV, όπως το BGN, μπορεί να χειριστεί ορισμένες πολυωνυμικές πραξεις σε κρυπτογραφημένα δεδομένα, επεκτείνοντας περαιτέρω τις δυνατότητες της PHE προς την κατεύθυνση της FHE.

Ο αλγόριθμος LTV

- Εισήχθη από τους Adriana Lopez-Alt, Eran Tromer, και Vinod Vaikuntanathan

- **Καινοτομία:** Το σχήμα LTV προσαρμόζει την προσέγγιση DGHV, εισάγοντας βελτιστοποιήσεις που καθιστούν το σύστημα πιο αποδοτικό και μειώνοντας τον θόρυβο ταχύτερα, ένα κρίσιμο ζήτημα στα ομομορφικά σχήματα κρυπτογράφησης.

- **Ομομορφική Ιδιότητα:** Το σχήμα LTV υποστηρίζει διάφορες ομομορφικές λειτουργίες, βελτιώνοντας τις δυνατότητες του DGHV ενώ διαχειρίζεται την αύξηση του θορύβου στα κρυπτογραφημένα δεδομένα πιο αποτελεσματικά.

4.5.3 Πλήρως ομομορφική κρυπτογραφία (FHE)

Το κύριο χαρακτηριστικό της FHE είναι η απόλυτη ομομορφία, δηλαδή η ικανότητα να υποστηρίζει έναν απεριόριστο αριθμό πράξεων, τόσο προσθέσεων όσο και πολλαπλασιασμών, πάνω σε κρυπτογραφημένα δεδομένα. Αυτό την καθιστά ιδανική για πολλές εφαρμογές, όπως η στατιστική ανάλυση, η εκτέλεση πολύπλοκων αλγορίθμων και πολλές άλλες εργασίες σε ευαίσθητα δεδομένα χωρίς να χρειάζεται αποκάλυψη της πραγματικής τους τιμής (Armknecht, et al. 2015).

Σε σύγκριση με τις SHE και PHE, η FHE προσφέρει απόλυτη ευελιξία στην εκτέλεση πράξεων, επιτρέποντας την εκτέλεση πολύπλοκων αλγορίθμων χωρίς την ανάγκη για αποκρυπτογράφηση (Armknecht, et al. 2015).

Ωστόσο, η FHE έρχεται με ορισμένα μειονεκτήματα. Είναι υπολογιστικά πιο δαπανηρή από τα άλλα δύο συστήματα, καθιστώντας τη λιγότερο αποδοτική για εφαρμογές που απαιτούν άμεση ανταπόκριση ή ότραν είναι διαθέσιμοι περιορισμένοι υπολογιστικοί πόροι. Επιπλέον, η υλοποίηση της FHE σε πραγματικές εφαρμογές μπορεί να είναι πολύπλοκη, απαιτώντας εξειδικευμένες γνώσεις και δεξιότητες (Armknecht, et al. 2015).

Εν κατακλείδι, η FHE προσφέρει υψηλά επίπεδα ευελιξίας και προστασίας δεδομένων, αλλά η υλοποίηση και το υπολογιστικό κόστος που συνεπάγεται η χρήση της μπορεί να την καθιστούν δύσκολο να εφαρμοστεί σε ορισμένες εφαρμογές/περιπτώσεις.

Παρακάτω ακολουθούν οι δημοφιλέστεροι ομομορφικοί αλγόριθμοι της FHE, συνοψίζοντας την ανάλυση της εργασίας (Armknecht, et al. 2015):

Ο Αυξητικός Κρυπταλγόριθμος του Gentry

- Εισήχθη το 2009 από τον Craig Gentry.
- **Καινοτομία:** Η εργασία του Craig Gentry το 2009 εισήγαγε καινοτομίες στον τομέα της κρυπτογραφίας, με κυριότερη εξ αυτών το concept του «bootstrapping», μια τεχνική για την ανανέωση των κρυπτοκειμένων και τη μείωση του θορύβου, επιτρέποντας έναν απεριόριστο αριθμό ομομορφικών λειτουργιών. Η αρχική δομή βασίστηκε σε πλέγματα, και αποτέλεσε την πρώτη πρακτική προσέγγιση για την επίτευξη του FHE.
- **Ομομορφική Ιδιότητα:** Η τεχνική του bootstrapping επέτρεψε τόσο τις προσθετικές όσο και τις πολλαπλασιαστικές λειτουργίες στα κρυπτοκείμενα, κορυφώνοντας σε ένα πλήρως ομομορφικό σύστημα κρυπτογράφησης.

Ο αλγόριθμος BV

- Εισήχθη το 2011 από τους Zvika Brakerski και Vinod Vaikuntanathan.
- **Καινοτομία:** Οι Brakerski και Vaikuntanathan απλοποίησαν τη δομή FHE του Gentry. Η σημαντικότερη συνεισφορά τους ήταν η εισαγωγή του «επιπέδου» FHE, που επιτρέπει υπολογισμούς περιορισμένου βάθους χωρίς την ανάγκη για bootstrapping, αυξάνοντας έτσι την αποδοτικότητα.
- **Ομομορφική Ιδιότητα:** Το σχήμα BV διατηρεί τις ιδιότητες της πλήρους ομομορφίας, επιτρέποντας τόσο τις προσθετικές όσο και τις πολλαπλασιαστικές λειτουργίες στα κρυπτοκείμενα.

Ο αλγόριθμος BGV

- Εισήχθη το 2011-2012 από τους Zvika Brakerski και Vinod Vaikuntanathan.
- **Καινοτομία:** Το σχήμα BGV είναι μια επέκταση του σχήματος BV. Είναι ιδιαίτερα σημαντικό για την ικανότητά του να χειρίζεται εφαρμογές πλήρους αλλά και σχετικώς ομομορφικής κρυπτογραφίας. Αυτή η προσαρμοστικότητα σημαίνει ότι ο αλγόριθμος BGV μπορεί να βελτιστοποιηθεί για αποδοτικότητα με βάση το συγκεκριμένο υπολογιστικό έργο που εκτελείται.
- **Ομομορφική Ιδιότητα:** Όπως και τα προηγούμενα σχήματα FHE, το σχήμα BGV υποστηρίζει έναν απεριόριστο αριθμό προσθετικών και πολλαπλασιαστικών λειτουργιών σε κρυπτοκείμενα, εφόσον επιλεγούν κατάλληλες παράμετροι.

Ο αλγόριθμος FV

- Εισήχθη το 2012 από τους Junfeng Fan και Frederik Vercauteren.
- **Καινοτομία:** Το σχήμα FV τελειοποίησε και βελτιστοποίησε περαιτέρω το σχήμα BGV. Διακρίνεται για την απλοποίηση των τεχνικών διαχείρισης θορύβου που χρησιμοποιούνται στα προηγούμενα σχήματα FHE, προσφέροντας αυξημένη αποδοτικότητα, ιδιαίτερα για ορισμένους τύπους υπολογισμών.

- **Ομομορφική Ιδιότητα:** Όπως και τα παραπάνω σχήματα FHE, το σχήμα FV είναι ικανό για προσθετικές και πολλαπλασιαστικές λειτουργίες στα κρυπτοκείμενα χωρίς να αποκαλύπτει τα υποκείμενα απλά κείμενα.

Ο αλγόριθμος CKKS

- Εισήχθη το 2016 από τους Joohee Cheon, Andrey Kim, Miran Kim, και Yongsoo Song.

- **Καινοτομία:** Το CKKS είναι ένα αξιοσημείωτο σχήμα FHE που σχεδιάστηκε ειδικά για προσεγγιστικούς αριθμητικούς υπολογισμούς, καθιστώντας το ιδιαίτερα κατάλληλο για ομομορφικές λειτουργίες σε πραγματικούς ή σύνθετους αριθμούς με σταθερή ακρίβεια. Λαμβάνοντας υπόψη τη συχνή χρήση της αριθμητικής κινητής υποδιαστολής σε πραγματικές εφαρμογές, ιδιαίτερα στη μηχανική μάθηση και τους επιστημονικούς υπολογισμούς, το CKKS σχεδιάστηκε για να εκτελεί λειτουργίες με ελάχιστη ενίσχυση σφάλματος. Αυτή η καινοτομία το καθιστά σημαντικό εργαλείο για εργασία σε εφαρμογές όπου μικρά σφάλματα προσέγγισης είναι αποδεκτά αλλά είναι απαραίτητο να εκτελούνται λειτουργίες σε κρυπτογραφημένους αριθμούς κινητής υποδιαστολής.

- **Ομομορφική Ιδιότητα:** Το σχήμα CKKS υποστηρίζει τόσο προσθετικές όσο και πολλαπλασιαστικές λειτουργίες σε κρυπτοκείμενα, επιτρέποντας ένα ευρύ φάσμα υπολογισμών. Ενώ δεν υποστηρίζει ακριβή αριθμητική όπως άλλα σχήματα FHE, η ικανότητά του να χειρίζεται προσεγγιστικούς υπολογισμούς σε πραγματικούς αριθμούς το καθιστά μοναδικό και με αξιοσημείωτη πρακτική χρησιμότητα σε ορισμένα σενάρια.

4.5.4 Σταθμισμένη Ομομορφική Κρυπτογραφία (LHE)

Η Σταθμισμένη Ομομορφική Κρυπτογραφία (*μτφρ. Leveled Homomorphic Encryption* - LHE) είναι μια παραλλαγή της πλήρους ομομορφικής κρυπτογράφησης (FHE). Για την κατανόηση της LHE, είναι σημαντικό να αναφερθούν πρώτα οι δυνατότητες της FHE.

Η FHE επιτρέπει αυθαίρετους υπολογισμούς σε κρυπτογραφημένα δεδομένα χωρίς αυτά να χρειάζεται να αποκρυπτογραφηθούν σε κανένα σημείο. Δηλαδή, με την FHE, μπορεί κανείς να εκτελέσει οποιονδήποτε αριθμό λειτουργιών (και προσθέσεις και πολλαπλασιασμούς) στα κρυπτογραφήματα, και κατά την αποκρυπτογράφηση, το αποτέλεσμα θα είναι το ίδιο όπως αν αυτές οι λειτουργίες εκτελέστηκαν στα απλά κείμενα. Ωστόσο, τα σχήματα FHE εισάγουν αυξανόμενο "θόρυβο" με κάθε λειτουργία. Αυτός ο θόρυβος είναι μέρος του σχήματος κρυπτογράφησης, και έχει ως στόχο τη διατήρηση του επίπεδου ασφάλειας, αλλά καθώς εκτελούνται λειτουργίες στο κρυπτογράφημα, το επίπεδο θορύβου αυξάνεται. Εάν ο θόρυβος αυξηθεί υπερβολικά, μπορεί να εμποδίσει την επιτυχημένη αποκρυπτογράφηση. Για να αντιμετωπίσουν αυτήν την αύξηση του θορύβου, τα σχήματα FHE ενσωματώνουν μια διαδικασία που ονομάζεται «bootstrapping» για να μειώσουν τον θόρυβο. Ωστόσο, το bootstrapping είναι υπολογιστικά δαπανηρό (Chillotti, et al. 2018).

Η κρυπτογράφηση επιπέδου ομομορφίας (LHE) προκύπτει ως μια πιο αποτελεσματική συμβιβαστική λύση. Με την LHE, το σύστημα ρυθμίζεται για να χειριστεί ένα συγκεκριμένο «επίπεδο» ή «βάθος» λειτουργιών χωρίς την ανάγκη για bootstrapping. Αυτό το βάθος ορίζεται εκ των προτέρων. Για παράδειγμα, ένα σχήμα LHE μπορεί να ρυθμιστεί για να χειριστεί υπολογισμούς με βάθος 10 λειτουργιών (όπως 10 πολλαπλασιασμοί). Εάν γνωρίζουμε εκ των προτέρων ότι οι υπολογισμοί δεν

θα υπερβούν αυτό το μέγεθος, τότε το LHE μπορεί να είναι πολύ πιο γρήγορο και αποτελεσματικό από τη γενική FHE, καθώς αποφεύγει το δαπανηρό βήμα του bootstrapping (Chillotti, et al. 2018).

Στη συνέχεια συνοψίζονται οι δημοφιλέστεροι ομομορφικοί αλγόριθμοι της LHE, όπως αυτοί καταγράφονται στην εργασία (Chillotti, et al. 2018):

Το Σχέδιο του Gentry

- Εισήχθη το 2009 από τον Craig Gentry.
- **Καινοτομία:** Η εργασία του Craig Gentry εισήγαγε την έννοια της πλήρως ομομορφικής κρυπτογράφησης. Η καινοτόμος ιδέα ήταν το «bootstrapping», μια τεχνική για τη μείωση του θορύβου που σχετίζεται με κάθε λειτουργία, επιτρέποντας έτσι έναν αυθαίρετο αριθμό υπολογισμών σε κρυπτογραφημένα δεδομένα.
- **Ομομορφική Ιδιότητα:** Το σχέδιο του Gentry, μέσω του bootstrapping, υποστηρίζει και τις δύο πράξεις πρόσθεσης και πολλαπλασιασμού σε κρυπτογραφημένα δεδομένα.

Ο αλγόριθμος BGV

- Εισήχθη το 2011 από τους Zvika Brakerski και Vinod Vaikuntanathan.
- **Καινοτομία:** Ο αλγόριθμος BGV βελτιώνει την αρχική κατασκευή του Gentry. Υποστηρίζει σταθμισμένη ομομορφική κρυπτογράφηση χωρίς bootstrapping, επιτρέποντας την εκτέλεση λειτουργιών σε κρυπτογραφήματα διαφορετικών «επιπέδων» και επίσης εισήγαγε μια τεχνική για την αλλαγή των παραμέτρων κρυπτογράφησης κατά τη διάρκεια του υπολογισμού.
- **Ομομορφική Ιδιότητα:** Το BGV υποστηρίζει τόσο σταθμισμένη όσο και πλήρη ομομορφική κρυπτογράφηση, επιτρέποντας τόσο τις πράξεις πρόσθεσης όσο και πολλαπλασιασμού.

Ο αλγόριθμος BFV

- Εισήχθη το 2012 από τους Zvika Brakerski και Vinod Vaikuntanathan.
- **Καινοτομία:** Ο αλγόριθμος BFV είναι μια απλούστευση του αλγορίθμου BGV. Παραλείπει κάποια χαρακτηριστικά του BGV για να επιτύχει ταχύτερη απόδοση και λιγότερο υπολογιστικό φόρτο σε πολλές περιπτώσεις.
- **Ομομορφική Ιδιότητα:** Το BFV προσφέρει αποδοτική ομομορφική κρυπτογράφηση, βελτιστοποιημένη για ορισμένους τύπους εφαρμογών.

Ο αλγόριθμος GSW

- Εισήχθη το 2013 από τους Craig Gentry, Amit Sahai και Brent Waters.
- **Καινοτομία:** Ο αλγόριθμος GSW εισήγαγε μια νέα τεχνική κωδικοποίησης για τα κρυπτογραφήματα, χρησιμοποιώντας πίνακες, επιτρέποντας πιο απλό και αποδοτικό ομομορφικό πολλαπλασιασμό.

- **Ομομορφική Ιδιότητα:** Ενώ το GSW μπορεί να θεωρηθεί ως άλλο ένα σχέδιο πλήρους ομομορφικής κρυπτογράφησης, οι καινοτομίες του βασίζονται κυρίως στην κωδικοποίηση και στις αποδοτικές πράξεις πολλαπλασιασμού.

Ο αλγόριθμος YASHE (Yet Another Somewhat Homomorphic Encryption)

- Εισήχθη στις αρχές του 2010 από τους Damien Stehlé και Ron Steinfeld.
- **Καινοτομία:** Το YASHE επικεντρώνεται στην αποδοτικότητα χρησιμοποιώντας συγκεκριμένους τύπους πολυωνυμικών δακτυλίων. Αυτό το σχέδιο έχει βρει εφαρμογές όπου απαιτούνται αποδοτικές, σταθμισμένες («leveled») ομομορφικές λειτουργίες χωρίς πλήρες bootstrapping.
- **Ομομορφική Ιδιότητα:** Το YASHE προσφέρει ικανότητα πράξεων πρόσθεσης και πολλαπλασιασμού σε μία σειρά "επιπέδων" κρυπτογραφημάτων.

5 Η Τεχνολογία Blockchain

Στην παρούσα ενότητα συνοψίζεται η τεχνολογία Blockchain, παρουσιάζοντας τις βασικές έννοιες, τα χαρακτηριστικά της, τους διαφορετικούς τύπους blockchain, αλλά και εφαρμογές της τεχνολογίας όπως τα έξυπνα συμβόλαια.

5.1 Βασικές έννοιες

Κρυπτονόμισμα (*μτφρ. Cryptocurrency*): ονομάζεται κάθε ψηφιακό νόμισμα το οποίο ενσωματώνει μεθόδους κρυπτογράφησης για τη διασφάλιση των πληροφοριών μεταξύ συναλλασσόμενων πλευρών. Όπως και με το φυσικό χρήμα, έτσι και τα κρυπτονομίσματα διέπονται από μεταξύ τους ισοτιμίες, ενώ τα δημοφιλέστερα ή/και ισχυρότερα εξ αυτών διαθέτουν ισοτιμία και έναντι φυσικών νομισμάτων. Ως κρυπτονομίσματα θεωρούνται και οι ψηφιακές μάρκες (*μτφρ.* tokens), οι οποίες αν και μπορούν να ανταλλαχθούν με άλλα νομίσματα, βρίσκουν χρήση κυρίως εντός κλειστών, ιδιωτικών δικτύων. Σε όλες τις περιπτώσεις, τα κρυπτονομίσματα θεωρούνται κεφάλαιο ή περιουσιακό στοιχείο (asset), διότι έχουν αξία και για τη δημιουργία τους έχουν δαπανηθεί πόροι. Η υποδομή που απαιτείται για τη δημιουργία κρυπτονομισμάτων, και ακολούθως για τη διακίνησή τους, βασίζεται στην τεχνολογία Blockchain (Komalavalli, Saxena and Laroiya 2020).

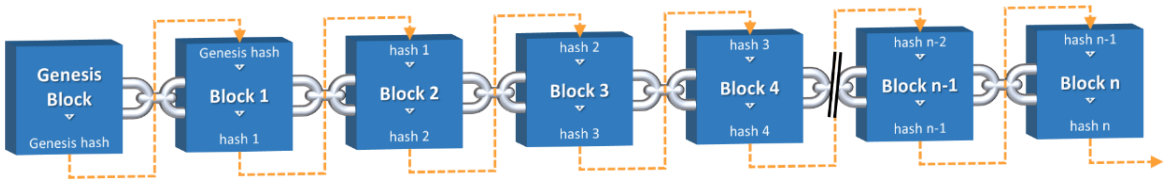
Συναλλαγή (*Transaction*): ονομάζεται κάθε δραστηριότητα μεταξύ δύο ή περισσότερων μερών, όπου λαμβάνει χώρα η ανταλλαγή αγαθών ή/και υπηρεσιών, συνήθως έναντι χρηματικού αντιτίμου ή κάποιας άλλης αξίας. Στον ψηφιακό κόσμο, και πιο συγκεκριμένα σε περιβάλλοντα Blockchain, οι συναλλαγές μπορούν να αφορούν ψηφιακές πληροφορίες χωρίς απαραίτητα να αντιστοιχούν σε κάποια νομισματική αξία (Komalavalli, Saxena and Laroiya 2020).

Κατακερματισμός (*μτφρ. Hashing*)**:** ονομάζεται η διαδικασία παραγωγής μιας συμβολοσειράς συγκεκριμένου μήκους (hash) που προκύπτει από υπολογιστικές κρυπτογραφικές συναρτήσεις οι οποίες χρειάζεται να λάβουν στην είσοδό τους ένα σύνολο δεδομένων. Η διαφοροποίηση στα δεδομένα εισόδου, έχει ως αποτέλεσμα μία διαφορετική έξοδο, ενώ είναι επιθυμητό μικρές "τοπικές" διαφοροποιήσεις στα δεδομένα να οδηγούν σε εκτεταμένες καθολικές διαφοροποιήσεις στο αποτέλεσμα, προκειμένου να μειώνεται η ικανότητα κρυπτανάλυσης. Η τεχνολογία Blockchain αξιοποιεί τέτοιες συναρτήσεις για την ασφαλή αποθήκευση και την επαλήθευση των δεδομένων. Το παραγόμενο hash συνοδεύει τα δεδομένα από τα οποία προέκυψε και μπορεί να χαρακτηριστεί ως το «δακτυλικό αποτύπωμά» τους (Komalavalli, Saxena and Laroiya 2020).

Μπλοκ (*μτφρ. Block*)**:** στην τεχνολογία Blockchain, έτσι ονομάζεται ένα σύνολο ομαδοποιημένων δεδομένων που αποθηκεύονται εντός δικτύου Blockchain. Κάθε block απαρτίζεται από τα δεδομένα που προορίζονται προς αποθήκευση, το hash του, το hash του προηγούμενου block και από χρονοσήμανση (Komalavalli, Saxena and Laroiya 2020).

Blockchain (*μτφρ. Αλυσίδα των Μπλοκ* ή *Αλυσίδα Συστοιχιών*)**:** ονομάζεται η τεχνολογία που λειτουργεί ως ένα ψηφιακό κατανεμημένο καθολικό στο οποίο καταχωρούνται χρονοσημασμένα δεδομένα συναλλαγών, σε μορφή ομαδοποιημένων πακέτων, μη δυνάμενων να τροποποιηθούν ως προς το περιεχόμενο ή την ιστορικότητά τους. Η αλληλουχία των blocks σχηματίζει αλυσίδα με το κάθε block να περιέχει το hash του προηγούμενου ενώ ταυτόχρονα «δίνει» το δικό του ως σημείο αγκύρωσης (anchoring) για το επόμενο. Με αυτόν τον τρόπο, δημιουργείται μια αλυσίδα από blocks, όπου το κάθε ένα αποτελεί κρίκο της αλυσίδας αυτής (Komalavalli, Saxena and Laroiya 2020) (**Εικόνα 5.1**).

Genesis Block: ονομάζεται το πρώτο θεμέλιο block κάθε Αλυσίδας, το οποίο είναι το μοναδικό που δεν διαθέτει εκ των πραγμάτων το hash του προηγούμενου (Komalavalli, Saxena and Laroiya 2020).



Εικόνα 5.1: *Γραφική αναπαράσταση Αλυσίδας Μπλοκ*

Κόμβος (*μτφρ. Node*): κόμβος, σε ένα περιβάλλον Blockchain, ονομάζεται κάθε μοναδική φυσική ή εικονική συσκευή η οποία είναι συνδεδεμένη στο κατανεμημένο δίκτυο ως σημείο επικοινωνίας, εκτελεί διάφορες λειτουργίες (π.χ. εξόρυξη, επικύρωση, κ.λπ.) και διατηρεί αποθηκευμένο ένα ενημερωμένο αντίγραφο της Αλυσίδας (Komalavalli, Saxena and Laroiya 2020).

Μηχανισμός Συναίνεσης (*μτφρ. Consensus Mechanism*)**:** ονομάζεται ο αλγοριθμικός μηχανισμός που διασφαλίζει τη διαδικασία επικύρωσης των δεδομένων εντός ενός δικτύου Blockchain. Οι Μηχανισμοί Συναίνεσης αξιοποιούνται από τα περιβάλλοντα Blockchain για την επίτευξη της απαραίτητης πλειοψηφίας για μία μοναδική τιμή δεδομένων, η οποία είναι το hash (Komalavalli, Saxena and Laroiya 2020).

Έξυπνο Συμβόλαιο ή **Έξυπνη Σύμβαση** (*μτφρ. Smart Contract*)**:** ονομάζεται ένα σύνολο προϋποθέσεων μεταφρασμένο σε κώδικα ηλεκτρονικού υπολογιστή, το οποίο αποδίδει αυτομάτως ένα προκαθορισμένο αποτέλεσμα όταν πληρούνται όλοι οι όροι και προϋποθέσεις του (Komalavalli, Saxena and Laroiya 2020).

5.2 Το τρίπτυχο χαρακτηριστικών της Τεχνολογίας Blockchain

Το blockchain καλύπτει κενά στον τομέα της εμπιστοσύνης αναφορικά με τα δεδομένα (Warkentin & Orgeron, 2020). Η εμπιστοσύνη ανέκαθεν αντιμετώπιζε εμπόδια, και αυτό διότι μεταξύ δύο ή περισσότερων πλευρών που επιθυμούν να συνδιαλλαγούν μεταξύ τους, η κάθε μία αποζητά εμφανώς ή αφανώς την εξασφάλιση πώς καθόλη τη διάρκεια της διαδικασίας δεν θα προκύψουν λάθη ή απόπειρες εξαπάτησης. Από τις πρώτες ακόμα εμπορικές συναλλαγές, οι εμπλεκόμενοι ήταν αναγκασμένοι να δείχνουν καλή πίστη, ωστόσο δεν αποδεικνύονται όλοι οι συναλλασσόμενοι αντάξιοι της εμπιστοσύνης, αλλά είναι δυνατόν να υπάρξουν και προστριβές λόγω παρανοήσεων. Αυτό το κενό ήρθαν να καλύψουν οι ουδέτεροι και έμπιστοι ενδιάμεσοι, οι οποίοι είχαν ρόλο εγγυητή των συναλλαγών. Στην αρχαιότητα τον ρόλο αυτόν διαδραμάτισαν οι ναοί και άλλοι λατρευτικοί χώροι. Στα νεότερα χρόνια, είτε κρατικές δομές όπως τα υποθηκοφυλακεία, είτε πιστοποιημένοι τρίτοι (π.χ. συμβολαιογράφοι) είτε το τραπεζικό σύστημα επιτελούν τον ρόλο ενός αμερόληπτου φορέα κοινής εμπιστοσύνης μεταξύ συναλλασσόμενων πλευρών, με τον ρόλο των τραπεζών να ενισχύεται. Αν και οι τράπεζες δεν συμμετέχουν σε όλες τις μικρές καθημερινές συναλλαγές, είναι παρούσες σε συγκεκριμένες κατηγορίες αυτών, κυρίως όπου απαιτείται διασφάλιση μεταξύ συναλλασσόμενων. Ωστόσο, παρόλη την ασφάλεια που παρέχεται από το τραπεζικό σύστημα, συντρέχουν παράλληλα δύο αξιοσημείωτα ζητήματα (Warkentin and Orgeron 2020):

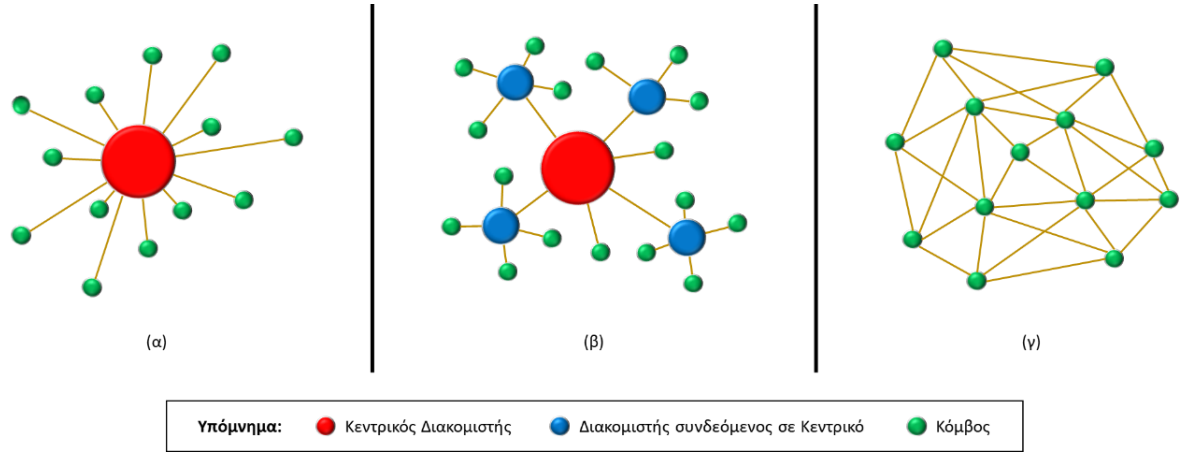
1. οι καταναλωτές επιβαρύνονται με επιπρόσθετα κόστη επί των συναλλαγών, τα οποία έχουν τη μορφή τραπεζικών προμηθειών

2. ο χρόνος εκτέλεσης των περισσότερων συναλλαγών δεν είναι άμεσος, εκτός εάν καταβληθεί μεγαλύτερη τραπεζική προμήθεια.

Σε όλες τις περιπτώσεις, τα τραπεζικά ιδρύματα διατηρούν ένα συγκεντρωτικό προφίλ, με απώτερο στόχο τη μεγιστοποίηση των κερδών με διάφορα μέσα, ένα εκ των οποίων είναι οι προμήθειες, οι τοκοφόρες ημερομηνίες (valeur), κ.λπ. Στον αντίποδα, η τεχνολογία Blockchain λειτουργεί με αποκεντρωμένο τρόπο, με το "δόγμα" της να χαρακτηρίζεται από το τρίπτυχο:

Αποκέντρωση - Αμεταβλητότητα - Ιχνηλασιμότητα

Αποκέντρωση (*μτφρ. Decentralization*) είναι η μεταφορά αρμοδιοτήτων, εξουσιών διαδικασιών ή δραστηριοτήτων, από μία κεντρική αρχή σε περισσότερες περιφερειακές της. Στην τεχνολογία Blockchain, η αποκέντρωση μπορεί να είναι πλήρης, με όλους τους συμμετέχοντες να είναι ισότιμοι. Παρομοιάζοντάς το με ένα παράδειγμα από τον φυσικό κόσμο, το Blockchain μπορεί να παραλληλιστεί με ένα αρχείο καταγραφών όπως ένα λογιστικό βιβλίο (καθολικό, *μτφρ.* ledger) το οποίο είναι διαμοιρασμένο (κατανεμημένο, *μτφρ. distributed*) και διαρκώς ενημερωμένο για όλους όσους συμμετέχουν σε αυτό. Το Blockchain ανήκει στις τεχνολογίες κατανεμημένων υπολογιστικών συστημάτων, και συγκαταλέγεται στις Τεχνολογίες Κατανεμημένου Καθολικού (*μτφρ*. Distributed Ledger Technology - DLT) (Warkentin and Orgeron 2020) (**Εικόνα 5.2**).



Εικόνα 5.2: *Συγκεντρωτικό Σύστημα (α), Αποκεντρωμένο Σύστημα (β), Κατανεμημένο Σύστημα (γ)*

Αμεταβλητότητα (*μτφρ. Immutability*) είναι το χαρακτηριστικό της τεχνολογίας Blockchain όπου τα δεδομένα που εγγράφονται σε μία Αλυσίδα, δεν δύνανται να τροποποιηθούν. Μόλις ολοκληρωθεί μια συναλλαγή εντός δικτύου Blockchain, δεν μπορεί να ανακληθεί παρά μόνο με τη δημιουργία μίας νέας. Εάν, φερ' ειπείν, σε μία μεταφορά χρημάτων αποσταλεί από λάθος στον παραλήπτη μεγαλύτερο χρηματικό ποσόν από το προσυμφωνημένο, τότε ο μόνος τρόπος για να αποκατασταθεί αυτό το σφάλμα είναι να δημιουργηθεί μια νέα συναλλαγή, με κατεύθυνση από τον παραλήπτη προς τον αρχικό αποστολέα, όπου θα πραγματοποιείται επιστροφή του υπερβάλλοντος ποσού. Σε αυτό συνεισφέρει η αποκεντρωμένη δομή της τεχνολογίας Blockchain η οποία της παρέχει ισχυρή ανθεκτικότητα ενάντια σε απόπειρες αλλοίωσης των δεδομένων των συναλλαγών, όπως για παράδειγμα μέσω μηχανισμών αποκατάστασης. Ως ένα τυπικό παράδειγμα από τον φυσικό κόσμο, ας θεωρήσουμε μία συναλλαγή στην οποία συμμετέχουν δύο συναλλασσόμενοι, καθώς και ένας τρίτος που έχει ρυθμιστικό ρόλο. Για την εν λόγω συναλλαγή εκδίδεται τριπλότυπη απόδειξη και

κάθε ένας από τους συμμετέχοντες λαμβάνει από ένα αντίτυπο. Στο υποθετικό σενάριο όπου ένας από τους τρεις αλλοιώσει/παραχαράξει το αντίτυπό του, τότε αυτό αντιπαραβάλλεται άμεσα με τα υπόλοιπα δύο όπου διαπιστώνεται η ακυρότητά του. Στον ψηφιακό κόσμο, ένα δίκτυο Blockchain μπορεί να αντικαθιστά τα μη-έγκυρα δεδομένα που προκύπτουν με έγκυρα αντίγραφα. Εδώ, γίνεται επίσης αντιληπτή η δημοκρατικότητα που διέπει τα δίκτυα Blockchain, καθώς αξιοποιείται η δύναμη της πλειοψηφίας για τη διασφάλιση των δεδομένων. Ωστόσο, σε ακραίες περιπτώσεις, μπορεί να δημιουργηθεί μία πλειοψηφική αλλοίωση η οποία κατορθώνει να υπερισχύσει (Warkentin and Orgeron 2020).

Για την επίτευξή της θα πρέπει η αλλοίωση να πραγματοποιηθεί σχεδόν ταυτόχρονα, από την πλειοψηφία των συμμετεχόντων στην Αλυσίδα. Αυτό ονομάζεται **Επίθεση 51%** (*μτφρ. 51% Attack*). Στα πρώιμα χρόνια της τεχνολογίας Blockchain, μια τέτοια επιτυχία υπήρχε μόνο στη σφαίρα της θεωρίας διότι οι "επιτιθέμενοι" θα έπρεπε σε πολύ μικρό χρονικό διάστημα να δαπανήσουν τεράστια ποσά επεξεργαστικής ισχύος που δεν τότε δεν ήταν ρεαλιστικά. Αυτό εξακολουθεί να ισχύει, κυρίως για μεγάλα δίκτυα Blockchain, όπως αυτό του Bitcoin. Ωστόσο, το εναλλακτικό νόμισμα (*μτφρ. altcoin*) Bitcoin Gold - το οποίο αποτελεί διακλάδωση της κύριας Αλυσίδας του Bitcoin - υπέστη Επίθεση 51% τον Μάιο του 2018, με αποτέλεσμα την κλοπή κρυπτονομισμάτων τότε αξίας 18 εκατομμυρίων δολαρίων.

Ιχνηλασιμότητα (*μτφρ. Traceability*) είναι η λειτουργία κατά την οποία τα δεδομένα προς αποθήκευση, συνοδεύονται από χρονοσήμανση (*μτφρ. timestamp*). Περιέχουν επίσης επιπρόσθετα δεδομένα ιχνηλασιμότητας που αφορούν μία συναλλαγή. Έτσι, συνδυάζοντας τη χρονοσήμανση που λαμβάνουν τα δεδομένα κατά την αποθήκευσή τους σε ένα δίκτυο Blockchain με την αμεταβλητότητα που προσφέρει η τεχνολογία αυτή, δημιουργείται μια αδιάψευστη ροή συναλλαγών που κάθε μία μπορούν να ιχνηλατηθεί μέχρι και το Genesis block της Αλυσίδας (Warkentin and Orgeron 2020).

Το αποτέλεσμα του τρίπτυχου χαρακτηριστικών της τεχνολογίας Blockchain, είναι η **Διαφάνεια** (*μτφρ. Transparency*), η οποία εγκαθιδρύει για τις ψηφιακές συναλλαγές ένα καθεστώς αμοιβαίας εμπιστοσύνης μέσω αμετάβλητων και αδιαμφισβήτητων δεδομένων.

Το Bitcoin αποτέλεσε το πρώτο ψηφιακό νόμισμα με αποκεντρωμένη φιλοσοφία και υποδομή. Χαρακτηρίζεται ως κρυπτονόμισμα, καθώς για τη δημιουργία του εφαρμόζονται τεχνικές κρυπτογράφησης για τη διασφάλιση των δεδομένων των συναλλαγών καθώς και για την επαλήθευση τους εντός του δικτύου. Στην υλοποίησή του, το Bitcoin, αντιμετωπίζει αποτελεσματικά ένα πλήθος ζητημάτων που εμφανίζουν τα συμβατικά συστήματα συναλλαγών όπως πολυπλοκότητα, περιττά επιπρόσθετα κόστη που επιβαρύνουν τους συναλλασσόμενους, ψηφιακές ευπάθειες και ανεπάρκειες. Η αποκεντρωμένη λειτουργία του Bitcoin εγκαθιδρύει για το συγκεκριμένο νόμισμα ένα καθεστώς όπου δεν υπάρχει μία σταθερή οντότητα που να το διαχειρίζεται, σε αντίθεση με το «πραγματικό» χρήμα το οποίο εκδίδεται και ελέγχεται από κεντρικούς οργανισμούς (Warkentin and Orgeron 2020).

Τα παραπάνω, μεταξύ άλλων, επιτυγχάνονται μέσω της τεχνολογικής υποδομής που χρησιμοποιείται και ονομάζεται Blockchain, το οποίο φροντίζει για την τήρηση της αξιοπιστίας εντός του δικτύου. Το εν λόγω υπόβαθρο, περιλαμβάνει ένα απαραίτητο υλισμικό καθώς και ένα αλγοριθμικό πλαίσιο λειτουργίας πάνω στο οποίο "εκτελούνται" οι σχετικές υλοποιήσεις.

Το Blockchain λειτουργεί ως ένα ψηφιακό καθολικό στο οποίο αποθηκεύονται συναλλαγές διαφόρων τύπων, συνοδευόμενες από χρονοσήμανση. Αν και στην καθημερινότητα, συνηθίζουμε να θεωρούμε ως "συναλλαγή" τη δραστηριότητα όπου δύο ή περισσότερα μέρη συμφωνούν στην ανταλλαγή αγαθών ή/και υπηρεσιών, συνήθως έναντι χρηματικού αντιτίμου (είτε παραστατικού είτε ψηφιακού), είναι σημαντικό να θυμόμαστε ότι στον ψηφιακό κόσμο, και κυρίως στο Blockchain, μια συναλλαγή αναφέρεται σε οποιαδήποτε δοσοληψία ψηφιακών δεδομένων η οποία λαμβάνει χώρα εντός του δικτύου, πληρώντας τις προκαθορισμένες προϋποθέσεις του. Τα δεδομένα αυτά μπορούν να αφορούν όχι μόνο αξίες αλλά και οποιοδήποτε άλλο είδος πληροφορίας (Warkentin and Orgeron 2020).

5.3 Κατηγορίες/τύποι Blockchain

Ανάλογα με την έκταση τους και τον τρόπο πρόσβασης σε αυτές, οι Αλυσίδες Block κατηγοριοποιούνται με τρόπο παρόμοιο με εκείνον των τυπικών πληροφοριακών δικτύων (LAN, WAN, κ.λπ.). Πιο συγκεκριμένα:

Public Blockchains (*Δημόσιες Αλυσίδες Blockchain*): Πρόκειται για αλυσίδες χωρίς ιδιοκτήτη. Κάθε χρήστης διαθέτει δικαιώματα ανάγνωσης (read) και εγγραφής (write), καθώς και να συμμετάσχει στις διαδικασίες συναίνεσης των δεδομένων τους, χωρίς να χρειάζεται κάποιου είδους άδεια για οποιαδήποτε από τις ανωτέρω ενέργειες. Ως εκ τούτου, οι συγκεκριμένες Αλυσίδες χαρακτηρίζονται και ως *Permissionless Blockchains* και χαρακτηριστικό παράδειγμα χρήσης τους αφορά τα κρυπτονομίσματα. Ενδεικτικά, το Bitcoin και το Ethereum αποτελούν τα δύο δημοφιλέστερα κρυπτονομίσματα, τα οποία βασίζονται σε δημόσιους καταλόγους Blockchain (Filatovas, et al. 2022).

Private Blockchains (*Ιδιωτικές Αλυσίδες Blockchain*): Σε αντίθεση με τις δημόσιες, οι ιδιωτικές αλυσίδες δεν είναι προσβάσιμες από το ευρύ κοινό καθώς ανήκουν σε έναν και μοναδικό κάτοχο (οργανισμό ή πρόσωπο) ο οποίος καθορίζει και τα δικαιώματα όλων των συμμετεχόντων (πρόσβαση, ανάγνωση, εγγραφή, κ.λπ.). Η πρόσβαση σε μία ιδιωτική αλυσίδα είναι αντίστοιχη με αυτή ενός τοπικού δικτύου υπολογιστών (LAN), όπου η πρόσβαση είναι εφικτή μόνο για συγκεκριμένους συμμετέχοντες. Οι χρήστες αυτοί μπορεί να αποτελούν μια ή περισσότερες έμπιστες ομάδες, αναγνωρίσιμες και αποδεκτές από το δίκτυο, ακόμα και αν μεταξύ τους διαθέτουν διαφορετικά δικαιώματα πρόσβασης (access rights). Για τον λόγο αυτό, οι συγκεκριμένες αλυσίδες χαρακτηρίζονται ως *Permissioned Blockchains*. Οι ιδιωτικές αλυσίδες χρησιμοποιούνται ιδιαίτερα από οντότητες που ενδιαφέρονται για τη διασφάλιση των εσωτερικών τους διεργασιών και των διακινούμενων δεδομένων, παραδείγματος χάριν για παραγγελιοληψίες, ή έκδοση διαφόρων εγγράφων όπως δελτία παραλαβής, ελέγχου και παραστατικών. Καθώς η χρήση τους περιορίζεται στους κλειστούς κόλπους μιας οντότητας, οι αλυσίδες αυτές δεν είναι πλήρως αποκεντρωμένες αλυσίδες, ωστόσο κατορθώνουν να είναι αρκετά ταχύτερες συγκριτικά με τις δημόσιες. Τρία από τα πιο δημοφιλή Private Blockchains είναι το Hyperledger Fabric, το Hyperledger Sawtooth, και το Corda (Filatovas, et al. 2022).

Hybrid Blockchains (*Υβριδικές Αλυσίδες Blockchain*): Οι υβριδικές αρχιτεκτονικές Blockchain απαρτίζονται από ένα ιδιωτικό και ένα δημόσιο τμήμα, συνδυάζοντας τα προτερήματά τους και με σκοπό να επιτύχουν διαλειτουργικότητα και αποτελεσματικότερη συνεργασία μεταξύ οντοτήτων. Ένας δημόσιος χρήστης μπορεί να συμμετέχει δημιουργώντας και προσφέροντας blocks δεδομένων στο δίκτυο της αλυσίδας, παραμένοντας ανώνυμος. Η ταυτότητά του δύναται να γνωστοποιηθεί μόνο

σε χρήστες με τους οποίους συναλλάσσεται. Ένας οργανισμός μπορεί να βασιστεί σε μια υβριδική λύση Blockchain για τη διασφάλιση των διαδικασιών του, συλλέγοντας δεδομένα από διάφορες πηγές (δυνητικά ετερογενείς), είτε αυτές ανήκουν στο κλειστό (ιδιωτικό) τμήμα του δικτύου είτε πρόκειται για δημόσιους συνεισφέροντες. Εν συνεχεία, μπορεί να γνωστοποιεί είτε δημόσια είτε σε επιλεγμένες ομάδες συμμετεχόντων εντός του κλειστού δικτύου, τόσο τα ίδια δεδομένα όσο και πληροφορίες-παράγωγα που προκύπτουν από την επεξεργασία τους. Προς διασφάλιση όλων τα σταδίων της ανωτέρω διαδικασίας, οι εκάστοτε οργανισμοί εφαρμόζουν πρακτικές KYC (Know Your Customer). Ίσως η κυριότερη κατηγορία οργανισμών που εφαρμόζουν πρακτικές KYC είναι τα χρηματοπιστωτικά ιδρύματα διότι, για λόγους ασφάλειας και διαφάνειας, δεν δύναται να επιτρέψουν συναλλαγές εντός του περιβάλλοντος από χρήστες που δεν είναι ταυτοποιημένοι σε αυτό. Δύο γνωστές υβριδικές πλατφόρμες Blockchain είναι το Dragonchain και το LTO Network (Filatovas, et al. 2022).

Consortium ή Federated Blockchains (*Κοινοπρακτικές Αλυσίδες Blockchain*): Πρόκειται για υβριδικές αλυσίδες, η διαχείριση των οποίων πραγματοποιείται όχι από μία οντότητα αλλά από μία ομάδα οντοτήτων. Είναι μερικώς αποκεντρωμένες και ρόλος τους είναι να διευκολύνουν τη συνεργασία μεταξύ οργανισμών προσφέροντας διαλειτουργικότητα μέσω ενός κοινού περιβάλλοντος που χαίρει αναγνωρισιμότητας και εμπιστοσύνης από όλους τους συμμετέχοντες. Ενδεικτικές πλατφόρμες κοινοπρακτικών Αλυσίδων είναι το Hyperledger, το Corda, και το Quorum (Filatovas, et al. 2022).

Πέραν από τον τύπο μιας αλυσίδας, είναι απαραίτητο να γνωρίζουμε ότι σε κάθε περίπτωση μία αλυσίδα block μπορεί να παραμετροποιηθεί ποικιλοτρόπως ώστε να ανταποκρίνεται όσο το δυνατόν καλύτερα τις ανάγκες που καλείται να καλύψει. Κατά συνέπεια, οποιαδήποτε από τις προαναφερθείσες κατηγορίες μπορεί να διαφοροποιείται περισσότερο ή λιγότερο, προσαρμοζόμενο στις ιδιαίτερες ανάγκες.

5.4 Έξυπνα Συμβόλαια

Ως Έξυπνο Συμβόλαιο ή Έξυπνη Σύμβαση (*Smart Contract*) ονομάζεται ο εκτελέσιμος κώδικας που εκτελείται σε περιβάλλον Blockchain και επιτελεί μία συγκεκριμένη αυτοματοποιημένη διεργασία. Ο όρος αποτελεί ευφημισμό διότι τα Smart Contracts δεν διαθέτουν κάποιο ιδιαίτερο ευφυές χαρακτηριστικό ούτε λειτουργούν ακριβώς όπως τα συμβόλαια. Στην ουσία πρόκειται για τμήματα κώδικα που περιέχουν όρους και προϋποθέσεις. Τα έξυπνα συμβόλαια δέχονται ψηφιακά δεδομένα ως εισόδους, κάποια εκ των οποίων αποτελούν τις συνθήκες που είτε θα το πυροδοτήσουν είτε θα το απενεργοποιήσουν. Τα εν λόγω δεδομένα μπορούν να προέρχονται τόσο από το ίδιο το δίκτυο Blockchain μέσα στο οποίο λειτουργεί το έξυπνο συμβόλαιο αλλά και από άλλες εξωτερικές πηγές όπως βάσεις δεδομένων, συσκευές edge, κ.λπ. Η γενική λειτουργία τους υλοποιείται από εντολές ελέγχου ροής προγράμματος, γεγονός που τους προσδίδει ιδιαίτερη ποικιλομορφία αλλά και ευελιξία ως προς το εύρος των δυνατοτήτων που μπορούν να προσφέρουν. Ένα έξυπνο συμβόλαιο μπορεί να υλοποιηθεί ούτως ώστε να αποτελεί μια δυναμικά προσαρμοζόμενη οντότητα η οποία μπορεί να τροποποιεί τη συμπεριφορά της ανάλογα με τις τρέχουσες συνθήκες. Για παράδειγμα, μπορούν να μην έχουν σταθερή χρονική ισχύ αλλά υπό όρους μεταβαλλόμενη, εφόσον αυτό προσυμφωνείται από τις συναλλασσόμενες πλευρές. Σε κάθε περίπτωση, ένα τέτοιο χαρακτηριστικό θα πρέπει να έχει προβλεφθεί κατά τη συγγραφή του κώδικα, ώστε να εξυπηρετεί αντίστοιχα σενάρια χρήσης (Filatovas, et al. 2022).

Αρχικά, ένα έξυπνο συμβόλαιο ελέγχει κατά πόσο ικανοποιούνται όλες οι συνθήκες τις οποίες εποπτεύει. Όταν συμβαίνει αυτό, τότε ενεργοποιείται αυτομάτως αποδίδοντας στην έξοδό του τα κατάλληλα αποτελέσματα, εγγράφοντας παράλληλα τις σχετικές πληροφορίες στο Blockchain. Ένα πολύ απλό παράδειγμα χρήσης έξυπνου συμβολαίου θα μπορούσε να αφορά μία πλατφόρμα συμμετοχικής χρηματοδότησης (crowdfunding), όπου μόλις συμπληρώνεται το απαιτούμενο χρηματικό ποσόν να αποστέλλεται άμεσα στον δικαιούχο, διαφορετικά, εάν το ποσόν-στόχος δεν συμπληρωθεί εντός συγκεκριμένου χρονικού ορίου, τα καταβληθέντα από τους χρηματοδότες ποσά να επιστρέφονται σε αυτούς.

Τα Smart Contracts αποτελούν ένα από τα συγκριτικά πλεονεκτήματα της τεχνολογίας Blockchain καθώς προσφέρουν ευελιξία και προσαρμοστικότητα στην εξυπηρέτηση πληροφοριακών αναγκών διασφάλισης δεδομένων, μέσω αυτοματοποιημένων λύσεων που απλοποιούν διεργασίες, ελαχιστοποιούν τους χρόνους διεκπεραίωσης και μειώνουν το λειτουργικό κόστος. Αν και η ενσωμάτωση κώδικα ελέγχου ροής είναι μια συνήθης πρακτική που εφαρμόζεται σε όλα τα προγράμματα εδώ και δεκαετίες, η χρήση Smart Contracts στο σύγχρονο τεχνολογικό τοπίο αποτελεί μια καινοτομία με αυξανόμενη αποδοχή. Ο λόγος που η δημοφιλία της τεχνολογίας Blockchain διευρύνεται, οφείλεται σε μεγάλο ποσοστό στην ύπαρξη των έξυπνων συμβάσεων καθότι εξυπηρετούν λειτουργίες με άμεσο τρόπο, χωρίς διαμεσολάβηση τρίτων και χωρίς να υποβαθμίζεται η ασφάλεια και η διαφάνεια των διαδικασιών. Τα σενάρια χρήσης που μπορούν να εξυπηρετηθούν μέσω smart contracts είναι πρακτικά απεριόριστα, και μπορούν να ξεκινήσουν από τυπικές συναλλαγές, (π.χ. ανταλλαγή δεδομένων ή ακόμα και μεταφορές χρημάτων), έως πολυσύνθετες διεργασίες όπως η εποπτεία των σταδίων μιας εφοδιαστικής αλυσίδας, από την παραγωγή μέχρι την πώληση στον τελικό χρήστη. Κατά την πορεία αυτή, όλες οι προσυμφωνημένες ενέργειες μπορούν να υποστηριχθούν από την τεχνολογία Blockchain, συνεπικουρούμενη από έξυπνα συμβόλαια (Filatovas, et al. 2022).

5.5 Αποκεντρωμένες Εφαρμογές (DApps)

Οι Αποκεντρωμένες Εφαρμογές (*Decentralized Applications - DApps*) είναι ψηφιακές εφαρμογές, το back-end κομμάτι των οποίων λειτουργεί σε περιβάλλοντα κατανεμημένων υπολογιστικών συστημάτων, και πιο συγκεκριμένα σε Blockchain, ενώ το front-end σχεδιάζεται συνήθως ως διαδικτυακή εφαρμογή (web application). Τα εισερχόμενα δεδομένα, μπορούν να προέρχονται από διάφορες πηγές, αλλά και από τα ίδια τα smart contracts τα οποία υποστηρίζουν τις διάφορες αυτοματοποιημένες λειτουργίες τους (Johnson , et al. 2019).

Μία αποκεντρωμένη εφαρμογή μπορεί να υποστηρίζεται ένα και μόνο smart contract. Ωστόσο, οι μεγαλύτερης κλίμακας αποκεντρωμένες εφαρμογές διαθέτουν περισσότερα, και το πλήθος τους είναι ανάλογο της πολυπλοκότητας της εφαρμογής αλλά και του αριθμού των λειτουργιών που τα smart contracts καλούνται να εξυπηρετήσουν (Johnson , et al. 2019).

Στο διαδίκτυο υπάρχει μια πληθώρα αποκεντρωμένων εφαρμογών που προσφέρουν υπηρεσία σε πολλούς και διαφορετικούς τομείς δραστηριότητας, μεταξύ των οποίων βρίσκονται οικονομικές υπηρεσίες, υπηρεσίες σύναψης συμφωνητικών, τζόγος, ακόμα και βιντεοπαιχνίδια (Johnson , et al. 2019).

Το CryptoKitties ήταν το πρώτο ευρέως αναγνωρισμένο παιχνίδι που βασίστηκε στην τεχνολογία Blockchain, στο οποίο οι παίκτες μπορούσαν να συλλέγουν, να διασταυρώνουν, να εκτρέφουν και

να εμπορεύονται ψηφιακές γάτες, οι οποίες απεικονίζονταν μέσα από ευφάνταστα σχέδια. Η διαδρομή της ιδιοκτησίας κάθε ψηφιακής γάτας που έχει δημιουργηθεί και υπάρχει εντός του παιχνιδιού ανιχνεύεται μέσω smart contract. Η κάθε γάτα διαθέτει τη δική της μοναδική εμφάνιση η οποία καθορίζεται βάσει των "γονιδίων" της και κάθε ψηφιακό κατοικίδιο καταχωρείται μαζί με το ιστορικό ιδιοκτησίας του στο Blockchain. Οι δυνητικοί γονιδιακοί συνδυασμοί που μπορούν να προκύψουν μέσω διασταυρώσεων υπολογίζεται στα 4 δισεκατομμύρια (Johnson , et al. 2019).

Μένοντας στον κατηγορία των παιγνίων, και πηγαίνοντας πιο συγκεκριμένα στον τομέα του τζόγου, είναι σημαντικό να αναφέρουμε την ύπαρξη blockchain-enabled διαδικτυακών καζίνο. Οι συγκεκριμένες πλατφόρμες καθίστανται ιδιαίτερα ελκυστικές για τους παίκτες διότι, εκτός από ανωνυμία, μπορούν να προσφέρουν μεγαλύτερες πιθανότητες δυνητικού κέρδους συνοδευόμενη από τη διασφάλιση ότι τα τυχερά παίγνια διεξάγονται δίκαια και με διαφάνεια (Johnson , et al. 2019).

Μία άλλη αποκεντρωμένη εφαρμογή που παρουσιάζει ενδιαφέρον είναι το theContractApp, όπου δύο υποψήφιοι συμβαλλόμενοι μπορούν να συνθέσουν, να διαπραγματευθούν και εν τέλει να συνυπογράψουν ένα συμφωνητικό εμπιστευτικότητας. Οι συμβαλλόμενες πλευρές έχουν πρόσβαση σε μία εκτενή λίστα με άρθρα, όρους και προϋποθέσεις, και κάθε μία καλείται να επιλέξει όλους όσους επιθυμεί να συμπεριλαμβάνονται στην τελική έκδοση του εγγράφου, σημειώνοντας παράλληλα τον βαθμό κρισιμότητας καθενός εκ των όρων: Απαιτείται – Προτιμάται – Αποδεκτός – Έσχατη Λύση – Μη αποδεκτός. Όταν όλοι οι συμβαλλόμενοι ολοκληρώσουν τη διαδικασία επιλογής των όρων, το theContractApp δημιουργεί αυτομάτως μία πρώτη έκδοση του συμφωνητικού, καλύπτοντας στον καλύτερο δυνατό βαθμό τις απαιτήσεις όλων των πλευρών. Στη συνέχεια το έγγραφο κοινοποιείται στους συμβαλλόμενους και τίθεται στη διάθεσή τους για περαιτέρω διαπραγμάτευση. Μόλις υπάρξει συμφωνία επί του τελικού κειμένου, τότε οι συμβαλλόμενοι μπορούν να προχωρήσουν στη διαδικασία υπογραφής του, είτε ψηφιακά είτε εκτυπώνοντάς το και υπογράφοντας τα φυσικά αντίγραφα. Στο διαδίκτυο υπάρχουν και άλλα web applications προσφέρουν την ίδια υπηρεσία: αφαιρούν από τους χρήστες τον βάρος της συγγραφής, αποθήκευσης και συντήρησης τέτοιων εγγράφων, ή και την ανάγκη εμπλοκής μεσαζόντων που προσθέτουν στο τελικό κόστος. Αντικειμενικά, η εφαρμογή δεν προσφέρει κάτι πρωτότυπο, ωστόσο η επιπρόσθετη αξία του theContractApp έγκειται στην ενσωμάτωση τεχνολογίας Blockchain (Johnson , et al. 2019).

Τα Decentralized Finance (DeFi), είναι αποκεντρωμένες εφαρμογές προσανατολισμένες σε αντικείμενα χρηματοοικονομικής φύσεως όπως η έκδοση και διαχείριση δανείων ή ασφαλιστηρίων, η συμμετοχική χρηματοδότησης (crowdfunding), κ.α., αφαιρώντας από τις διαδικασίες του περιττούς μεσάζοντες. Η πιο οικεία κατηγορία DeFi είναι τα ανταλλακτήρια νομισμάτων. Σε αυτά, οι χρήστες μπορούν να μετατρέψουν ένα χρηματικό ποσόν από ένα νόμισμα σε ένα άλλο. Φυσικά, στον κόσμο του Blockchain, αυτά τα ανταλλακτήρια εξυπηρετούν επί το πλείστον ανταλλαγές μεταξύ κρυπτονομισμάτων, υποστηρίζοντας παράλληλα και κάποια νομίσματα «πραγματικού» χρήματος, συνήθως δολάρια ΗΠΑ, Ευρώ ή Κινεζικό γουαν. Άλλη κατηγορία DeFi είναι τα Prediction Markets (*Αγορές Προβλέψεων*) όπου εξυπηρετούν στοιχηματισμούς για μελλοντικά γεγονότα, όπως αποτελέσματα εκλογικών αναμετρήσεων, νικητές αθλητικών διοργανώσεων ή άλλων διαγωνισμών, κ.λπ. (Johnson , et al. 2019).

Τα παραπάνω ενδεικτικά παραδείγματα καθιστούν σαφές πως εάν μία εφαρμογή επιθυμεί να ενσωματώσει τεχνολογίες διασφάλισης πληροφοριών, κοινής εμπιστοσύνης και διαφάνειας, τότε η υιοθεσία λύσεων τεχνολογίας Blockchain θεωρείται μία από τις καλύτερες επιλογές ώστε να επιτευχθεί η απαραίτητη επιπρόσθετη αξία (Johnson , et al. 2019).

6 Αξιοποίηση ομομορφικών αλγορίθμων σε δεδομένα blockchain για εφαρμογές Μηχανικής Μάθησης

Η χρήση ομομορφικών αλγορίθμων κρυπτογράφησης σε δεδομένα Blockchain για εφαρμογές Μηχανικής Μάθησης προσφέρει έναν ιδιαίτερο συνδυασμό πλεονεκτημάτων που αφορούν τόσο την ιδιωτικότητα όσο και την υπολογιστική αποδοτικότητα.

Ένα από τα σημαντικότερα πλεονεκτήματα της χρήσης ομομορφικών αλγορίθμων κρυπτογράφησης με δεδομένα Blockchain είναι η δυνατότητα διατήρησης της ιδιωτικότητας του χρήστη. Σε περιβάλλοντα όπου ευαίσθητα δεδομένα αποθηκεύονται σε ένα blockchain - όπως ιατρικά αρχεία ή χρηματοοικονομικές συναλλαγές - η διασφάλιση της ιδιωτικότητας είναι μία σημαντική πρόκληση. Η ομομορφική κρυπτογράφηση επιτρέπει την ανάλυση ή την επεξεργασία αυτών των δεδομένων χωρίς να χρειάζεται να τα αποκρυπτογραφήσουμε. Επομένως, επιτρέπει λειτουργίες, όπως η ανάλυση δεδομένων καταναλωτών και η πρόληψη απάτης, να διεξάγονται με ασφάλεια χωρίς να εκτίθενται τα ιδιωτικά δεδομένα των χρηστών. Αυτό αντιμετωπίζει μία από τις πιο επίκαιρες ηθικές και νομικές προκλήσεις στην ανάλυση δεδομένων σήμερα: την προστασία της ιδιωτικότητας του χρήστη (Ali, et al. 2022)

Το δεύτερο πλεονέκτημα είναι η πιθανή βελτίωση στην εκπαίδευση των μοντέλων μηχανικής μάθησης. Οι παραδοσιακοί αλγόριθμοι μηχανικής μάθησης συχνά απαιτούν πρόσβαση σε ακατέργαστα δεδομένα για αποτελεσματική εκπαίδευση του μοντέλου. Ωστόσο, με την ομομορφική κρυπτογράφηση, τα μοντέλα μηχανικής μάθησης μπορούν να εκπαιδευτούν απευθείας στα κρυπτογραφημένα δεδομένα. Αυτό όχι μόνο διατηρεί την ιδιωτικότητα, αλλά επιτρέπει επίσης πιο ασφαλή και πιθανώς πιο αποδοτική συγκέντρωση δεδομένων από πολλαπλές πηγές. Εκπαιδεύοντας τα μοντέλα σε συγκεντρωμένα δεδομένα, τα μοντέλα μπορούν να αξιοποιήσουν ευρύτερο φάσμα δεδομένων, αυξάνοντας τη γενίκευση και βελτιώνοντας την ακρίβεια. Αυτό έχει επίσης θετικό αντίκτυπο στην υπολογιστική αποδοτικότητα, μειώνοντας πιθανώς τον χρόνο και τους πόρους που απαιτούνται για την εκπαίδευση αποδοτικών μοντέλων (Ali, et al. 2022).

Συνοπτικά, η συνδυασμένη χρήση ομομορφικών αλγορίθμων κρυπτογράφησης και δεδομένων blockchain μπορεί να προσφέρει βελτιωμένες λύσεις σε προκλήσεις που αφορούν την ιδιωτικότητα, την ασφάλεια και την αποδοτικότητα σε εφαρμογές μηχανικής μάθησης. Αυτό παρέχει νέες προοπτικές για την ανάπτυξη ασφαλών και αποδοτικών συστημάτων που επιλύουν καίρια ζητήματα στον τομέα της τεχνητής νοημοσύνης και της διατήρησης της ιδιωτικότητας. Η έρευνα για τη χρήση ομομορφικών αλγορίθμων σε δεδομένα blockchain για εφαρμογές μηχανικής μάθησης βρίσκεται ακόμα σε πρώιμο στάδιο. Ωστόσο, υπάρχουν πολλά υποσχόμενα αποτελέσματα που δείχνουν ότι αυτή η τεχνολογία μπορεί να έχει σημαντικό αντίκτυπο σε μια σειρά από βιομηχανίες. Στη συνέχεια, αναφέρονται παραδείγματα που παρουσιάζουν αυτήν τη συνέργεια και σκιαγραφούν τις δυνατότητες που παρέχει (Ali, et al. 2022):

- **Ανάλυση δεδομένων καταναλωτών:** Στην εποχή των μεγάλων δεδομένων, τα δεδομένα των καταναλωτών είναι μια πηγή πληροφοριών που οι επιχειρήσεις είναι πρόθυμες να εκμεταλλευτούν. Ωστόσο, η ανάγκη για ισορροπία μεταξύ της αξιοποίησης των δεδομένων και της προστασίας της ιδιωτικότητας αποτελεί σημαντική πρόκληση. Οι ομομορφικοί αλγόριθμοι προσφέρουν λύση σε αυτό το ζήτημα. Με την εφαρμογή αυτών των αλγορίθμων σε δεδομένα που αποθηκεύονται σε Blockchain, οι επιχειρήσεις μπορούν να διεξάγουν αναλύσεις σε κρυπτογραφημένα δεδομένα συμπεριφοράς των καταναλωτών χωρίς ποτέ να

εκθέτουν τις ταυτότητες των ατόμων. Αυτό οδηγεί σε μια κατάσταση αμοιβαίου οφέλους (win-win): οι επιχειρήσεις κερδίζουν πολύτιμες πληροφορίες ενώ διασφαλίζουν την ιδιωτικότητα των χρηστών, παραμένοντας πάντα σε συμμόρφωση με τους υφιστάμενους κανονισμούς προστασίας δεδομένων όπως το GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων)[4] και το CCPA[5] (Νόμος για την Προστασία της Ιδιωτικότητας των Καταναλωτών της Καλιφόρνια).

- **Πρόληψη απάτης:** Οι οικονομικές και ηλεκτρονικές απάτες αποτελούν διαδεδομένες απειλές που προκαλούν απώλειες δισεκατομμυρίων κάθε χρόνο. Παραδοσιακά, τα μοντέλα μηχανικής μάθησης που χρησιμοποιούνται για την ανίχνευση απάτης απαιτούσαν πρόσβαση σε ακατέργαστα, ευαίσθητα δεδομένα συναλλαγών. Με την εφαρμογή ομομορφικών αλγορίθμων σε δεδομένα Blockchain, ωστόσο, γίνεται εφικτή η εκπαίδευση μοντέλων μηχανικής μάθησης σε κρυπτογραφημένες εγγραφές συναλλαγών. Η αξιοπιστία της τεχνολογίας Blockchain διασφαλίζει ότι τα δεδομένα αυτά είναι αδιάβλητα, προσθέτοντας ένα επιπλέον επίπεδο αξιοπιστίας στα μοντέλα. Ως αποτέλεσμα, η εφαρμογή της μηχανικής μάθησης σε κρυπτογραφημένα δεδομένα Blockchain θα μπορούσε να αποτελέσει μια βασική συνιστώσα στις σύγχρονες στρατηγικές πρόληψης απάτης.

- **Ανάπτυξη νέων προϊόντων και υπηρεσιών:** Η ευελιξία των σύγχρονων επιχειρήσεων εξαρτάται συχνά από την ταχύτητα και την ακρίβεια των αποφάσεων που βασίζονται σε δεδομένα. Και εδώ, η ολοκληρωμένη εφαρμογή των ομομορφικών αλγορίθμων με την τεχνολογία Blockchain μπορεί να παίξει σημαντικό ρόλο. Με την ασφαλή επεξεργασία κρυπτογραφημένων δεδομένων Blockchain, οι εταιρείες μπορούν να αποκτήσουν ενδείξεις και γνώση για τις τάσεις της αγοράς, τις προτιμήσεις των πελατών, ακόμα και για τις λειτουργικές ανεπάρκειες, όλα αυτά χωρίς υποβάθμιση της προστασίας των δεδομένων.

Ενώ η έρευνα στην ολοκληρωμένη εφαρμογή ομομορφικών αλγορίθμων, τεχνολογίας Blockchain και μηχανικής μάθησης βρίσκεται ακόμη στα αρχικά της στάδια, οι πρώτες εκτιμήσεις αναδεικνύουν σημαντική προοπτική. Δεδομένης της αυξανόμενης σημασίας της προστασίας των δεδομένων και της ασφάλειας στη σημερινή ψηφιακή εποχή, αυτός ο συνδυασμός τεχνολογιών θα μπορούσε να γίνει καθοριστικός για τον σχεδιασμό πιο ασφαλών, ιδιωτικών και αποδοτικών ψηφιακών υποδομών (Ali, et al. 2022).

6.1 Landscape analysis / State of the Art

Σε μια εποχή όπου τα θέματα της ιδιωτικότητας των δεδομένων, της ασφάλειας και της υπολογιστικής αποδοτικότητας θεωρούνται αυξημένης σημασίας, ο συνδυασμός αλγορίθμων ομομορφικής κρυπτογράφησης, τεχνολογίας blockchain και Μηχανικής Μάθησης μπορεί να αποτελέσει σημαντικό καταλύτη. Ο συνδυασμός αλγορίθμων ομομορφικής κρυπτογράφησης, τεχνολογίας blockchain και μηχανικής μάθησης αποτελεί ένα καινοτόμο πεδία στην υπολογιστική έρευνα, παρουσιάζοντας σημαντικές δυνατότητες για μια πληθώρα εφαρμογών που κυμαίνονται από τα οικονομικά συστήματα έως την υγεία. Οι προκαταρκτικές προσπάθειες που καταβάλλονται από τεχνολογικές εταιρείες σηματοδοτούν το σημαντικό δυναμικό της χρήσης κρυπτογραφημένων, αποκεντρωμένων δεδομένων για εργασίες μηχανικής μάθησης χωρίς να διακυβεύεται η ιδιωτικότητα

[4]: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679
[5] https://oag.ca.gov/privacy/ccpa

των χρηστών. Αν και η έρευνα και η ανάπτυξη σε αυτόν τον τομέα είναι ακόμα σε πρώιμα στάδια, τα πρώιμα αποτελέσματα υποδηλώνουν ότι αυτός ο συνδυασμός τεχνολογιών θα μπορούσε να αλλάξει τα δεδομένα σε διάφορους βιομηχανικούς τομείς (Krupitzer and Stein 2021).

Συνεργασία Microsoft και ConsenSys

Η Microsoft και η ConsenSys (μια εταιρεία λογισμικού blockchain), έχουν συνεργαστεί για την ανάπτυξη λύσεων για το Ethereum. Η ConsenSys αναπτύσσει λογισμικό που λειτουργεί στο δίκτυο Ethereum. Η Microsoft έχει επενδύσει στην ConsenSys, διπλασιάζοντας την αξία της σε 7 δισεκατομμύρια δολάρια (Bradford 2023).

Όσον αφορά την ομομορφική κρυπτογράφηση, η Microsoft έχει αναπτύξει τη βιβλιοθήκη Simple Encrypted Arithmetic Library (SEAL). Η SEAL επιτρέπει στους χρήστες της υποδομής cloud να αποθηκεύουν τα δεδομένα σε υποδομές παρόχων, χωρίς οι τελευταίοι να έχουν πρόσβαση σε μη-κρυπτογραφημένα δεδομένα που αποθηκεύονται στα συστήματά τους. Αυτή η τεχνολογία ομομορφικής κρυπτογράφησης επιτρέπει την εκτέλεση υπολογισμών απευθείας σε κρυπτογραφημένα δεδομένα. Τα αποτελέσματα τέτοιων κρυπτογραφημένων υπολογισμών παραμένουν κρυπτογραφημένα και μπορούν να αποκρυπτογραφηθούν μόνο από τον κάτοχο των δεδομένων χρησιμοποιώντας το μυστικό κλειδί (Bradford 2023).

Συνεργασία IBM και R3

Η IBM και η R3, μια εταιρεία λογισμικού επιχειρήσεων, ανακοίνωσαν μια νέα συνεργασία για να επεκτείνουν επίσημα την επιλογή για πελάτες που θέλουν να υιοθετήσουν λύσεις τεχνολογίας blockchain, παρέχοντας υψηλότερα επίπεδα απόδοσης, συμμόρφωσης και προστασίας δεδομένων. Στο πλαίσιο της συνεργασίας, η R3 ανακοίνωσε ένα νέο ανοιχτό πρόγραμμα beta για να φέρει την επιχειρηματική πλατφόρμα blockchain της R3, το Corda Enterprise, στο IBM LinuxONE σε όλο το hybrid cloud, τόσο on-premises όσο και στο IBM Cloud, παρέχοντας σχετικές υπηρεσίες μέσω των IBM Cloud Hyper Protect Services. Το πρόγραμμα beta R3 στο IBM LinuxONE άνοιξε στις 2 Νοεμβρίου 2020 και ήταν διαθέσιμο στο IBM Cloud και on-premises. Η γενική διαθεσιμότητα (GA) αναμενόταν το πρώτο τρίμηνο του 2021 (Chow, Dial & Gambetta, 2021) ενώ σήμερα η πλατφόρμα cloud της IBM υποστηρίζει την υπηρεσία IBM Support for Hyperledger Fabric[6] και το IBM Blockchain[7].

Για πελάτες με εξαιρετικά ευαίσθητα δεδομένα και εργασίες, όπως ψηφιακή ταυτότητα, ψηφιακά στοιχεία, ψηφιακά νομίσματα κεντρικής τράπεζας, tokens, πληροφορίες πληρωμών ή έξυπνα συμβόλαια που αποθηκεύονται σε περιβάλλοντα hybrid cloud, το IBM LinuxONE παρέχει μια πλατφόρμα υψηλής ασφάλειας που έχει πιστοποιηθεί ότι πληροί το υψηλότερο επίπεδο εμπορικά διαθέσιμης πιστοποίησης ασφαλείας. Το IBM LinuxONE και τα IBM Cloud Hyper Protect Services παρέχουν στους πελάτες δυνατότητες Confidential Computing, συμπεριλαμβανομένων των δυνατοτήτων κρυπτογράφησης απομόνωσης εργασίας «Keep Your Own Key» που υποστηρίζονται από την πιστοποίηση FIPS 140-2 Level 4, προστασία από παραβίαση από προνομιούχους χρήστες και κρυπτογράφηση όλων των δεδομένων τόσο κατά τη μεταφορά όσο και την αποθήκευση,

[6] https://cloud.ibm.com/docs/blockchain?topic=blockchain-ibp-console-overview
[7] https://www.ibm.com/blockchain?lnk=fps

καθιστώντας το IBM public cloud το πιο ασφαλές και ανοιχτό δημόσιο cloud για επιχειρήσεις (Chow, Dial and Gambetta 2021).

Άλλα παραδείγματα είναι:

- **NuCypher:** Η NuCypher ήταν μια εταιρεία που προσφέρει υπηρεσίες κρυπτό-θωράκισης (crypto-shielding) για δεδομένα Blockchain, χρησιμοποιώντας ομομορφική κρυπτογράφηση και proxy re-encryption. Το proxy re-encryption είναι μια άλλη τεχνολογία που χρησιμοποιεί η NuCypher η οποία επιτρέπει σε έναν μη έμπιστο proxy κόμβο να επανακρυπτογραφεί δεδομένα που έχουν ήδη κρυπτογραφηθεί με το δημόσιο κλειδί του αποστολέα. Έτσι, τα δεδομένα μπορούν να παραμείνουν κρυπτογραφημένα καθ' όλη τη διάρκεια της μετάδοσης, ενώ παράλληλα επιτρέπεται η επανακρυπτογράφηση των δεδομένων από τον παραλήπτη Από τον Ιανουάριο του 2022 το κρυπτοδίκτυο της NuCypher συγχωνεύτηκε με αυτό του Keep Network, κάτω από την επωνυμία " **Threshold Network**".

- **Secret Network** (πρώην **Enigma**)**:** Είναι μια πλατφόρμα βασισμένη στην τεχνολογία Blockchain που σχεδιάστηκε για να παρέχει ιδιωτικότητα για έξυπνα συμβόλαια. Η πλατφόρμα στοχεύει στην επίλυση του ζητήματος της ιδιωτικότητας στην τεχνολογία Blockchain, επιτρέποντας την τέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα. Σε αντίθεση με τα παραδοσιακά έξυπνα συμβόλαια, τα οποία είναι δημόσια και διαφανή, τα έξυπνα συμβόλαια του Enigma (συχνά αναφέρονται ως «μυστικά συμβόλαια») στοχεύουν στη διατήρηση της εχεμυθείας των εισαγόμενων δεδομένων (Bradford 2023).

  Η αρχιτεκτονική του Enigma αρχικά σχεδιάστηκε για να χρησιμοποιεί ασφαλή υπολογισμό πολλαπλών μερών (*μτφρ. secure multi-party computation, sMPC*), μια κρυπτογραφική τεχνική που επιτρέπει στα μέρη να υπολογίζουν κοινά μια συνάρτηση χωρίς να αποκαλύπτουν τις εισόδους τους στο άλλο μέρος. Με αυτόν τον τρόπο, τα δεδομένα μπορούν να παραμείνουν εμπιστευτικά ενώ εξακολουθούν να υποβάλλονται σε επεξεργασία.

  Το πρωτόκολλο Enigma λειτουργεί ως ένα δίκτυο δεύτερου επιπέδου, γεγονός που σημαίνει ότι μπορεί να λειτουργήσει πάνω από υφιστάμενες αλυσίδες, ένα σημαντικό χαρακτηριστικό που επιτρέπει πιο ευέλικτες και ευρέως εφαρμόσιμες λύσεις.

- **Zama:** Η Zama είναι μια εταιρεία που εξειδικεύεται στην ομομορφική κρυπτογράφηση και την εφαρμογή της σε εφαρμογές Μηχανικής Μάθησης. Σύμφωνα με την επίσημη ιστοσελίδα της, η Zama παρέχει εργαλεία που επιτρέπουν στους επιστήμονες δεδομένων και τους προγραμματιστές να χρησιμοποιούν την ομομορφική κρυπτογράφηση χωρίς να χρειάζεται να γνωρίζουν κρυπτογραφία. Η τεχνολογία της Zama επιτρέπει οποιονδήποτε υπολογισμό να πραγματοποιηθεί πάνω σε κρυπτογραφημένα δεδομένα, ανεξάρτητα από το πόσο περίπλοκα είναι (Bradford 2023).

  Μερικά παραδείγματα εφαρμογών Μηχανικής Μάθησης που η Zama έχει υλοποιήσει ή σχεδιάζει να υλοποιήσει με τη χρήση των ομομορφικών αλγορίθμων της είναι τα εξής:

  - Κρυπτογραφημένη συνομιλία με το ChatGPT-4, ένα μεγάλο μοντέλο γλώσσας (large language model/LLM) που μπορεί να παράγει ρεαλιστικό κείμενο και εικόνες. Η Zama στοχεύει να ενσωματώσει κρυπτογράφηση στην πλήρη ροή εργασιών του ChatGPT-4 με χρήση ομομορφικής κρυπτογράφησης, έτσι ώστε οι χρήστες να

μπορούν να χρησιμοποιούν το μοντέλο χωρίς να αποκαλύπτουν τα προσωπικά τους δεδομένα.

- Κρυπτογραφημένη εφαρμογή φίλτρων εικόνας, που επιτρέπει στους χρήστες να εφαρμόζουν φίλτρα σε εικόνες χωρίς να αποκαλύπτουν το περιεχόμενο της εικόνας. Η Zama έχει δημιουργήσει έναν χώρο στο Hugging Face, όπου οι χρήστες μπορούν να δοκιμάσουν την εφαρμογή, χρησιμοποιώντας τα εργαλεία Concrete-Numpy και Concrete-ML.

- Κρυπτογραφημένη εκπαίδευση και πρόβλεψη μοντέλων μηχανικής μάθησης, που επιτρέπει στους χρήστες να εκπαιδεύουν και να χρησιμοποιούν μοντέλα μηχανικής μάθησης σε κρυπτογραφημένα δεδομένα. Η Zama έχει υλοποιήσει το πρότυπο ResNet-20 με το σχήμα ομομορφικής κρυπτογράφησης RNS-CKKS και το έχει επαληθεύσει με το σύνολο δεδομένων CIFAR-10[8] και τις παραμέτρους του μοντέλου σε απλό κείμενο.

Συνολικά, η Zama προσφέρει μια πρωτοποριακή λύση για την προστασία της ιδιωτικότητας των δεδομένων σε εφαρμογές Μηχανικής Μάθησης, χρησιμοποιώντας την ομομορφική κρυπτογράφηση για να επιτρέψει την επεξεργασία και την ανάλυση των δεδομένων χωρίς να αποκαλύπτεται η πραγματική τους τιμή.

- **SAP:** Ένας κορυφαίος πάροχος λύσεων λογισμικού για επιχειρήσεις, ο οποίος χρησιμοποιεί τους ομομορφικούς αλγόριθμους για να προσφέρει υψηλό επίπεδο ασφάλειας και ιδιωτικότητας στα δεδομένα των πελατών του, επιτρέποντάς τους να εκτελούν ανάλυση και μάθηση σε κρυπτογραφημένα δεδομένα χωρίς να χρειάζεται να τα αποκωδικοποιήσουν. Η πρωτοβουλία της SAP στην ομομορφική κρυπτογράφηση στοχεύει στη βελτίωση των δυνατοτήτων της τεχνητής νοημοσύνης παρέχοντας έναν ασφαλή τρόπο για την εκπαίδευση των μοντέλων μηχανικής μάθησης με ευαίσθητα δεδομένα. Η SAP συνεργάζεται ενεργά με άλλες εταιρείες, πανεπιστήμια και startups για τον τυποποίηση της ομομορφικής κρυπτογράφησης και να την καταστήσει πιο εφαρμόσιμη για πρακτική χρήση. Εντός της SAP, λειτουργεί το Innovation Center Network μια κρίσιμη μονάδα που επικεντρώνεται στις τεχνολογίες μηχανικής μάθησης και Blockchain. Αυτή η μονάδα στοχεύει στην επίλυση των εμφανιζόμενων προκλήσεων μέσω της πρωτοπορίας νέων τεχνολογιών που συμπληρώνουν τα βασικά πλεονεκτήματα της SAP (Bradford 2023).

6.2 Προκλήσεις / Προβλήματα

Η χρήση ομομορφικών αλγορίθμων σε δεδομένα blockchain για εφαρμογές Μηχανικής Μάθησης είναι μια πρωτοποριακή προσέγγιση που συνδυάζει την ασφάλεια της κρυπτογραφίας με την ισχύ της Μηχανικής Μάθησης. Ωστόσο, όπως αναδείχθηκε σε προηγούμενες παραγράφους, αυτή η προσέγγιση παρουσιάζει ορισμένες προκλήσεις, οι οποίες συνοψίζονται στις ακόλουθες ενότητες.

6.2.1 Υπολογιστική Πολυπλοκότητα

Η πρόκληση της υπολογιστικής πολυπλοκότητας είναι ένα από τα κύρια εμπόδια για την εφαρμογή των ομομορφικών αλγορίθμων σε περιβάλλοντα blockchain για εφαρμογές μηχανικής μάθησης. Οι ομομορφικοί αλγόριθμοι επιτρέπουν την εκτέλεση πράξεων πάνω σε κρυπτογραφημένα δεδομένα

[8] https://www.cs.toronto.edu/~kriz/cifar.html

χωρίς να απαιτείται η αποκρυπτογράφησή τους, διατηρώντας έτσι την ιδιωτικότητα και την ασφάλειά τους. Ωστόσο, αυτό συνεπάγεται ότι οι πράξεις σε ομομορφικά δεδομένα είναι πολύ πιο πολύπλοκες από τις απλές αριθμητικές πράξεις, καθώς χρησιμοποιούν μεγάλους αριθμούς και σύνθετους κανόνες. Αυτό σημαίνει ότι οι ομομορφικοί αλγόριθμοι απαιτούν σημαντικά ποσά υπολογιστικών πόρων, τόσο για τη δημιουργία και τη διαχείριση των κλειδιών κρυπτογράφησης, όσο και για την εκτέλεση των πράξεων. Σε ένα περιβάλλον blockchain, όπου ο χώρος και ο χρόνος είναι περιορισμένοι, αυτό μπορεί να αποδειχθεί πρόβλημα, καθώς μπορεί να επηρεάσει την ικανότητα κλιμάκωσης και επέκτασης, τη συμβατότητα και τη διαδικασία επίτευξης συναίνεσης του δικτύου (π.χ. blockchain consensus). Γι' αυτό, είναι απαραίτητο να βρεθούν λύσεις που να βελτιώνουν την απόδοση και τη βεβαιότητα των ομομορφικών αλγορίθμων, χωρίς να υποβαθμίζουν τη λειτουργία και τη δυναμική του blockchain (Jordan and Mitchell 2015).

6.2.2 Χρόνοι Εκτέλεσης

Όπως αναφέρθηκε, οι ομομορφικοί αλγόριθμοι απαιτούν συγκριτικά περισσότερους υπολογισμούς και μνήμη για να εκτελέσουν τις πράξεις στα κρυπτογραφημένα δεδομένα. Αυτό σημαίνει ότι η επεξεργασία των δεδομένων σε περιβάλλοντα blockchain, όπου οι πόροι είναι περιορισμένοι και η επικοινωνία είναι αργή, μπορεί να είναι ασύμφορη. Επίσης, η εκπαίδευση και η πρόβλεψη των μοντέλων Μηχανικής Μάθησης απαιτούν συχνά πολλές επαναλήψεις και αλληλεπίδραση με τα δεδομένα, που μπορεί να γίνουν ακόμη πιο χρονοβόρες με τους ομομορφικούς αλγόριθμους. Γι' αυτό, είναι σημαντικό να βρεθούν τρόποι να βελτιωθεί η απόδοση και η κλιμάκωση των ομομορφικών αλγόριθμων, ώστε να μπορέσουν να χρησιμοποιηθούν αποτελεσματικά σε περιβάλλοντα blockchain για εφαρμογές μηχανικής μάθησης (Jordan and Mitchell 2015).

6.2.3 Δυσκολία Εφαρμογής

Η χρήση ομομορφικών αλγορίθμων σε περιβάλλοντα blockchain για εφαρμογές μηχανικής μάθησης είναι δύσκολη και απαιτεί μια σειρά από εξειδικευμένες γνώσεις και δεξιότητες. Ειδικοί στον τομέα της κρυπτογραφίας πρέπει να διαθέτουν βαθιά κατανόηση των μαθηματικών και των αλγοριθμικών θεμελίων της ομομορφικής κρυπτογραφίας, ενώ παράλληλα πρέπει να έχουν και την ικανότητα να ενσωματώσουν αυτές τις γνώσεις σε μια πλατφόρμα blockchain.

Ωστόσο, η κρυπτογραφία δεν είναι ο μόνος τομέας στον οποίο απαιτείται αυξημένη εξειδίκευση. Επιπρόσθετα, απαιτείται εμπειρία και εξειδίκευση στη μηχανική μάθηση, ιδιαίτερα στον σχεδιασμό και την ανάπτυξη αλγορίθμων που μπορούν να λειτουργήσουν αποτελεσματικά με κρυπτογραφημένα δεδομένα. Η επιλογή των κατάλληλων μοντέλων, η κατανόηση των περιορισμών της ομομορφικής κρυπτογραφίας ως προς τις υπολογιστικές δυνατότητες και οι προσαρμογές για την επίτευξη αποδοτικότητας είναι κρίσιμα στοιχεία.

Προσθέτοντας σε αυτό το σύνθετο μίγμα τις απαιτήσεις της αρχιτεκτονικής blockchain, η οποία θα πρέπει να είναι αποτελεσματική, ασφαλής και αξιόπιστη, καθίσταται φανερό ότι οι ομάδες εργασίας πρέπει να διαθέτουν αυξημένες γνώσεις και δεξιότητες σε ένα πλήθος επιστημονικών πεδίων. Αυτό ενδέχεται να σηματοδοτεί την ανάγκη για στενή συνεργασία μεταξύ διάφορων ειδικοτήτων, συμπεριλαμβανομένων ανθρώπων με εμπειρία στη διαχείριση δεδομένων, στην ασφάλεια δικτύων και στην υλοποίηση λογισμικού ή ακόμη και στη διάδραση ανθρώπου-υπολογιστή έτσι ώστε οι τελικές λύσεις να παρουσιάζονται στους χρήστες με εύληπτο τρόπο και να είναι δυνατόν να αξιοποιηθούν. Όλα αυτά συνδυαστικά καθιστούν την εφαρμογή των ομομορφικών αλγορίθμων σε τέτοιου είδους περιβάλλοντα μια πολύπλοκη αλλά και πολύ ενδιαφέρουσα πρόκληση (Jordan and Mitchell 2015).

6.2.4 Προστασία της ιδιωτικότητας

Η εφαρμογή ομομορφικών αλγορίθμων σε τεχνολογίες blockchain συνδυαζόμενη με εφαρμογές μηχανικής μάθησης αποτελεί δύσκολη πρόκληση, ειδικά στο ζήτημα της διαφύλαξης της ιδιωτικότητας. Η κρυπτογραφική εμπειρογνωμοσύνη θα πρέπει να είναι πολύ προχωρημένη, καθώς οι αποφάσεις που θα ληφθούν μπορεί να έχουν σημαντικές επιπτώσεις στην ασφάλεια και την προστασία της ιδιωτικότητας των δεδομένων. Επίσης, σε ό,τι αφορά το κομμάτι του blockchain, η κατανόηση των συναφών αρχιτεκτονικών και μηχανισμών ασφάλειας είναι εξίσου κρίσιμη. Το blockchain προσφέρει ένα αποκεντρωμένο και ασφαλές περιβάλλον, και η εισαγωγή ομομορφικών αλγορίθμων προσθέτει ένα επιπλέον επίπεδο πολυπλοκότητας.

Παρά τις προσπάθειες για υψηλό επίπεδο προστασίας της ιδιωτικότητας, πάντα υπάρχει το ενδεχόμενο διαρροών πληροφοριών. Αυτό μπορεί να οφείλεται σε αδυναμίες ή ευπάθειες στο σχεδιασμό του συστήματος, σε ανθρώπινα λάθη ή σε εξωτερικούς παράγοντες όπως ψηφιακές επιθέσεις. Επομένως, εκτός από την τεχνική εμπειρογνωμοσύνη, απαιτείται συνεχής ενημέρωση για τις τελευταίες εξελίξεις στην κρυπτογραφία και την ασφάλεια της πληροφορίας, καθώς και στενή συνεργασία με ειδικούς σε θέματα ασφάλειας και νομοθεσίας (Jordan and Mitchell 2015).

6.2.5 Διασυνδεσιμότητα

Στο αντικείμενο που ερευνά η συγκεκριμένη εργασία, η έλλειψη τεχνικής διασυνδεσιμότητας μπορεί να οφείλεται σε ασυμβατότητες μεταξύ διαφορετικών τεχνολογικών πλαισίων, αλλά και στο γεγονός ότι διάφορες βιβλιοθήκες μηχανικής μάθησης και πλατφόρμες Blockchain έχουν κατασκευαστεί με διαφορετικούς στόχους και υποθέσεις κατά τον σχεδιασμό τους. Συνεπώς, απαιτείται μια σε βάθος κατανόηση τόσο της μηχανικής μάθησης όσο και της τεχνολογίας blockchain από τους ενδιαφερόμενους. Το προσωπικό που εργάζεται σε αυτά τα έργα θα πρέπει να κατανοεί πλήρως τις αρχές των ομομορφικών αλγορίθμων, την αρχιτεκτονική των blockchain δικτύων και τους αλγορίθμους μηχανικής μάθησης που είναι απαραίτητοι για την εκάστοτε εφαρμογή (Jordan and Mitchell 2015).

Από το εννοιολογικό επίπεδο, η ομάδα θα πρέπει να εργάζεται συνεχώς για τη γεφύρωση και τη διασυνδεσιμότητα των διάφορων τεχνολογικών κομματιών. Αυτό μπορεί να περιλαμβάνει την κατασκευή διασυνδέσεων μεταξύ διαφορετικών βιβλιοθηκών ή τη χρήση πρότυπων δεδομένων και πρωτοκόλλων που επιτρέπουν τη συνεργασία μεταξύ των συστημάτων.

Εκτός από την τεχνική εμπειρογνωμοσύνη, είναι απαραίτητο να υπάρχει και μια στρατηγική οπτική. Η εκάστοτε ομάδα ανάπτυξης θα πρέπει να είναι σε θέση να αξιολογεί τις μεταβλητές του εγχειρήματος, μεταξύ των οποίων το κόστος, το χρονικό πλαίσιο και οι επιπτώσεις στην ασφάλεια, και να τις συνδυάζει με τους τεχνολογικούς περιορισμούς χωρίς να αφήνει ανεκμετάλλευτες τις όποιες ευκαιρίες.

Φυσικά, η ικανότητα στην επικοινωνία και τη συνεργασία είναι ζωτικής σημασίας. Είναι απαραίτητο τα μέλη της ομάδας να μπορούν να ανταλλάσσουν ιδέες και πληροφορίες αποτελεσματικά, να κατανοούν τις διάφορες προκλήσεις και περιορισμούς και να εργάζονται από κοινού για την επίτευξη των στόχων του έργου (Jordan and Mitchell 2015).

7 Ενδεικτικά πεδία για την ανάπτυξη καινοτόμων λύσεων (Beyond the State of the Art)

Οι δυνητικοί συνδυασμοί των ομομορφικών αλγορίθμων, της τεχνολογίας Blockchain, και της μηχανικής μάθησης ανοίγουν νέους ορίζοντες για την ανάπτυξη προηγμένων λύσεων σε διάφορους τομείς. Το Blockchain, με την κατανεμημένη του φύση και την ικανότητα να παρέχει αμετάβλητα δεδομένα, δημιουργεί μια αξιόπιστη βάση για την αποθήκευση και διαχείριση δεδομένων. Οι ομομορφικοί αλγόριθμοι, από την άλλη πλευρά, επιτρέπουν την εκτέλεση υπολογισμών πάνω σε κρυπτογραφημένα δεδομένα χωρίς αυτά να χρειάζεται να αποκρυπτογραφηθούν, παρέχοντας έτσι εγγυήσεις για την προστασία της ιδιωτικότητας και την ασφάλεια.

Η μηχανική μάθηση, με την ικανότητα να δημιουργεί προβλεπτικά μοντέλα και να ανακαλύπτει μοτίβα μέσα από μεγάλα σύνολα δεδομένων, μπορεί να επωφεληθεί σημαντικά από την πλούσια και ασφαλή πηγή δεδομένων που παρέχεται από το Blockchain. Επιπλέον, η δυνατότητα εκτέλεσης υπολογισμών πάνω σε κρυπτογραφημένα δεδομένα με ομομορφικούς αλγορίθμους θέτει τις προϋποθέσεις για νέες, ασφαλείς εφαρμογές μηχανικής μάθησης σε περιβάλλοντα Blockchain.

Οι εν λόγω τεχνολογίες καταδεικνύουν τη συνεχή εξέλιξη προς την κατεύθυνση της ανάπτυξης προηγμένων λύσεων σε τομείς όπως η υγεία, η χρηματοπιστωτική τεχνολογία, η αλυσίδα εφοδιασμού, η δημόσια διοίκηση και η ενέργεια, όπου η ακρίβεια, η ασφάλεια, και η ιδιωτικότητα των δεδομένων είναι κρίσιμης σημασίας. Ενδεικτικές κατευθύνσεις για προηγμένες λύσεις σε διάφορους τομείς παρουσιάζονται στις ακόλουθες παραγράφους.

7.1 Υγεία

7.1.1 Προστατευμένη ιατρική έρευνα

Η ιατρική έρευνα είναι ένας τομέας ο οποίος επωφελείται σημαντικά από την ανάλυση μεγάλων όγκων δεδομένων. Η ανάλυση αυτών των δεδομένων μπορεί να προσφέρει σημαντικές ενδείξεις για την ανάπτυξη νέων φαρμάκων, την κατανόηση της πορείας διάφορων ασθενειών και την κατάρτιση πιο αποτελεσματικών πρωτοκόλλων θεραπείας, πιθανώς προσαρμοσμένων σε ατομικό επίπεδο. Ωστόσο, η πρόσβαση και η ανάλυση των ιατρικών δεδομένων πρέπει να γίνεται με τρόπο που να σέβεται την ιδιωτικότητα των ασθενών, σύμφωνα με το νομικό αλλά και το δεοντολογικό πλαίσιο (Liu, et al. 2020).

Σε αυτό το πλαίσιο, η τεχνολογία blockchain συνδυασμένη με ομομορφικούς αλγορίθμους και αλγορίθμους μηχανικής μάθησης μπορεί να προσφέρει μια λειτουργική και βιώσιμη λύση. Το blockchain μπορεί να προσφέρει ένα ασφαλές και περιβάλλον για την αποθήκευση και διαχείριση των ιατρικών δεδομένων, παρέχοντας εγγυήσεις για την αυθεντικότητα και την ακεραιότητά τους. Κάθε εγγραφή δεδομένων μπορεί να καταγραφεί με έναν μοναδικό κωδικό (hash) που εγγυάται την αυθεντικότητα και το αμετάβλητο των δεδομένων. Συμπληρωματικά, οι ομομορφικοί αλγόριθμοι, επιτρέπουν την επεξεργασία των δεδομένων χωρίς να αποκαλύπτεται η πραγματική τους τιμή, προσφέροντας έτσι ένα επίπεδο προστασίας της ιδιωτικότητας που είναι απαραίτητο στην ιατρική έρευνα. Αυτό επιτρέπει στους ερευνητές να αναλύουν τα δεδομένα και να εξάγουν χρήσιμα συμπεράσματα χωρίς να κινδυνεύει η ιδιωτικότητα των ασθενών (Liu, et al. 2020).

Παράλληλα, οι αλγόριθμοι μηχανικής μάθησης μπορούν να εφαρμοστούν στα κρυπτογραφημένα αυτά δεδομένα για την ανάλυση τάσεων, την πρόβλεψη εξελίξεων και την εξαγωγή βαθύτερων ενδείξεων που μπορούν να συμβάλλουν στην προώθηση της ιατρικής έρευνας και πρακτικής. Με

αυτόν τον τρόπο, η συνεργασία των τεχνολογιών blockchain, ομομορφικών αλγορίθμων και μηχανικής μάθησης μπορεί να δημιουργήσει ένα πολύ ισχυρό εργαλείο για την προώθηση της ιατρικής έρευνας, διατηρώντας παράλληλα την ασφάλεια και την ιδιωτικότητα των δεδομένων των ασθενών (Telenti and Jiang 2020).

Δυνητικές εφαρμογές:

- Πρόβλεψη πιθανών επιπλοκών υγείας βάσει προσωπικών ιατρικών δεδομένων.
- Ανίχνευση πιθανών αλληλεπιδράσεων και εμφάνισης ανεπιθύμητων παρενεργειών φαρμάκων με βάση το ιατρικό ιστορικό του ασθενούς.
- Πρόβλεψη επιδημιών ή εξάπλωσης νοσημάτων μέσα σε πληθυσμούς, με βάση τα ιατρικά δεδομένα και τα μοτίβα που ανιχνεύονται.
- Αυτόματη προσαρμογή δόσεων φαρμάκων ή θεραπειών βάσει των ατομικών αναγκών και αποτελεσμάτων.
- Ανάλυση της απόκρισης του ασθενούς σε θεραπευτικές παρεμβάσεις για τη βελτίωση της αποτελεσματικότητας των μελλοντικών θεραπειών.

7.1.2 Εξατομικευμένη αγωγή και φροντίδα

Στον τομέα της υγείας καταγράφεται μια δυναμική προς την κατεύθυνση της προσαρμοσμένης φροντίδας, όπου οι θεραπευτικές προσεγγίσεις και οι συστάσεις υγείας προσαρμόζονται στις μοναδικές ανάγκες και συνθήκες κάθε ασθενούς. Τεχνολογίες όπως το blockchain, οι ομομορφικοί αλγόριθμοι και οι αλγόριθμοι μηχανικής μάθησης μπορούν να παίξουν κεντρικό ρόλο στην υλοποίηση αυτής της προσέγγισης (Telenti and Jiang 2020).

Το blockchain μπορεί να προσφέρει ένα ασφαλές πλαίσιο για την αποθήκευση και διαχείριση των ιατρικών καταγραφών των ασθενών, ενώ οι ομομορφικοί αλγόριθμοι επιτρέπουν την ανάλυση των δεδομένων χωρίς να αποκαλύπτεται η πραγματική τους τιμή, διατηρώντας την ιδιωτικότητα των ασθενών (Telenti and Jiang 2020).

Με τη βοήθεια των αλγορίθμων μηχανικής μάθησης, οι επαγγελματίες της υγείας μπορούν να αναλύσουν τις ιατρικές καταγραφές, να αναγνωρίσουν τάσεις και να προβλέψουν πιθανές επιπλοκές, επιτρέποντας την πρόληψη και την έγκαιρη αντιμετώπιση. Επιπλέον, μπορούν να δημιουργήσουν προσαρμοσμένα πλάνα φροντίδας που να ανταποκρίνονται στις μοναδικές ανάγκες κάθε ασθενούς, βελτιώνοντας την ποιότητα της φροντίδας και την ικανοποίηση των ασθενών.

Η συνένωση αυτών των τεχνολογιών ανοίγει τον δρόμο για καινοτόμες εφαρμογές στην ιατρική φροντίδα, όπου η προσαρμοσμένη θεραπεία και η προστασία της ιδιωτικότητας των ασθενών συμβαδίζουν με την αποτελεσματικότητα και την ακρίβεια της ιατρικής ανάλυσης και διάγνωσης.

Δυνητικές εφαρμογές:

- Αυτόματη παρακολούθηση της υγείας των ατόμων με βάση τις προσωπικές τους ιατρικές καταγραφές και την πρόβλεψη πιθανών επιπλοκών.
- Ανάλυση προσωπικών ιατρικών καταγραφών για την αναγνώριση τάσεων και πιθανών παθήσεων που μπορεί να αντιμετωπιστούν προληπτικά.

- Δημιουργία προσαρμοσμένων πλάνων θεραπείας για κάθε ασθενή, βελτιώνοντας την ποιότητα και την αποτελεσματικότητα της φροντίδας.

- Εξατομικευμένη αναγνώριση και παρακολούθηση αντιδράσεων του οργανισμού σε θεραπευτικές παρεμβάσεις για τη βελτίωση της θεραπευτικής απόκρισης.

- Ανάπτυξη εξατομικευμένων προγραμμάτων πρόληψης για τη βελτίωση της υγείας, με βάση ατομικές ανάγκες και προσεγγίσεις.

7.1.3 Διαχείριση φαρμάκων και εφοδιαστικών αλυσίδων ιατρικών σκευασμάτων

Η διαχείριση φαρμάκων και οι εφοδιαστικές αλυσίδες ιατρικών σκευασμάτων αποτελούν κρίσιμους τομείς όπου η ακρίβεια, η ασφάλεια και η διαφάνεια των δεδομένων είναι ζωτικής σημασίας. Μέσω της τεχνολογίας blockchain, μπορεί να δημιουργηθεί ένα περιβάλλον το οποίο παρέχει εγγυήσεις για την ασφάλεια και το αμετάβλητο των δεδομένων, για την καταγραφή και παρακολούθηση των στοιχείων των φαρμάκων και των ιατρικών σκευασμάτων κατά μήκος της εφοδιαστικής αλυσίδας, εξασφαλίζοντας την αυθεντικότητα των προϊόντων και την τήρηση των κανονισμών.

Οι ομομορφικοί αλγόριθμοι επιτρέπουν την επεξεργασία δεδομένων χωρίς να διακυβεύεται η εμπιστευτικότητα των πληροφοριών, επιτρέποντας στους εμπειρογνώμονες του τομέα να αναλύσουν τις τάσεις της αγοράς, τις ανάγκες αποθέματος και άλλους σημαντικούς παράγοντες χωρίς να αποκαλύπτεται ευαίσθητη πληροφορία (Telenti and Jiang 2020).

Ταυτόχρονα, οι αλγόριθμοι μηχανικής μάθησης μπορούν να χρησιμοποιηθούν για την πρόβλεψη πιθανών διακυμάνσεων στη ζήτηση, τη βελτιστοποίηση των επιπέδων αποθέματος και την εξοικονόμηση πόρων κατά τη διαδικασία εφοδιασμού.

Συνδυάζοντας την τεχνολογία blockchain, τους ομομορφικούς αλγορίθμους και τη μηχανική μάθηση, οι φορείς του τομέα της υγείας μπορούν να αναπτύξουν πιο αποτελεσματικές και ασφαλείς εφοδιαστικές αλυσίδες, βελτιώνοντας την παράδοση των φαρμάκων και των ιατρικών σκευασμάτων, ενώ ταυτόχρονα διασφαλίζουν την ιδιωτικότητα και την ασφάλεια των δεδομένων (Telenti & Jiang, 2020).

Δυνητικές εφαρμογές:

- Ανάλυση τάσεων αγοράς και ανάγκες αποθέματος χωρίς αποκάλυψη ευαίσθητης πληροφορίας.

- Πρόβλεψη πιθανών διακυμάνσεων στη ζήτηση και βελτιστοποίηση επιπέδων αποθέματος.

- Διασφάλιση ιδιωτικότητας και ασφάλειας δεδομένων κατά τη διαχείριση φαρμάκων και εφοδιαστικών αλυσίδων ιατρικών σκευασμάτων.

7.1.4 Τηλεϊατρική και απομακρυσμένη παρακολούθηση ασθενών

Η τηλεϊατρική και η απομακρυσμένη παρακολούθηση ασθενών παρουσιάζουν νέες δυνατότητες για την παροχή φροντίδας υγείας, ενισχύοντας την πρόσβαση στις υπηρεσίες υγείας και παράλληλα διατηρώντας ή ακόμα και βελτιώνοντας την ποιότητα της φροντίδας. Ωστόσο, οι τεχνολογίες αυτές δημιουργούν τεράστιους όγκους δεδομένων, η διαχείριση των οποίων πρέπει να πραγματοποιείται με ασφάλεια και αποτελεσματικότητα (Telenti and Jiang 2020).

Στο πλαίσιο αυτό, το blockchain μπορεί να παράσχει μια ασφαλή και διαφανή πλατφόρμα για την αποθήκευση και διαχείριση των δεδομένων από συσκευές τηλεϊατρικής και αισθητήρες απομακρυσμένης παρακολούθησης. Κάθε δεδομένο που παράγεται μπορεί να καταγραφεί σε ένα αμετάβλητο ledger, το οποίο παρέχει εγγυήσεις για την ακεραιότητα και την αυθεντικότητα των δεδομένων.

Επιπλέον, οι ομομορφικοί αλγόριθμοι επιτρέπουν την επεξεργασία και ανάλυση των δεδομένων χωρίς να αποκαλύπτουν τις πραγματικές τιμές τους, υποστηρίζοντας τη διατήρηση της ιδιωτικότητας των ασθενών. Αυτό είναι ιδιαίτερα σημαντικό όταν τα δεδομένα περιλαμβάνουν ευαίσθητες ιατρικές πληροφορίες.

Τέλος, οι αλγόριθμοι μηχανικής μάθησης μπορούν να εφαρμοστούν στα κρυπτογραφημένα αυτά δεδομένα για την αναγνώριση μοτίβων, την πρόβλεψη εξελίξεων και την εξαγωγή ενημερωμένων ευρημάτων που μπορούν να ενημερώσουν τους επαγγελματίες της υγείας για την κατάσταση των ασθενών και να βοηθήσουν στην παροχή πιο ενημερωμένης και προσαρμοσμένης φροντίδας. Μέσω της αξιοποίησης της τεχνολογίας blockchain, των ομομορφικών αλγορίθμων και της μηχανικής μάθησης, η τηλεϊατρική και η απομακρυσμένη παρακολούθηση ασθενών μπορούν να καταστούν πιο ασφαλείς, αποτελεσματικές και αξιόπιστες, βελτιώνοντας την ποιότητα της φροντίδας υγείας που παρέχεται στους ασθενείς (Telenti and Jiang 2020).

Δυνητικές εφαρμογές:

- Αναγνώριση αλλαγών στα βιοσήματα ασθενών για την πρόβλεψη εξελίξεων στην υγεία τους.
- Αυτόματη ανίχνευση επειγόντων περιστατικών που αφορούν την κατάσταση της υγείας και αποστολή συναγερμών στους ιατρούς ή σε κέντρα επείγουσας φροντίδας.
- Παροχή εξατομικευμένων συμβουλών υγείας και θεραπείας με βάση τα συστήματα μηχανικής μάθησης.
- Αυτοματοποιημένη πρόβλεψη πιθανών παρενεργειών φαρμάκων με βάση τα ιστορικά δεδομένα και την ατομική αντίδραση των ασθενών.

7.2 Χρηματοπιστωτικός τομέας

7.2.1 Ασφαλής ανάλυση συναλλαγών

Στον χρηματοπιστωτικό τομέα, η ασφάλεια και η ιδιωτικότητα των δεδομένων είναι θεμελιώδεις παράγοντες που διασφαλίζουν την εμπιστοσύνη των πελατών και τη συμμόρφωση προς τους κανονισμούς. Η ασφαλής ανάλυση συναλλαγών επιτρέπει στις τράπεζες και τα χρηματοπιστωτικά ιδρύματα να ανιχνεύσουν απάτες, να ελέγξουν την νομιμότητα των συναλλαγών και να αξιολογήσουν τους συναλλακτικούς κινδύνους, διατηρώντας ταυτόχρονα την ιδιωτικότητα των εμπλεκομένων μερών.

Η τεχνολογία blockchain παρέχει μια ασφαλή και διαφανή πλατφόρμα για την αποθήκευση και τη διαχείριση των δεδομένων των συναλλαγών. Οι ομομορφικοί αλγόριθμοι, από την άλλη πλευρά, επιτρέπουν την επεξεργασία των δεδομένων αυτών χωρίς να αποκαλύπτεται η πραγματική τους τιμή, παρέχοντας ένα επιπλέον επίπεδο προστασίας για την ιδιωτικότητα. Αυτό καθιστά δυνατή την ανάλυση και την επεξεργασία των δεδομένων συναλλαγών για αναγνώριση ανωμαλιών ή απάτης, χωρίς να κινδυνεύει η ασφάλεια των πληροφοριών (Kou, et al. 2019).

Επιπλέον, η χρήση αλγορίθμων μηχανικής μάθησης μπορεί να ενισχύσει την ανάλυση συναλλαγών, ανακαλύπτοντας πιθανά πρότυπα και τάσεις που μπορεί να είναι δύσκολο να ανιχνευθούν με τις παραδοσιακές μεθόδους. Αυτό μπορεί να οδηγήσει σε πιο αποδοτικές και ασφαλείς χρηματοπιστωτικές υπηρεσίες, βελτιώνοντας την εμπειρία του πελάτη και την ανταγωνιστικότητα των χρηματοπιστωτικών οργανισμών στην ψηφιακή εποχή (Kou, et al. 2019).

Δυνητικές εφαρμογές:

- Πρόβλεψη κινδύνων σε συναλλαγές και αξιολόγηση της νομιμότητας συναλλαγών.
- Αυτόματη ανίχνευση ασυνήθιστων συμπεριφορών ή παραβάσεων στις χρηματοοικονομικές δραστηριότητες.
- Αυτόματη ανίχνευση απάτης σε χρηματοπιστωτικές συναλλαγές, μέσω ανάλυσης μοτίβων και ανωμαλιών.
- Ανάλυση τάσεων και προβλέψεις για τις μελλοντικές εξελίξεις στον χρηματοπιστωτικό τομέα με βάση τα δεδομένα των συναλλαγών.
- Προσαρμοσμένες χρηματοπιστωτικές υπηρεσίες βασισμένες στην ανάλυση των συναλλαγών και των προτιμήσεων των πελατών.

7.2.2 Έξυπνες Συμβάσεις για ασφαλείς χρηματοπιστωτικές συναλλαγές

Το σύγχρονο χρηματοπιστωτικό περιβάλλον απαιτεί υψηλού επιπέδου ασφάλεια, διαφάνεια και ταχύτητα στις συναλλαγές. Οι έξυπνες συμβάσεις (smart contracts) που εκτελούνται σε πλατφόρμες blockchain, μπορούν να αποτελέσουν έναν αξιόπιστο μηχανισμό για την αυτοματοποίηση και την εκτέλεση χρηματοπιστωτικών συναλλαγών, αυξάνοντας την ασφάλεια, τη διαφάνεια και την ταχύτητα των διαδικασιών.

Μέσω της χρήσης blockchain, οι έξυπνες συμβάσεις ενισχύουν την ταυτοποίηση και την επιβεβαίωση των συμβαλλομένων μερών, εξασφαλίζοντας την εκτέλεση των συναλλαγών όπως έχουν συμφωνηθεί. Η αυτοματοποίηση που προσφέρουν οι έξυπνες συμβάσεις μπορεί να μειώσει τις καθυστερήσεις και τα λάθη που συχνά συνδέονται με τις παραδοσιακές χρηματοπιστωτικές διαδικασίες, ενώ ταυτόχρονα διασφαλίζεται η συμμόρφωση με τους εφαρμοστέους κανονισμούς και τις νομοθετικές απαιτήσεις (Kou, et al. 2019).

Επιπλέον, οι ομομορφικοί αλγόριθμοι μπορούν να προσθέσουν ένα επιπλέον επίπεδο ασφάλειας, επιτρέποντας την επεξεργασία και την ανάλυση των δεδομένων που εμπεριέχονται στις συμβάσεις, χωρίς να κινδυνεύει η ιδιωτικότητα των εμπλεκομένων μερών. Αυτό μπορεί να είναι ιδιαίτερα χρήσιμο για την ανάλυση του ρίσκου και την βελτίωση των χρηματοπιστωτικών υπηρεσιών και προϊόντων, ενώ διατηρείται ένα υψηλό επίπεδο ασφάλειας και προστασίας των δεδομένων.

Δυνητικές εφαρμογές:

- Παροχή ασφαλών και διαφανών χρηματοοικονομικών συμβουλών με βάση την αυτόματη εκτέλεση έξυπνων συμβάσεων.
- Ανάλυση της συμπεριφοράς της αγοράς και πρόβλεψη τάσεων με βάση τα δεδομένα που ανακτώνται από έξυπνες συμβάσεις.

7.2.3 Ενιαία πλατφόρμα πληρωμών

Τον τελευταίο καιρό, η ανάγκη για πιο γρήγορες, πιο ασφαλείς και διαφανείς χρηματοπιστωτικές συναλλαγές έχει καταστεί έντονα αισθητή, ειδικά σε μια παγκοσμιοποιημένη οικονομία. Η δημιουργία ενιαίων πλατφορμών πληρωμών είναι ένα βήμα προς την κατεύθυνση αυτή, επιτρέποντας την άμεση και απρόσκοπτη διεκπεραίωση συναλλαγών μεταξύ διαφορετικών τραπεζικών και χρηματοπιστωτικών ιδρυμάτων.

Με την εφαρμογή της τεχνολογίας blockchain, είναι δυνατή η κατασκευή πλατφορμών που ενισχύουν τη διαφάνεια και την ασφάλεια των συναλλαγών, δημιουργώντας ένα αξιόπιστο ιστορικό που δεν μπορεί να τροποποιηθεί. Επιπλέον, η εφαρμογή ομομορφικών αλγορίθμων μπορεί να ενισχύσει την προστασία των δεδομένων των συναλλαγών, επιτρέποντας την επεξεργασία τους χωρίς να παρασχεθεί πρόσβαση στις πραγματικές τους τιμές (Kou, et al. 2019).

Από την άλλη πλευρά, η χρήση αλγορίθμων μηχανικής μάθησης μπορεί να βελτιώσει την αποδοτικότητα της πλατφόρμας, ανιχνεύοντας πιθανές απάτες, προβλέποντας τις συναλλαγματικές τάσεις και βελτιώνοντας την εμπειρία του χρήστη. Οι ενιαίες πλατφόρμες πληρωμών είναι ένα σημαντικό βήμα προς την κατεύθυνση της δημιουργίας ενός πιο αποτελεσματικού, ασφαλούς και διαφανούς χρηματοπιστωτικού συστήματος, που μπορεί να εξυπηρετήσει τις αυξανόμενες ανάγκες της ψηφιακής οικονομίας (Kou, et al. 2019).

Δυνητικές εφαρμογές:

- Πρόβλεψη των τάσεων συναλλαγματικών ισοτιμιών μέσω ανάλυσης των συναλλαγών και της συμπεριφοράς των χρηστών.
- Αυτοματοποιημένη ανίχνευση απάτης και ασφάλειας στις συναλλαγές μέσω αναγνώρισης ανωμαλιών στα πρότυπα συμπεριφοράς.
- Βελτίωση της εμπειρίας του χρήστη μέσω προσαρμοσμένων προτάσεων και εξατομικευμένων υπηρεσιών βάσει του ιστορικού συναλλαγών και των προτιμήσεων του.
- Αυτόματη πρόβλεψη και προσαρμογή των υπηρεσιών της πλατφόρμας σύμφωνα με τις ανάγκες και τις αλλαγές στο χρηματοοικονομικό περιβάλλον.

7.2.4 Αυτοματοποιημένοι χρηματοοικονομικοί σύμβουλοι

Στον χρηματοπιστωτικό τομέα, η παροχή εξατομικευμένων, ακριβών και έγκαιρων συμβουλών είναι κρίσιμη για τη διατήρηση της εμπιστοσύνης και της ικανοποίησης του πελάτη. Οι αυτοματοποιημένοι χρηματοοικονομικοί σύμβουλοι, που επωφελούνται από την τεχνολογία της μηχανικής μάθησης, μπορούν να αναλύσουν μεγάλους όγκους δεδομένων για να εντοπίσουν τις ανάγκες και τις προτιμήσεις των πελατών, προσφέροντας εξατομικευμένες συμβουλές και συστάσεις για τη διαχείριση των χρηματοοικονομικών τους (Kou, et al. 2019).

Η τεχνολογία blockchain παρέχει μια αξιόπιστη και ασφαλή πλατφόρμα για την αποθήκευση και τη διαχείριση των δεδομένων των πελατών, διασφαλίζοντας την προστασία της ιδιωτικότητας και την συμμόρφωση με τους ρυθμιστικούς κανονισμούς. Οι ομομορφικοί αλγόριθμοι επιτρέπουν την ασφαλή επεξεργασία των δεδομένων χωρίς την αποκάλυψη ευαίσθητων πληροφοριών, προσφέροντας εναλλακτικές για την προστασία των δεδομένων κατά τη διάρκεια της ανάλυσης.

Με την εφαρμογή αυτών των τεχνολογιών, οι χρηματοπιστωτικοί οργανισμοί μπορούν να αναπτύξουν αυτοματοποιημένους χρηματοοικονομικούς σύμβουλους που μπορούν να παρέχουν προσαρμοσμένες συμβουλές με βάση τις προτιμήσεις και τις χρηματοοικονομικές συνθήκες του κάθε πελάτη. Αυτό μπορεί να βελτιώσει την εμπειρία του πελάτη, αυξάνοντας την αποτελεσματικότητα των χρηματοοικονομικών συστάσεων και βελτιώνοντας την επιτυχία των χρηματοπιστωτικών στρατηγικών των πελατών (Kou, et al. 2019).

Δυνητικές εφαρμογές:

- Ανάλυση του οικονομικού προφίλ κάθε πελάτη για την προσαρμογή επενδυτικών προτάσεων.
- Αυτόματη παρακολούθηση της αγοράς για την ανίχνευση επενδυτικών ευκαιριών ή επικείμενων απειλών.
- Εξατομικευμένες συμβουλές για τη βελτιστοποίηση του χρηματοπιστωτικού προγράμματος ή του χαρτοφυλακίου κάθε πελάτη βάσει των ατομικών στόχων και συνθηκών.
- Παροχή αυτοματοποιημένων συμβουλών για την αντιμετώπιση οικονομικών δυσκολιών ή αλλαγών στην κατάσταση του πελάτη.

7.3 Εφοδιαστική αλυσίδα

7.3.1 Προβλεπτική ανάλυση και βελτιστοποίηση διεργασιών

Η προβλεπτική ανάλυση και βελτιστοποίηση διεργασιών στον τομέα της εφοδιαστικής αλυσίδας είναι κρίσιμης σημασίας για την αποτελεσματικότητα και την αξιοπιστία της αλυσίδας. Οι αλγόριθμοι Μηχανικής Μάθησης μπορούν να αξιοποιήσουν τα δεδομένα που είναι αποθηκευμένα σε περιβάλλοντα Blockchain για τη διεξαγωγή προβλεπτικής ανάλυσης και να εξάγουν πολύτιμες πληροφορίες για τις διεργασίες της αλυσίδας εφοδιασμού (Carbonneau, Laframboise and Vahidov 2008).

Οι αλγόριθμοι Μηχανικής Μάθησης μπορούν να αναλύσουν τα ιστορικά δεδομένα της αλυσίδας εφοδιασμού, όπως οι χρόνοι παράδοσης, οι καθυστερήσεις, οι αποθέματα, και τα επίπεδα ζήτησης, για να προβλέψουν τυχόν καθυστερήσεις ή ανωμαλίες που μπορεί να εμφανιστούν στο μέλλον. Με τη βοήθεια των προβλέψεων αυτών, οι επιχειρήσεις μπορούν να λάβουν εγκαίρως μέτρα για την αποφυγή ή την ελαχιστοποίηση των προβλημάτων, ενισχύοντας έτσι την αποτελεσματικότητα της αλυσίδας.

Παράλληλα, η ανάλυση των μοτίβων κίνησης των προϊόντων και η παρακολούθηση των διεργασιών σε πραγματικό χρόνο μπορούν να βοηθήσουν στη βελτιστοποίηση των επιχειρηματικών διεργασιών. Οι αλγόριθμοι ML μπορούν να αναλύσουν τα δεδομένα αυτά για να εντοπίσουν τυχόν βελτιστοποιήσεις που μπορούν να γίνουν στις διαδρομές εφοδιασμού, στην αποθήκευση, στη διαχείριση των αποθεμάτων, ή ακόμη και στην πρόβλεψη της ζήτησης, επιτρέποντας έτσι την καλύτερη διαχείριση των πόρων και τη μείωση του κόστους (Carbonneau, Laframboise and Vahidov 2008).

Ο συνδυασμός των πληροφοριών από το Blockchain, που παρέχει ακεραιότητα και διαφάνεια, με τις προβλεπτικές ικανότητες των αλγορίθμων Μηχανικής Μάθησης, ανοίγει νέους ορίζοντες για τη βελτιστοποίηση των εφοδιαστικών αλυσίδων και την εξασφάλιση της συνεχούς βελτίωσης των διεργασιών τους.

Δυνητικές εφαρμογές:

- Πρόβλεψη χρόνου παράδοσης και διαχείριση καθυστερήσεων στις μεταφορές εμπορευμάτων.
- Ανάλυση των επιπέδων ζήτησης για προϊόντα και προβλέψεις για μελλοντική ζήτηση.
- Βελτιστοποίηση διαδρομών και αποθηκευτικών χώρων για μείωση κόστους και βελτίωση χρόνων παράδοσης.
- Αυτόματη πρόταση βελτιστοποιημένων στρατηγικών διανομής και αποθήκευσης βάσει των προβλέψεων και των αλλαγών στην αγορά.

7.3.2 Διαφάνεια και εντοπισμός προέλευσης

Στον τομέα της εφοδιαστικής αλυσίδας, η διαφάνεια και η ακριβής εντοπισμός της προέλευσης των προϊόντων είναι κρίσιμες για την αξιοπιστία της αλυσίδας, την ασφάλεια των προϊόντων και την εμπιστοσύνη των καταναλωτών. Η τεχνολογία blockchain προσφέρει μια σταθερή πλατφόρμα για την καταγραφή και την παρακολούθηση των δεδομένων προέλευσης, παρέχοντας εγγυήσεις για το αμετάβλητο και εξασφαλίζοντας τη διαφάνεια.

Χρησιμοποιώντας το blockchain, κάθε φάση της αλυσίδας εφοδιασμού, από την παραγωγή μέχρι τη διανομή και την πώληση, μπορεί να καταγραφεί και να επικυρωθεί σε ένα αμετάβλητο ηλεκτρονικό αποθετήριο. Οι πληροφορίες αυτές μπορούν να περιλαμβάνουν λεπτομέρειες όπως ο τόπος παραγωγής, οι χρονικές στιγμές μεταφοράς και παράδοσης, οι συνθήκες αποθήκευσης και πολλά άλλα. Αυτό επιτρέπει την παροχή μιας πλήρους εικόνας της πορείας του προϊόντος σε όλη τη διάρκεια της αλυσίδας εφοδιασμού (Carbonneau, Laframboise and Vahidov 2008).

Οι επιχειρήσεις και οι καταναλωτές μπορούν επίσης να αποκτήσουν πρόσβαση σε αυτές τις πληροφορίες για να επιβεβαιώσουν την αυθεντικότητα και την ποιότητα των προϊόντων. Οι ελεγκτικοί φορείς και οι ρυθμιστικές αρχές μπορούν επίσης να χρησιμοποιήσουν τα δεδομένα αυτά για να διασφαλίσουν τη συμμόρφωση με τους κανονισμούς και τις προδιαγραφές.

Με τον τρόπο αυτό, η τεχνολογία blockchain συμβάλλει σημαντικά στη διαφάνεια και στον εντοπισμό της προέλευσης των προϊόντων, ενισχύοντας την αξιοπιστία των εφοδιαστικών αλυσίδων και προσφέροντας μια ισχυρή βάση για την ανάπτυξη και τη βελτίωση των διεργασιών τους (Carbonneau, Laframboise and Vahidov 2008).

Δυνητικές εφαρμογές:

- Πλήρης ιχνηλασιμότητα των προϊόντων κατά μήκος όλης της αλυσίδας εφοδιασμού, συμπεριλαμβανομένης της παραγωγής, μεταφοράς και διανομής.
- Εξασφάλιση της αυθεντικότητας και της ποιότητας των προϊόντων για επιχειρήσεις και καταναλωτές μέσω πρόσβασης σε πληροφορίες προέλευσης.
- Χρήση των δεδομένων για ελέγχους από αρμόδιους φορείς και ρυθμιστικές αρχές.
- Παροχή πλήρους εικόνας της διαδρομής του προϊόντος σε κάθε στάδιο της αλυσίδας εφοδιασμού για βελτίωση των διαδικασιών.

- Ενίσχυση της αξιοπιστίας των εφοδιαστικών αλυσίδων και εντοπισμός πιθανών προβλημάτων στο σύστημα παραγωγής και διανομής.

7.3.3 Ασφαλής κοινοποίηση δεδομένων

Η ασφαλής κοινοποίηση δεδομένων είναι ένα κρίσιμο στοιχείο στην αλυσίδα εφοδιασμού, ειδικά όταν πρόκειται για συνεργασίες μεταξύ διάφορων εταιρειών και φορέων. Οι ομομορφικοί αλγόριθμοι παρέχουν τη δυνατότητα για την ανάλυση και επεξεργασία δεδομένων χωρίς την ανάγκη αποκάλυψης της πραγματικής τους τιμής, διασφαλίζοντας έτσι την ιδιωτικότητα και την ασφάλεια των εμπλεκομένων μερών.

Σε ένα περιβάλλον Blockchain, τα δεδομένα μπορούν να κοινοποιηθούν με ασφάλεια σε όλους τους ενδιαφερόμενους φορείς της αλυσίδας εφοδιασμού, ενώ ταυτόχρονα διατηρούνται οι απαραίτητες εγγυήσεις ιδιωτικότητας και εμπιστευτικότητας. Οι ομομορφικοί αλγόριθμοι επιτρέπουν την επεξεργασία των δεδομένων αυτών για την εξαγωγή χρήσιμων εισόδων, χωρίς την αποκάλυψη ευαίσθητων πληροφοριών που μπορεί να υπονομεύσει την ανταγωνιστικότητα ή τη συμμόρφωση με τους κανονισμούς (Carbonneau, Laframboise and Vahidov 2008).

Αυτό μπορεί να είναι ιδιαίτερα χρήσιμο σε σενάρια όπου οι εταιρείες ή οι φορείς επιθυμούν να αναλύσουν κοινά δεδομένα για τη βελτίωση της απόδοσης της αλυσίδας εφοδιασμού, αλλά χωρίς να κινδυνεύουν την αποκάλυψη εμπιστευτικών ή ανταγωνιστικών πληροφοριών. Με αυτόν τον τρόπο, η ασφαλής κοινοποίηση δεδομένων μέσω ομομορφικών αλγορίθμων ενισχύει την συνεργασία και την αμοιβαία ωφέλεια μεταξύ των φορέων της αλυσίδας εφοδιασμού, διευκολύνοντας την ανταλλαγή γνώσεων και την κοινή βελτίωση των διεργασιών (Carbonneau, Laframboise and Vahidov 2008).

Δυνητικές εφαρμογές:

- Ανάλυση κοινοποιημένων δεδομένων για τη βελτίωση της απόδοσης και της αποτελεσματικότητας της αλυσίδας εφοδιασμού.
- Πρόβλεψη τάσεων και ανίχνευση ανωμαλιών στην αλυσίδα εφοδιασμού με βάση τα κοινοποιημένα δεδομένα.
- Ανάλυση δεδομένων για τη βελτίωση της διαχείρισης αποθεμάτων και την εξοικονόμηση πόρων.
- Αυτόματη πρόβλεψη και αντίδραση σε πιθανές διακυμάνσεις της αγοράς ή των απαιτήσεων των πελατών.
- Ανάπτυξη κοινών στρατηγικών και βέλτιστων πρακτικών μεταξύ των συνεργαζόμενων φορέων της αλυσίδας εφοδιασμού.

7.3.4 Αυτοματοποιημένη εκτέλεση συμβάσεων

Η αυτοματοποιημένη εκτέλεση συμβάσεων μέσω των έξυπνων συμβολαίων στην τεχνολογία blockchain ανοίγει νέες προοπτικές για τον τομέα των εφοδιαστικών αλυσίδων. Τα έξυπνα συμβόλαια είναι αυτόνομα προγράμματα που εκτελούνται όταν συμπληρώνονται συγκεκριμένοι όροι και συνθήκες, επιτρέποντας την αυτόματη εκτέλεση συμβάσεων χωρίς την ανάγκη για τρίτους διαμεσολαβητές (Carbonneau, Laframboise and Vahidov 2008).

Στο πλαίσιο της αλυσίδας εφοδιασμού, τα έξυπνα συμβόλαια μπορούν να διαχειριστούν τις συμφωνίες μεταξύ των διαφόρων φορέων, όπως προμηθευτές, μεταφορικές εταιρείες και λιανοπωλητές, εξασφαλίζοντας την τήρηση των όρων των συμβάσεων, όπως οι χρόνοι παράδοσης, η ποιότητα των προϊόντων και οι πληρωμές. Με την εκτέλεση των συμβάσεων αυτών αυτόματα, οι επιχειρήσεις μπορούν να μειώσουν τον κίνδυνο των ανθρωπίνων λαθών, τις καθυστερήσεις και τα πρόσθετα κόστη που συνδέονται με την παραδοσιακή διαχείριση συμβάσεων.

Επιπλέον, η διαφάνεια και η ακεραιότητα των δεδομένων που παρέχεται από το blockchain εξασφαλίζει την εμπιστοσύνη μεταξύ των εμπλεκομένων μερών, καθώς όλες οι συμβάσεις και οι συναλλαγές καταγράφονται ανεξίτηλα στην αλυσίδα μπλοκ, προσφέροντας ένα αμετάκλητο ιστορικό των συμφωνιών (Carbonneau, Laframboise and Vahidov 2008).

Τέλος, η χρήση των ομομορφικών αλγορίθμων μπορεί να ενισχύσει περαιτέρω την ασφάλεια και την ιδιωτικότητα των δεδομένων κατά τη διάρκεια της εκτέλεσης των έξυπνων συμβάσεων, επιτρέποντας την ασφαλή κοινοποίηση και ανάλυση των δεδομένων χωρίς να αποκαλύπτονται ευαίσθητες πληροφορίες.

Δυνητικές εφαρμογές:

- Αυτόματη διαχείριση των χρόνων παράδοσης και των όρων πληρωμής μεταξύ προμηθευτών και εταιρειών μεταφορών.
- Αυτόματη εκκίνηση των διαδικασιών ελέγχου ποιότητας για τα προϊόντα κατά την παράδοση.
- Αυτόματη αποζημίωση σε περίπτωση καθυστέρησης ή παραβίασης των συμβατικών όρων.
- Αυτόματη διαχείριση επιστροφών και αντικαταστάσεων προϊόντων σύμφωνα με τους όρους σύμβασης.
- Αυτόματη καταγραφή και αντιμετώπιση προβλημάτων στην αλυσίδα εφοδιασμού, όπως απώλειες ή ζημιές κατά τη μεταφορά.

7.4 Δημόσια Διοίκηση

7.4.1 Αυτοματοποιημένη διαχείριση υπηρεσιών

Η αυτοματοποιημένη διαχείριση υπηρεσιών αποτελεί έναν σημαντικό τομέα όπου οι τεχνολογίες blockchain και οι αλγόριθμοι μηχανικής μάθησης μπορούν να συνεισφέρουν σημαντικά. Στο πλαίσιο της δημόσιας διοίκησης, η αξιοπιστία, η αποδοτικότητα και η διαφάνεια έχουν αυξημένη σημασία για την αποτελεσματική παροχή υπηρεσιών στους πολίτες (Anastasopoulos and Whitford 2019).

Οι έξυπνες συμβάσεις που εκτελούνται σε πλατφόρμες blockchain μπορούν να αυτοματοποιήσουν πολλές διαδικασίες, όπως η εκχώρηση πόρων, η επιβεβαίωση της πληρωμής για τις υπηρεσίες και η επικύρωση των συναλλαγών. Αυτό μπορεί να επιφέρει μείωση των διοικητικών επιβαρύνσεων και τη βελτίωση της εμπειρίας των πολιτών. Επιπλέον, οι έξυπνες συμβάσεις μπορούν να διασφαλίσουν ότι οι διαδικασίες είναι διαφανείς και διεξάγονται σύμφωνα με τους κανονισμούς και τις πολιτικές της δημόσιας διοίκησης (Anastasopoulos and Whitford 2019).

Από την άλλη πλευρά, οι αλγόριθμοι μηχανικής μάθησης μπορούν να εφαρμοστούν για την ανάλυση των δεδομένων που παράγονται και αποθηκεύονται στο blockchain, προκειμένου να βελτιωθεί η

αποδοτικότητα των υπηρεσιών. Για παράδειγμα, η προβλεπτική ανάλυση μπορεί να βοηθήσει τις δημόσιες αρχές να αναγνωρίσουν τα μοτίβα χρήσης των υπηρεσιών και να αναπροσαρμόσουν τους πόρους ανάλογα, ενώ η ανάλυση σε πραγματικό χρόνο μπορεί να παρέχει στιγμιαία ανατροφοδότηση για τη βελτίωση της απόκρισης σε αλλαγές στη ζήτηση (Anastasopoulos and Whitford 2019).

Σε αυτό το πλαίσιο, οι ομομορφικοί αλγόριθμοι μπορούν να προσφέρουν ένα επιπλέον επίπεδο ασφάλειας και προστασίας της ιδιωτικότητας, επιτρέποντας την ανάλυση και την επεξεργασία των δεδομένων χωρίς να αποκαλύπτεται ευαίσθητη πληροφορία. Αυτό είναι ιδιαίτερα σημαντικό σε τομείς όπως η δημόσια διοίκηση, όπου η προστασία των δεδομένων των πολιτών είναι κρίσιμης σημασίας (Anastasopoulos and Whitford 2019).

Δυνητικές εφαρμογές:

- Αυτοματοποίηση διαδικασιών εκχώρησης πόρων και πιστοποίησης πληρωμών για τις δημόσιες υπηρεσίες.
- Προβλεπτική ανάλυση για την αναγνώριση μοτίβων χρήσης των υπηρεσιών και την αναπροσαρμογή των πόρων της δημόσιας διοίκησης ανάλογα.
- Ανάλυση σε πραγματικό χρόνο για την παροχή στιγμιαίας ανατροφοδότησης και βελτίωσης της απόκρισης σε αλλαγές στη ζήτηση υπηρεσιών.
- Αυτοματοποιημένη παρακολούθηση και εκτέλεση συμβάσεων για εξασφάλιση διαφάνειας και συμμόρφωσης με τους κανονισμούς.
- Προστασία της ιδιωτικότητας μέσω της εφαρμογής ομομορφικών αλγορίθμων για την ανάλυση και επεξεργασία δεδομένων χωρίς αποκάλυψη ευαίσθητης πληροφορίας.

7.4.2 Διαφάνεια και ελεγχόμενη απόδοση

Η ελεγχόμενη απόδοση[9] στο πλαίσιο της δημόσιας διοίκησης αναφέρεται στην αξιολόγηση και τον έλεγχο της αποτελεσματικότητας, της αποδοτικότητας και της ποιότητας των δημοσίων υπηρεσιών και πολιτικών. Αυτό περιλαμβάνει την παρακολούθηση και την ανάλυση της επίδοσης των δημοσίων οργανισμών, την αξιολόγηση της σχέσης κόστους-οφέλους των δημοσίων προγραμμάτων, και τη διαφάνεια στην αναφορά και την επικοινωνία των αποτελεσμάτων προς το κοινό και άλλους ενδιαφερόμενους φορείς (Zervopoulos and Palaskas 2010).

Τόσο η διαφάνεια όσο και η ελεγχόμενη απόδοση είναι κεντρικές έννοιες για την αποτελεσματικότητα και την αξιοπιστία της δημόσιας διοίκησης. Οι τεχνολογίες blockchain μπορούν να υποστηρίξουν αυτές τις διαστάσεις παρέχοντας ένα αποθετήριο για την καταγραφή όλων των συναλλαγών και των διεργασιών, το οποίο προσφέρει εγγυήσεις διαφάνειας και μη μεταβολής. Αυτό μπορεί να επιτρέψει στους πολίτες και στις ενδιαφερόμενες ομάδες να ελέγχουν τη διαχείριση των δημόσιων πόρων και την εκτέλεση των δημόσιων πολιτικών με ανοιχτό και διαφανή τρόπο (Anastasopoulos and Whitford 2019).

[9] Αφορά την αξιολόγηση και τη μέτρηση της αποδοτικότητας, της αποτελεσματικότητας και της αποδοτικότητας στη Δημόσια Διοίκηση, και πιο συγκεκριμένα στην ικανότητα ενός οργανισμού να επιτυγχάνει προκαθορισμένους στόχους. Οι μετρήσεις αυτές αποτελούν αναγκαίο υπόβαθρο για την περαιτέρω επιδίωξη των στόχων της διαφάνειας, της οικονομίας και της λογοδοσίας.

Επιπλέον, η εφαρμογή των αλγορίθμων μηχανικής μάθησης μπορεί να βοηθήσει τις δημόσιες αρχές να αξιολογούν και να βελτιώνουν συνεχώς την απόδοση των υπηρεσιών. Μέσω της ανάλυσης των δεδομένων που καταγράφονται στο blockchain, είναι δυνατή η ανίχνευση των περιθωρίων βελτίωσης, η ανάδειξη των καλύτερων πρακτικών και η αντιμετώπιση των προκλήσεων που αντιμετωπίζουν οι δημόσιες υπηρεσίες.

Στο πλαίσιο αυτό, οι ομομορφικοί αλγόριθμοι μπορούν να διαδραματίσουν καίριο ρόλο στην εξασφάλιση της ιδιωτικότητας και της ασφάλειας των δεδομένων κατά τη διάρκεια της ανάλυσης, επιτρέποντας την εξαγωγή χρήσιμων πληροφοριών χωρίς την αποκάλυψη ευαίσθητων στοιχείων. Αυτό επιτρέπει την ολοκληρωμένη ανάλυση της απόδοσης των δημόσιων υπηρεσιών με τρόπο που σέβεται την ιδιωτικότητα των πολιτών και την εμπιστευτικότητα των δεδομένων, προσφέροντας ταυτόχρονα ένα ανοιχτό και ελεγχόμενο πλαίσιο για την εξέλιξη των δημοσίων υπηρεσιών.

Δυνητικές εφαρμογές:

- Παρακολούθηση και αξιολόγηση της απόδοσης των δημόσιων οργανισμών μέσω ανάλυσης δεδομένων blockchain.
- Αξιολόγηση σχέσης κόστους-οφέλους των δημοσίων προγραμμάτων.
- Ενίσχυση της διαφάνειας και της ελεγχόμενης απόδοσης μέσω της καταγραφής όλων των συναλλαγών και διεργασιών.
- Ανίχνευση περιθωρίων βελτίωσης και αντιμετώπιση προκλήσεων στις δημόσιες υπηρεσίες μέσω ανάλυσης δεδομένων blockchain και εφαρμογής μηχανικής μάθησης.

7.4.3 Εξατομικευμένη διαχείριση κοινωνικής πρόνοιας

Η εξατομικευμένη διαχείριση κοινωνικής πρόνοιας είναι ένας σημαντικός τομέας για την ενίσχυση της κοινωνικής ευημερίας. Οι τεχνολογίες blockchain και οι αλγόριθμοι μηχανικής μάθησης έχουν το δυναμικό να προωθήσουν αυτή την προσέγγιση, επιτρέποντας μια πιο εξατομικευμένη και αποτελεσματική διαχείριση των πόρων της κοινωνικής πρόνοιας.

Μέσω της ανάλυσης των δεδομένων που είναι αποθηκευμένα σε πλατφόρμες blockchain, οι δημόσιες αρχές μπορούν να αποκτήσουν βαθύτερη κατανόηση των αναγκών και των προτιμήσεων των δικαιούχων. Οι αλγόριθμοι μηχανικής μάθησης μπορούν να εφαρμοστούν για την ανάλυση των δεδομένων αυτών, προκειμένου να εντοπιστούν τα μοτίβα και να προταθούν στρατηγικές για την καλύτερη κατανομή των πόρων. Αυτό μπορεί να περιλαμβάνει, για παράδειγμα, την αυτόματη αναγνώριση των ατόμων που χρειάζονται περισσότερη υποστήριξη ή την προσαρμοσμένη διανομή των διαθέσιμων πόρων με βάση τις ανάγκες.

Οι ομομορφικοί αλγόριθμοι, από την άλλη πλευρά, προσφέρουν ένα επιπλέον επίπεδο προστασίας της ιδιωτικότητας, επιτρέποντας την ασφαλή επεξεργασία των δεδομένων χωρίς να αποκαλύπτεται ευαίσθητη πληροφορία. Αυτό είναι ιδιαίτερα σημαντικό σε τομείς όπως η κοινωνική πρόνοια, όπου η προστασία των προσωπικών δεδομένων είναι κρίσιμης σημασίας. Συνεπώς, οι δημόσιες αρχές μπορούν να αναλύσουν και να διαχειριστούν τα δεδομένα με ασφάλεια, εξασφαλίζοντας την ιδιωτικότητα και την ακεραιότητα των πληροφοριών, ενώ ταυτόχρονα βελτιώνουν την παροχή των υπηρεσιών κοινωνικής πρόνοιας (Anastasopoulos and Whitford 2019).

Δυνητικές εφαρμογές:

- Ανάλυση δεδομένων για την αυτόματη αναγνώριση ατόμων που χρειάζονται περισσότερη υποστήριξη στον τομέα της κοινωνικής πρόνοιας.
- Πρόβλεψη των αναγκών των δικαιούχων για τη βελτιστοποίηση της κατανομής πόρων κοινωνικής πρόνοιας.
- Αυτόματη κατανομή πόρων βάσει των αναγκών των δικαιούχων για μεγαλύτερη αποτελεσματικότητα στη διαχείριση της κοινωνικής πρόνοιας.
- Αναγνώριση μοτίβων και τάσεων από τα δεδομένα για την ανάπτυξη προσαρμοσμένων προγραμμάτων υποστήριξης.

7.4.4 Ψηφιακές εκλογές και ψηφοφορίες

Οι ψηφιακές εκλογές και ψηφοφορίες είναι τομείς που έχουν τη δυνατότητα να επωφεληθούν σημαντικά από τις τεχνολογίες blockchain, ομομορφικών αλγορίθμων και μηχανικής μάθησης. Το blockchain μπορεί να προσφέρει μια ασφαλή, διαφανή και αμετάβλητη πλατφόρμα για την καταγραφή και την αποθήκευση των ψήφων, ενώ εγγυάται την ακεραιότητα των δεδομένων κατά τη διάρκεια της διαδικασίας.

Οι ομομορφικοί αλγόριθμοι επιτρέπουν την επεξεργασία των δεδομένων ψηφοφορίας χωρίς να αποκαλύπτεται η ταυτότητα του ψηφοφόρου ή η ψήφος του, διασφαλίζοντας την ιδιωτικότητα και την ανωνυμία. Αυτό είναι ιδιαίτερα σημαντικό για τη διασφάλιση όπως εμπιστοσύνης του κοινού στο εκλογικό σύστημα.

Από την άλλη πλευρά, οι αλγόριθμοι μηχανικής μάθησης μπορούν να αναπτυχθούν για να εντοπίσουν και να προλάβουν πιθανές προσπάθειες απάτης ή επίθεσης στο σύστημα ψηφοφορίας, όπως η διπλοψηφία ή η παραποίηση των αποτελεσμάτων. Η ανάλυση των δεδομένων σε πραγματικό χρόνο και η ανίχνευση ασυνήθιστων μοτίβων μπορεί να συμβάλλει στην αποτελεσματική αντιμετώπιση των προβλημάτων πριν αυτά επηρεάσουν την ακεραιότητα και τη διαφάνεια της διαδικασίας (Anastasopoulos and Whitford 2019).

Μέσω αυτών των τεχνολογιών, οι δημόσιες αρχές μπορούν να ενθαρρύνουν την ευρύτερη συμμετοχή των πολιτών στις δημοκρατικές διαδικασίες, προσφέροντας μια πιο ασφαλή, διαφανή και προσβάσιμη πλατφόρμα για τη ψηφοφορία και την εκλογική διαδικασία.

Δυνητικές εφαρμογές:

- Προστασία της ανωνυμίας των ψηφοφόρων και της εμπιστοσύνης στη διαδικασία ψηφοφορίας μέσω ασφαλούς αποθήκευσης των ψήφων σε πλατφόρμα blockchain.
- Ανίχνευση προσπαθειών απάτης ή επιθέσεων στο εκλογικό σύστημα μέσω ανάλυσης δεδομένων σε πραγματικό χρόνο και ανίχνευσης ασυνήθιστων μοτίβων.
- Αυτόματη αντιμετώπιση πιθανών προβλημάτων στο εκλογικό σύστημα πριν αυτά επηρεάσουν την ακεραιότητα και τη διαφάνεια της διαδικασίας.

- Ενίσχυση της ευρύτερης συμμετοχής των πολιτών στις δημοκρατικές διαδικασίες μέσω μιας ασφαλούς, διαφανούς και προσβάσιμης πλατφόρμας ηλεκτρονικής ψηφοφορίας.

7.5 Ενέργεια

7.5.1 Έξυπνα δίκτυα ενέργειας

Τα Έξυπνα Δίκτυα Ενέργειας αποτελούν μια προηγμένη προσέγγιση στη διαχείριση και τη διανομή της ενέργειας, προσφέροντας έναν αυτοματοποιημένο και ευέλικτο τρόπο για την αντιμετώπιση των ενεργειακών αναγκών. Η ενσωμάτωση της τεχνολογίας blockchain σε αυτά τα δίκτυα μπορεί να ενισχύσει την αξιοπιστία, τη διαφάνεια και την ασφάλεια των συναλλαγών και των δεδομένων. Επιπλέον, η χρήση αλγορίθμων Μηχανικής Μάθησης μπορεί να βελτιώσει την αποδοτικότητα και την ευελιξία των δικτύων αυτών (Chen, et al. 2019).

Μέσω της τεχνολογίας blockchain, είναι δυνατή η δημιουργία αξιόπιστων πλατφορμών για τη διαχείριση των ενεργειακών πόρων, παρέχοντας αποθετήριο για την καταγραφή του ιστορικού των συναλλαγών και της κατανάλωσης ενέργειας, το οποίο παρέχει εγγυήσεις για το αμετάβλητο των δεδομένων. Έτσι καθίσταται δυνατή η άμεση επικοινωνία και η πραγματοποίηση συναλλαγών μεταξύ των παραγωγών και των καταναλωτών ενέργειας, καθώς και η αυτοματοποίηση της τιμολόγησης και της χρέωσης βάσει πραγματικής κατανάλωσης.

Επιπλέον, η χρήση αλγορίθμων Μηχανικής Μάθησης μπορεί να επιτρέψει την ανάλυση των δεδομένων των δικτύων ενέργειας για την πρόβλεψη της ζήτησης, την αποφυγή ενεργειακών απωλειών και τη βελτιστοποίηση της παραγωγής και της κατανομής ενέργειας. Αυτό μπορεί να συμβάλει στην εξοικονόμηση πόρων και στην ελαχιστοποίηση των εκπομπών ρύπων (Chen, et al. 2019).

Συνολικά, η συνένωση της τεχνολογίας blockchain με τους αλγορίθμους Μηχανικής Μάθησης μπορεί να προσφέρει καινοτόμες λύσεις για τη δημιουργία αποδοτικότερων, αξιόπιστων και βιώσιμων έξυπνων δικτύων ενέργειας, ενισχύοντας την ενεργειακή διαχείριση στον κόσμο του αύριο.

Δυνητικές εφαρμογές:

- Πρόβλεψη ζήτησης ενέργειας βάσει ιστορικών δεδομένων και τάσεων κατανάλωσης.
- Βελτιστοποίηση διανομής ενέργειας με βάση την πραγματική κατανάλωση και τις προβλεπόμενες ανάγκες.
- Αυτόματη προσαρμογή της παραγωγής ενέργειας σε πραγματική κατανάλωση και διαθεσιμότητα πηγών.
- Ελαχιστοποίηση ενεργειακών απωλειών μέσω βελτιστοποίησης των προγραμματισμένων συντηρήσεων.
- Αυτόματη προσαρμογή των τιμών και της χρέωσης βάσει της πραγματικής κατανάλωσης και της προσφοράς ενέργειας.

7.5.2 Προστασία ιδιωτικότητας για αναλύσεις δεδομένων

Η ανάλυση δεδομένων αποτελεί κρίσιμο στοιχείο για την ενεργειακή βιομηχανία, καθώς μέσω αυτής είναι δυνατή η ανίχνευση τάσεων και προβλημάτων, και η βελτιστοποίηση των ενεργειακών

συστημάτων. Ωστόσο, η προστασία της ιδιωτικότητας των δεδομένων είναι ζωτικής σημασίας, ειδικά όταν πρόκειται για δεδομένα παραγωγής και κατανάλωσης ενέργειας που μπορεί να αποκαλύψουν ευαίσθητες πληροφορίες για τις εταιρείες ή τους καταναλωτές (Chen, et al. 2019).

Οι ομομορφικοί αλγόριθμοι αποτελούν ένα σημαντικό εργαλείο για την αντιμετώπιση αυτών των προκλήσεων, παρέχοντας τη δυνατότητα εκτέλεσης αναλύσεων και υπολογισμών επάνω σε κρυπτογραφημένα δεδομένα, χωρίς να απαιτείται η αποκρυπτογράφησή τους. Αυτό σημαίνει ότι τα δεδομένα παραμένουν ασφαλή και προστατευμένα κατά τη διάρκεια της ανάλυσης, ενώ ταυτόχρονα εξασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των αποτελεσμάτων (Chen, et al. 2019).

Στο πεδίο της ενέργειας, οι ομομορφικοί αλγόριθμοι μπορούν να επιτρέψουν την ασφαλή ανάλυση των δεδομένων παραγωγής και κατανάλωσης, καθιστώντας δυνατή την εξαγωγή σημαντικών ευρημάτων και την ανάπτυξη στρατηγικών για βελτιστοποίηση χωρίς να κινδυνεύει η ιδιωτικότητα των εμπλεκόμενων φορέων. Αυτό αποτελεί ένα σημαντικό βήμα προς την κατεύθυνση της ενίσχυσης της ασφάλειας και της εμπιστοσύνης στις ενεργειακές υποδομές, ενώ ταυτόχρονα διευκολύνεται η αξιοποίηση της αναλυτικής ικανότητας της Μηχανικής Μάθησης για την ανάπτυξη πιο αποδοτικών και αειφόρων ενεργειακών συστημάτων.

Δυνητικές εφαρμογές:

- Ανώνυμη ανάλυση καταναλωτικών προτιμήσεων για βελτίωση της προσφοράς ενέργειας.
- Ανάπτυξη αναλυτικών μοντέλων για τη βελτιστοποίηση της ενεργειακής απόδοσης.
- Πρόβλεψη τάσεων και αναγνώριση πιθανών προβλημάτων στην παραγωγή ενέργειας με βάση ανώνυμες αναλύσεις δεδομένων.
- Προστασία της ιδιωτικότητας κατά την ανάλυση δεδομένων παραγωγής και κατανάλωσης ενέργειας.

7.5.3 Προληπτική συντήρηση

Ο τομέας της προληπτικής συντήρησης αποκτά ιδιαίτερη σημασία στο πλαίσιο των ενεργειακών δικτύων, καθώς η έγκαιρη ανίχνευση και επιδιόρθωση βλαβών μπορεί να συμβάλλει σημαντικά στην αποφυγή διακοπών και στην εξοικονόμηση πόρων. Οι αλγόριθμοι Μηχανικής Μάθησης, μέσω της ανάλυσης των δεδομένων που συλλέγονται και αποθηκεύονται σε περιβάλλοντα blockchain, μπορούν να διαδραματίσουν κεντρικό ρόλο σε αυτήν την προσπάθεια (Chen, et al. 2019).

Συγκεκριμένα, οι αλγόριθμοι Μηχανικής Μάθησης μπορούν να αναλύσουν τα μοτίβα και τις τάσεις στα δεδομένα λειτουργίας των ενεργειακών συστημάτων, προβλέποντας πιθανές βλάβες ή ανάγκες για συντήρηση πριν αυτές προκαλέσουν σοβαρά προβλήματα. Είτε πρόκειται για φθορές σε εξαρτήματα, είτε για απροσδόκητες αλλαγές στην απόδοση, η προληπτική ανάλυση μπορεί να επιτρέψει την έγκαιρη επέμβαση και την αποφυγή δαπανηρών επισκευών ή ακόμη και αποτυχιών (Chen, et al. 2019).

Επιπλέον, το blockchain προσφέρει ένα περιβάλλον για την αποθήκευση και διαχείριση των δεδομένων που απαιτούνται για αυτούς τους ελέγχους, το οποίο παρέχει εγγυήσεις ασφάλειας και διαφάνειας. Η ακεραιότητα και η προσβασιμότητα των δεδομένων είναι κρίσιμης σημασίας για την επιτυχή εφαρμογή των στρατηγικών προληπτικής συντήρησης, και η τεχνολογία blockchain μπορεί

να προσφέρει μια αξιόπιστη λύση για τη διαχείριση αυτών των προκλήσεων, εξασφαλίζοντας την ασφάλεια, την ακεραιότητα και την ιδιωτικότητα των ενεργειακών δεδομένων.

Δυνητικές εφαρμογές:

- Πρόβλεψη πιθανών αστοχιών ή φθορών σε εξαρτήματα ενεργειακών συστημάτων.
- Αυτόματη ανίχνευση απροσδόκητων αλλαγών στην απόδοση των ενεργειακών συστημάτων.
- Πρόβλεψη της ανάγκης για συντήρηση ή αντικατάσταση εξαρτημάτων πριν από την εμφάνιση προβλημάτων.
- Ανάλυση μοτίβων και τάσεων στη λειτουργία των ενεργειακών συστημάτων για τη βελτιστοποίηση της προληπτικής συντήρησης.

7.5.4 Βελτιστοποίηση ενεργειακής απόδοσης

Η βελτιστοποίηση της ενεργειακής απόδοσης είναι ιδιαίτερα σημαντική για την επίτευξη των στόχων σε επίπεδο ενεργειακής αποδοτικότητας και μείωσης των εκπομπών. Οι αλγόριθμοι Μηχανικής Μάθησης, όταν συνδυάζονται με την τεχνολογία blockchain, μπορούν να παίξουν κρίσιμο ρόλο στην επίτευξη αυτών των στόχων (Chen, et al. 2019).

Μέσω του blockchain, είναι δυνατή η καταγραφή και αποθήκευση των δεδομένων κατανάλωσης και παραγωγής ενέργειας, παρέχοντας εγγυήσεις για την ασφάλεια και τη διαφάνεια, και υποστηρίζοντας τη δημιουργία ενός ιστορικού που δεν δύναται να αλλοιωθεί, το οποίο μπορεί να αξιοποιηθεί για αναλύσεις και βελτιστοποιήσεις. Οι αλγόριθμοι Μηχανικής Μάθησης μπορούν να εξετάσουν αυτά τα δεδομένα για να αναγνωρίσουν τάσεις και πρότυπα κατανάλωσης, επιτρέποντας την προσαρμογή των στρατηγικών παραγωγής και διανομής ενέργειας (Chen, et al. 2019).

Με την εφαρμογή προηγμένων αναλυτικών τεχνικών, είναι δυνατή η πρόβλεψη της ζήτησης ενέργειας, η αποφυγή πλεονασμάτων και η βελτιστοποίηση των υφιστάμενων ενεργειακών πόρων. Αυτό μπορεί να συμβάλει στην εξοικονόμηση ενέργειας και τη μείωση του λειτουργικού κόστους.

Συνολικά, η συνεργασία της τεχνολογίας blockchain με τη Μηχανική Μάθηση προσφέρει μια προοπτική για τη δημιουργία πιο αποδοτικών και αειφόρων ενεργειακών συστημάτων, καθώς και για την ενίσχυση της ενεργειακής ασφάλειας και αποδοτικότητας σε έναν κόσμο με αυξανόμενες ενεργειακές ανάγκες.

Δυνητικές εφαρμογές:

- Πρόβλεψη της ζήτησης ενέργειας βάσει ιστορικών δεδομένων και τάσεων κατανάλωσης.
- Ανίχνευση και πρόβλεψη ενεργειακών πλεονασμάτων μέσω αναλύσεων δεδομένων παραγωγής και κατανάλωσης ενέργειας.
- Αυτόματη προσαρμογή παραγωγής και διανομής ενέργειας με βάση προβλέψεις και προσδιορισμό των αναγκών.
- Βελτιστοποίηση της απόδοσης ενεργειακών πόρων με τη χρήση προηγμένων αναλυτικών τεχνικών.

8 Συμπεράσματα

Στην παρούσα εργασία εξετάστηκε η αξιοποίηση των αποθηκευμένων δεδομένων σε περιβάλλοντα Blockchain από εφαρμογές αλγορίθμων Μηχανικής Μάθησης. Μέσα από την εξερεύνηση των διαφόρων τεχνολογικών και κρυπτογραφικών στοιχείων, καθώς και των προκλήσεων και ευκαιριών που προκύπτουν, διαφαίνεται ότι η αξιοποίηση των δεδομένων που έχουν αποθηκευθεί σε περιβάλλοντα blockchain από εφαρμογές αλγορίθμων Μηχανικής Μάθησης μπορεί να αναδειχθεί μια σειρά από τεχνολογικές συμβολές και δυνατότητες. Καταρχάς, το Blockchain προσφέρει μια πλατφόρμα για την αποθήκευση δεδομένων η οποία παρέχει εγγυήσεις διαφάνειας και μη τροποποίησης, προσφέροντας στις εφαρμογές Μηχανικής Μάθησης τη δυνατότητα να έχουν πρόσβαση σε αξιόπιστα δεδομένα για την εκπαίδευσή τους και τον μετέπειτα υπολογισμό προβλέψεων. Η συνδυαστική χρήση των τεχνολογιών Blockchain και ομομορφικής κρυπτογραφίας μπορεί να επιτρέψει την επεξεργασία των δεδομένων χωρίς να αποκαλύπτεται η πραγματική τους τιμή, ενισχύοντας την προστασία των προσωπικών δεδομένων.

Επιπλέον, η δυνατότητα εκτέλεσης αλγορίθμων Μηχανικής Μάθησης επί κρυπτογραφημένων δεδομένων σε ένα Blockchain μπορεί να ανοίξει νέους δρόμους για την επεξεργασία και ανάλυση δεδομένων. Με την ενσωμάτωση αυτών των αλγορίθμων, τα Blockchain μπορούν να επωφεληθούν από αυτοματοποιημένες αναλύσεις και βελτιώσεις, οδηγώντας σε αυξημένη αποτελεσματικότητα και απόδοση.

Η επιτυχής σύνδεση των διάφορων τεχνολογικών πλαισίων και βιβλιοθηκών που αφορούν την Μηχανική Μάθηση και το Blockchain μπορεί να αυξήσει τη διασυνδεσιμότητα και την ενσωμάτωση διαφόρων τεχνολογιών, ενώ παράλληλα δημιουργεί ευκαιρίες για καινοτομία σε διάφορους τομείς, όπως η υγεία, ο χρηματοπιστωτικός τομέας, οι εφοδιαστικές αλυσίδες, η δημόσια διοίκηση και ο τομέας της ενέργειας.

Τέλος, η ικανότητα της Μηχανικής Μάθησης να ανακαλύψει κρυμμένες σχέσεις και μοτίβα μέσα από τα δεδομένα του blockchain μπορεί να οδηγήσει σε βελτιωμένες επιδόσεις και νέες ευκαιρίες.

8.1 Κοινωνικές και οικονομικές επιπτώσεις

Η αξιοποίηση των αποθηκευμένων δεδομένων σε περιβάλλοντα Blockchain μέσω εφαρμογών αλγορίθμων Μηχανικής Μάθησης ανοίγει νέους ορίζοντες για την ανάπτυξη εφαρμογών, οι οποίες έχουν επιπτώσεις τόσο στον κοινωνικό όσο και στον οικονομικό τομέα.

Το Blockchain, με την αρχιτεκτονική του στη διαχείριση δεδομένων, προσφέρει ένα επίπεδο διαφάνειας και ασφάλειας που είναι ζωτικής σημασίας για πολλές εφαρμογές. Από την άλλη πλευρά, οι αλγόριθμοι Μηχανικής Μάθησης επιτρέπουν την εξόρυξη γνώσης και την ανάκτηση χρήσιμων πληροφοριών από τα δεδομένα αυτά. Στον χρηματοπιστωτικό τομέα, για παράδειγμα, η εν λόγω τεχνολογική σύνθεση μπορεί να βελτιώσει την ασφάλεια των συναλλαγών, την ανάλυση των ρίσκων και την απόδοση των υπηρεσιών. Στον τομέα της υγείας, η αξιοποίηση των δεδομένων Blockchain μπορεί να προσφέρει προστατευμένη πλατφόρμα για την ανταλλαγή ιατρικών δεδομένων, ενώ οι αλγόριθμοι Μηχανικής Μάθησης μπορούν να βοηθήσουν στην ανάλυση των δεδομένων αυτών για καλύτερη διάγνωση και θεραπεία.

Επιπλέον, στη δημόσια διοίκηση όπου η διαφάνεια των διαδικασιών είναι ιδιαίτερης σημασίας, η τεχνολογία αυτή μπορεί να συμβάλει στην αυτοματοποίηση των διοικητικών διαδικασιών και στην

παροχή πιο διαφανών και αποδοτικών υπηρεσιών. Επίσης, οι οικονομικές επιπτώσεις της συνδυαστικής αξιοποίησης της τεχνολογίας Blockchain και Μηχανικής Μάθησης είναι επίσης σημαντικές.

Με τη βελτίωση της αποδοτικότητας και της ασφάλειας στις επιχειρηματικές διεργασίες, μπορεί να αυξηθεί η εμπιστοσύνη των επενδυτών και των καταναλωτών, και με τη σειρά τους να δημιουργηθούν νέες επιχειρηματικές ευκαιρίες και αγορές. Επιπλέον, με την επίλυση τεχνικών προβλημάτων και προκλήσεων, υπάρχει το δυναμικό για σημαντικές εξοικονομήσεις κόστους και βελτιωμένη υπηρεσιακή παροχή σε διάφορους τομείς της οικονομίας.

Σε γενικές γραμμές, η συνδυαστική χρήση των τεχνολογιών Blockchain και Μηχανικής Μάθησης προσφέρει μια προοπτική για μια πιο ασφαλή, διαφανή και αποδοτική κοινωνία και οικονομία, καθιστώντας την εξερεύνηση και την ανάπτυξη αυτής της τεχνολογικής σύνθεσης ένα σημαντικό πεδίο για μελλοντική έρευνα και καινοτομία.

8.2 Μελλοντικές διερευνήσεις

Η αξιοποίηση των δεδομένων που αποθηκεύονται σε περιβάλλοντα Blockchain μέσω εφαρμογών αλγορίθμων Μηχανικής Μάθησης αναδεικνύει ένα εξαιρετικά ενδιαφέρον και εποικοδομητικό πεδίο για μελλοντική έρευνα. Στον κόσμο όπου η ποσότητα των δεδομένων αυξάνεται εκθετικά, η δυνατότητα εξόρυξης γνώσης από αυτά τα δεδομένα σε ένα ασφαλές και διαφανές πλαίσιο είναι πολύτιμη. Η υβριδική αυτή τεχνολογική συνάντηση μπορεί να επιτρέψει την ανάπτυξη νέων εφαρμογών και λύσεων για πολλές βιομηχανίες και τομείς της κοινωνίας.

Στο πεδίο της Μηχανικής Μάθησης, η πρόσβαση και η ανάλυση των δεδομένων αποτελούν τον πυρήνα για την εξαγωγή χρήσιμων πληροφοριών και γνώσεων. Ωστόσο, σε εποχές όπου η προστασία των προσωπικών δεδομένων και η ασφάλεια των πληροφοριών έχουν προχωρήσει στο προσκήνιο, η δυνατότητα επεξεργασίας δεδομένων με παράλληλη διασφάλιση των δικαιωμάτων αυτών έχει αποκτήσει αυξημένο ενδιαφέρον. Αυτό είναι ιδιαίτερα σημαντικό σε περιβάλλοντα blockchain, όπου τα δεδομένα αποθηκεύονται με ασφαλή τρόπο και διατηρούνται κρυπτογραφημένα για να εξασφαλίσουν την ακεραιότητα και την ασφάλειά τους.

Η ανάπτυξη αλγορίθμων Μηχανικής Μάθησης που μπορούν να λειτουργήσουν αποδοτικά σε κρυπτογραφημένα δεδομένα αποτελεί μια εκ των σημαντικών προκλήσεων στον τομέα αυτό. Αυτό σημαίνει ότι οι αλγόριθμοι πρέπει να είναι σε θέση να εκτελούν υπολογισμούς και να εξάγουν συμπεράσματα από τα δεδομένα χωρίς να απαιτείται η αποκρυπτογράφηση τους, πράγμα που θα μπορούσε να εκθέσει τα δεδομένα σε κινδύνους. Η επίτευξη αυτού του στόχου θα συνεισφέρει σημαντικά στην προώθηση της ασφάλειας και της ιδιωτικότητας στην επεξεργασία δεδομένων, δύο παράγοντες που έχουν κεντρική σημασία για την ευρύτερη αποδοχή και εφαρμογή των τεχνολογιών Blockchain.

Πέραν τούτου, η εξερεύνηση των δυνατοτήτων που προσφέρουν οι ομομορφικοί αλγόριθμοι κρυπτογράφησης αποτελεί έναν άλλον σημαντικό τομέα έρευνας. Οι ομομορφικοί αλγόριθμοι κρυπτογράφησης επιτρέπουν την εκτέλεση υπολογισμών επάνω σε κρυπτογραφημένα δεδομένα χωρίς αποκρυπτογράφηση, και η συνένωσή τους με τεχνικές μηχανικής μάθησης μπορεί να ανοίξει νέους ορίζοντες για την επεξεργασία και ανάλυση δεδομένων σε περιβάλλοντα blockchain. Η ενσωμάτωση των ομομορφικών αλγορίθμων κρυπτογράφησης με αλγορίθμους Μηχανικής Μάθησης μπορεί να οδηγήσει σε πιο αποδοτικές και ασφαλείς τεχνικές επεξεργασίας δεδομένων, ενισχύοντας

την αξία και την αξιοπιστία των πληροφοριών που προκύπτουν από την ανάλυση των δεδομένων blockchain.

Όπως έχει αναφερθεί, η τεχνολογία blockchain, με την ικανότητά της να παρέχει διαφάνεια, ασφάλεια και ανεξαρτησία, αναδεικνύεται ως μια πρωτοποριακή πλατφόρμα για τη διαχείριση δεδομένων. Σε αυτό το πλαίσιο, η ανάπτυξη προτύπων και πλαισίων που επιτρέπουν την αποτελεσματική διαχείριση και αξιοποίηση των δεδομένων blockchain γίνεται ένας σημαντικός τομέας έρευνας. Αυτά τα πρότυπα και τα πλαίσια πρέπει να είναι σε θέση να υποστηρίξουν την αποτελεσματική ανάλυση και επεξεργασία των δεδομένων, ενώ ταυτόχρονα διατηρούν τα υψηλά επίπεδα ασφάλειας και προστασίας της ιδιωτικότητας που παρέχει η τεχνολογία blockchain.

Επιπρόσθετα, η δυνατότητα συνδυασμού της τεχνολογίας blockchain με αλγορίθμους Μηχανικής Μάθησης ανοίγει νέους ορίζοντες για τη δημιουργία καινοτόμων εφαρμογών και λύσεων που ανταποκρίνονται στις ανάγκες της σύγχρονης κοινωνίας. Οι εφαρμογές αυτές μπορούν να κυμαίνονται από την ενίσχυση της ασφάλειας στις διαδικασίες διαχείρισης δεδομένων, μέχρι την ανάπτυξη προηγμένων αναλυτικών εργαλείων που μπορούν να παράγουν ενδεικτικές πληροφορίες και να διευκολύνουν τη λήψη αποφάσεων βασισμένων σε δεδομένα.

Μέσα από την ανάπτυξη νέων εφαρμογών και λύσεων, ο συνδυασμός των τεχνολογιών blockchain και Μηχανικής Μάθησης μπορεί να επιτρέψει την ανάπτυξη πιο σύνθετων και εξελιγμένων συστημάτων, που θα είναι σε θέση να αντιμετωπίσουν πολυδιάστατα προβλήματα και να παράγουν λύσεις που είναι συνδεδεμένες με τις πραγματικές ανάγκες της κοινωνίας. Είτε πρόκειται για τη βελτίωση της διαφάνειας στις χρηματοπιστωτικές συναλλαγές, είτε για την ενίσχυση της ασφάλειας των δεδομένων στον τομέα της υγείας, οι εφαρμογές αυτές μπορούν να παράγουν σημαντικά οφέλη για την κοινωνία στο σύνολό της.

Η αυξανόμενη εφαρμογή των τεχνολογιών blockchain και Μηχανικής Μάθησης αναδεικνύει μια σειρά από ηθικές, νομικές και κοινωνικές προκλήσεις που απαιτούν προσεκτική αξιολόγηση και διερεύνηση. Η συνένωση αυτών των τεχνολογιών, παρόλο που υπόσχεται σημαντικά οφέλη σε θέματα ασφάλειας και αποδοτικότητας επεξεργασίας δεδομένων, φέρει επίσης τον κίνδυνο κατάχρησης ή ακόμη και παραβίασης της ιδιωτικότητας και άλλων ατομικών δικαιωμάτων.

Στο ηθικό πλαίσιο, η διαφάνεια και η ευθύνη κατά την επεξεργασία δεδομένων είναι ζωτικής σημασίας. Είναι απαραίτητο να κατανοηθεί πώς και γιατί τα δεδομένα υπόκεινται σε επεξεργασία, , ποιος έχει πρόσβαση σε αυτά και ποιες είναι οι πιθανές επιπτώσεις της ανάλυσης αυτών των δεδομένων. Επίσης, είναι κρίσιμο να αναπτυχθούν μηχανισμοί που θα επιτρέπουν την εποπτεία και τον έλεγχο των εφαρμογών Μηχανικής Μάθησης πάνω σε περιβάλλοντα blockchain, για να διασφαλίσουν την ακεραιότητα και τη διαφάνεια των διεργασιών.

Νομικά, η ρύθμιση της χρήσης και της διαχείρισης των δεδομένων blockchain είναι ένα πεδίο που απαιτεί αυξημένη προσοχή. Η διασφάλιση της συμμόρφωσης με τις νομικές και κανονιστικές απαιτήσεις, συμπεριλαμβανομένης της προστασίας των προσωπικών δεδομένων, είναι απαραίτητη για την αποδοχή και την εφαρμογή των τεχνολογιών αυτών σε ευρύτερη κλίμακα.

Κοινωνικά, η κατανόηση και η αποδοχή των τεχνολογιών αυτών από το κοινό είναι ζωτικής σημασίας. Η ενημέρωση και η εκπαίδευση του κοινού σχετικά με τα οφέλη, τις προκλήσεις και τις πιθανές επιπτώσεις της αξιοποίησης των δεδομένων blockchain σε εφαρμογές Μηχανικής Μάθησης

είναι κεντρικής σημασίας για την ενίσχυση της κοινωνικής αποδοχής και της εμπιστοσύνης σε αυτές τις τεχνολογίες.

Η ανάπτυξη κατευθυντήριων γραμμών και πολιτικών που θα παρέχουν εγγυήσεις για την ασφαλή και υπεύθυνη χρήση των τεχνολογιών blockchain και Μηχανικής Μάθησης αποτελεί μια αναγκαιότητα για το μέλλον της αξιοποίησης των δεδομένων αυτών. Μέσω της διεξαγωγής εκτενών διαβουλεύσεων μεταξύ των ενδιαφερόμενων μερών, των ρυθμιστικών αρχών, των ερευνητών και των κοινοτήτων των χρηστών, μπορεί να διαμορφωθεί ένα πλαίσιο που θα επιτρέπει την ανάπτυξη και την υλοποίηση των τεχνολογιών αυτών με τρόπο που σέβεται τις αξίες και τα πρότυπα σε ηθικό, νομικό και κοινωνικό επίπεδο.

9 Βιβλιογραφία

Abubakar, Adamu, Shehu Jabaka, Bello Idrith Tijjani, Akram Zeki, Haruna Chiroma, Mohammed Joda Usman, Shakirat Raji, and Murni Mahmud. 2014. "Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: issues and challenges." *Journal of Theoretical and Applied Information Technology*, June.

Acar, Abbas, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. 2018. "A Survey on Homomorphic Encryption Schemes: Theory and Implementation." *ACM Computing Surveys*, January: 1-35. doi:10.1145/3214303.

Ali, Aitizaz, Muhammad Fermi Pasha, Jehad Ali, Ong Huey Fang, Mehedi Masud, Anca Delia Jurcut, and Mohammed A. Alzain. 2022. "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography." *Sensors*, January. doi:10.3390/s22020528.

Al-Sabaawi, Aiman. 2022. "Cryptanalysis of Block Cipher: Method Implementation." *2022 IEEE International Conference for Advancement in Technology (ICONAT 2022).* Goa, India. doi:10.1109/ICONAT53423.2022.9726054.

Anastasopoulos, Lefteris Jason, and Andrew B. Whitford. 2019. "Machine Learning for Public Administration Research, With Application to Organizational Reputation." *Journal of Public Administration Research and Theory*, June: 491-510. doi:10.1093/jopart/muy060.

Armknecht, Frederik, Colin Boyd, Christopher Carr, Kristian Gjøsteen, Angela Jäschke, Christian A. Reuter, and Martin Strand. 2015. "A Guide to Fully Homomorphic Encryption." *Cryptology ePrint Archive*, 1192. https://eprint.iacr.org/2015/1192.

Ayodele, Taiwo Oladipupo. 2010. "Types of Machine Learning Algorithms." In *New Advances in Machine Learning*. doi:10.5772/9385.

Bauer, Craig. 2021. *Secret history: The story of cryptology (second edition).* New York: CRC Press. doi:10.1201/9781315162539 .

Bendlin, Rikke, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. 2011. *Semi-homomorphic encryption and multiparty computation.* Accessed 10 14, 2023. https://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_11.pdf.

Bhanot, Rajdeep, and Rahul Hans. 2015. "A Review and Comparative Analysis of Various Encryption Algorithms." *International Journal of Security and Its Applications*, 289-306. doi:10.14257/ijsia.2015.9.4.27.

Bradford, Deanna. 2023. "Microsoft Azure and ConsenSys Quorum Blockchain Service: Using blockchain to enable companies to apply the SDGs." *Global studies*, March 23: 51-63.

Brenner, Michael P., Jan Wiebelitz, Gabriele von Voigt, and Matthew Smith. 2011. *Secret program execution in the cloud applying homomorphic encryption.* Accessed 10 14, 2023. http://ieeexplore.ieee.org/document/5936608.

Britannica, The Editors of Encyclopaedia. 2024. *Enigma - German code device.* Encyclopedia Britannica, April 19. https://www.britannica.com/topic/Enigma-German-code-device.

Cao, Xiaolin, Ciara Moore, Maire O'Neill, Neil Hanley, and Elizabeth O'Sullivan. 2014. *High-Speed Fully Homomorphic Encryption Over the Integers.* Accessed 10 14, 2023. https://pure.qub.ac.uk/portal/files/17845079/high_speed_fhe_over_the_integers_cameraready.pdf.

Carbonneau, Réal André, Kevin Laframboise, and Rustam Vahidov. 2008. "Application of machine learning techniques for supply chain demand forecasting." *European Journal of Operational Research*, February: 1140-1154. doi:10.1016/j.ejor.2006.12.004.

Chen, Mingzhe, Ursula Challita, Walid Saad, Changchuan Yin, and Mérouane Debbah. 2019. "Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial." *IEEE Communications Surveys & Tutorials*, July 3: 3039-3071. doi:10.1109/COMST.2019.2926625.

Chillotti, Ilaria, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. 2018. "TFHE: Fast Fully Homomorphic Encryption over the Torus." *Journal of Cryptology.* https://eprint.iacr.org/2018/421.

Chow, Jerry, Oliver Dial, and Jay Gambetta. 2021. "IBM Quantum breaks the 100-qubit processor barrier." *IBM Research Blog*, November 16. https://www.ibm.com/quantum/blog/127-qubit-quantum-processor-eagle?social_post=5922928345&linkId=140353937.

Cohen, Fred. 1990-1995. *A Short History of Cryptography.* Fred Cohen &Associates. Accessed October 11, 2023. https://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf.

Cord, Matthieu, and Pádraig Cunningham. 2008. "Machine Learning Techniques for Multimedia: Case Studies on Organization and Retrieval." *Cognitive Technologies*, January. doi:10.1007/978-3-540-75171-7.

Cunningham, P.´, M. Cord, and S.J. Delany. 2008. "Supervised Learning." In *Machine Learning Techniques for Multimedia. Cognitive Technologies*, by M. Cord and P. Cunningham, 21–49. Berlin, Heidelberg: Springer. doi:https://doi.org/10.1007/978-3-540-75171-7_2.

Dara, Sashank. 2013. *Cryptography Challenges for Computational Privacyin Public Clouds.* Accessed 10 14, 2023. https://eprint.iacr.org/2013/272.pdf.

Dooley, John F. 2018. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms.* Springer-VerlagISBN. https://www.researchgate.net/publication/330503278_History_of_Cryptography_and_Cryptanalysis_Codes_Ciphers_and_Their_Algorithms.

Filatovas, Ernestas, Marco Marcozzi, Leonardo Mostarda, and Remigijus Paulavičius. 2022. "A MCDM-based framework for blockchain consensus protocol selection." *2022Expert Systems with Applications ,* October. doi:10.1016/j.eswa.2022.117609.

Gobeyn, Sacha, Ans M. Mouton, Anna Cord, Andrea Kaim, Martin Volk, and Peter Goethals. 2019. "Evolutionary algorithms for species distribution modelling: A review in the context of

machine learning." *Ecological Modelling*, January: 179-195. doi:10.1016/j.ecolmodel.2018.11.013.

Henry, Kevin. 2008. *The Theory and Applications of Homomorphic Cryptography.* Waterloo, Ontario: Thesis presented to the University of Waterloo. https://uwspace.uwaterloo.ca/bitstream/handle/10012/3901/uw-ethesis.pdf?sequence=1.

Heron, Simon. 2009. "Encryption: Advanced Encryption Standard (AES)." *Network Security*, 8-12. doi:10.1016/S1353-4858(10)70006-4.

Hussain, S. M. Suhail, Shaik Mullapathi Farooq, and Taha Selim Ustun. 2019. "Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security." *IEEE Access* , June. doi:10.1109/ACCESS.2019.2923728.

Johnson , Matthew, Michael Jones, Mark Shervey, Joel T. Dudley, and Noah Zimmerman. 2019. "Building a Secure Biomedical Data Sharing Decentralized App (DApp): Tutorial." *2019Journal of Medical Internet Research*, October. doi:10.2196/13601 .

Jordan, Michael, and T. M. Mitchell. 2015. "Machine Learning: Trends, Perspectives, and Prospects." *Science*, 255-260. doi:10.1126/science.aaa8415.

Joux, Antoine, and Kim Nguyen. 2003. "Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups." *Journal of Cryptology*, September: 239-247. doi:10.1007/s00145-003-0052-4.

Kaelbling, Leslie Pack, Michael L. Littman, and Andrew W. Moore. 1996. "Reinforcement Learning: A survey." *Journal of Artificial Intelligence Research*, May: 237–285. doi:10.1613/jair.301.

Kapoor, Vivek, Vivek Sonny Abraham, and Ramesh Singh. 2008. "Elliptic curve cryptography." *Ubiquity*, May: 1-8. doi:10.1145/1378355.1378356.

Katz, Jonathan, and Yehuda Lindell. 2007. *Introduction to modern cryptography.* CRC Press.

Komalavalli, C., Deepika Saxena, and Chetna Laroiya. 2020. "Overview of Blockchain Technology Concepts." In *Handbook of Research on Blockchain Technology*, by Saravanan Krishnan, Valentina E. Balas, E. Golden Julie, Y. Harold Robinson, S. Balaji and Raghvendra Kumar, 349–371. Academic Press.

Kotsiantis, S. B., I. D. Zaharakis, and P. E. Pintelas. 2007. "Machine learning: a review of classification and combining techniques." *Informatica*, November: 249-268. doi:10.1007/s10462-007-9052-3.

Kou, Gang, Xiangrui Chao, Yi Peng, and Fawaz Alsaadi. 2019. "Machine learning methods for systemic risk analysis in financial sectors." *Technological and Economic Development of Economy*, May: 1-27. doi:10.3846/tede.2019.8740.

Krupitzer, Christian, and Anthony Stein. 2021. "Food Informatics - Review of the Current State-of-the-Art, Revised Definition, and Classification into the Research Landscape." *Foods* , November. doi:10.3390/foods10112889.

Liu, Yiming, F. Richard Yu, Xi Li, Hong Ji, and Victor C. M. Leung. 2020. "Blockchain and Machine Learning for Communications and Networking Systems." *IEEE Communications Surveys & Tutorials* , February: 1392-1431. doi:10.1109/COMST.2020.2975911.

Maulud, Dastan, and Adnan M. Abdulazeez. 2020. "A Review on Linear Regression Comprehensive in Machine Learning." *Journal of Applied Science and Technology Trends*, December: 140-147. doi:10.38094/jastt1457.

McGregor, Anthony, Mark Hall, Perry Lorier, and James Brunskill. 2004. "Flow Clustering Using Machine Learning Techniques." *Passive and Active Network Measurement.* Berlin: Springer. 205-214. doi:10.1007/978-3-540-24668-8_21.

Meier, A. 2005. "The elgamal cryptosystem." *Joint Advanced Students Seminar*.

Mitchell, Tom M. 1997. *Machine Learning.* The Mc-Graw-Hill Companies, Inc. Accessed 10 14, 2023. https://www.cs.cmu.edu/~tom/mlbook.html.

Mololoth, Vidya Krishnan, Saguna Saguna, and Christer Åhlund. 2022. "Blockchain and Machine Learning for Future Smart Grids: A Review." *Energies*, November. doi:10.3390/en16010528.

Moore, Ciara, Maire O'Neill, Elizabeth O'Sullivan, Yarkin Doröz, and Berk Sunar. 2014. “Practical homomorphic encryption: A survey.” *2014 IEEE International Symposium on Circuits and Systems (ISCAS).* Melbourne, VIC, Australia: IEEE. 2792-2795. Accessed 10 14, 2023. doi:10.1109/ISCAS.2014.6865753.

Moore, Ciara, Máire O'Neill, Elizabeth O'Sullivan, Yarkin Doroz, and Berk Sunar. 2014. "Practical homomorphic encryption: A survey." *IEEE International Symposium on Circuits and Systems (ISCAS).* IEEE. 2792-2795. doi:10.1109/ISCAS.2014.6865753.

Muhammad, S. J., H. Chiroma, and M. Mahmud. 2014. "Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: issues and challenges." *J Theor Appl Inf Technol* 61 (1).

Naser, S. M. 2021. "Cryptography: From the ancient history to now, it’s applications and a new complete numerical model." *International Journal of Mathematics and Statistics Studies*, pp.11-30. https://www.eajournals.org/wp-content/uploads/Cryptography.pdf.

Nicolaou, Nicolas. 2017. *Implementation and performance evaluation of cryptographic algorithms.* Latsia: Master Thesis, Open University of Cyprus. http://hdl.handle.net/11128/3088.

NIST. 1992. *The digital signature standard.* Vol. 35. New York, NY: Association for Computing Machinery. doi:10.1145/129902.129904.

Penard, Wouter, and Tim van Werkhoven. 2008. "On the Secure Hash Algorithm." *Cryptography in context*, January: 1-18. https://blog.infocruncher.com/resources/ethereum-whitepaper-annotated/On%20the%20Secure%20Hash%20Algorithm%20family%20(2008).pdf.

Rosenblatt, Frank. 1958. "The perceptron: a probabilistic model for information storage and organization in the brain." *Psychology Review*, November: 386-408. doi:10.1037/H0042519.

Russell, Stuart, and Peter Norvig. 2010. *Artificial Intelligence - A Modern Approach.* 3rd edition. Pearson Education, Inc.

Schaefer, Edward. 2009. *An introduction to cryptography and Cryptanalysis.* https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6915fc636cf3b9c14f86fe7d12116f3bb1fc648d.

Sen, Jaydip. 2013. "Homomorphic Encryption - Theory and Application." In *Theory and Practice of Cryptography and Network Security Protocols and Technologies*, by Jaydip Sen. Accessed 10 14, 2023. doi:10.5772/56687.

Sharma, Dilip Kumar, Ningthoujam Chidananda Singh, Daneshwari Ashok Noola, Amala Nirmal Doss, and Janaki Sivakumar. 2021. "A review on various cryptographic techniques & algorithms." *Materials Today Proceedings*, May. doi:10.1016/j.matpr.2021.04.583.

Sharma, Shivani, and Yash Gupta. 2017. "Study on Cryptography and Techniques." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 249-252. doi:10.32628/CSEIT172150.

Simmons, Gustavus J. 2023. *Cryptology.* Encyclopaedia Britannica, October 11. Accessed October 14, 2023. https://www.britannica.com/topic/cryptology.

Telenti, Amalio, and Xiaoqian Jiang. 2020. "Treating medical data as a durable asset." *Nature Genetics*, September. doi: 10.1038/s41588-020-0698-y.

The Editors of Encyclopædia Britannica. 2023. *Enigma - German code device.* Encyclopaedia Britannica, October 13. Accessed October 20, 2023. https://www.britannica.com/topic/Enigma-German-code-device.

Tutorials Point India Private Limited. n.d. *Cryptography Tutorial.* Tutorials Point. Accessed 10 10, 2023. https://www.tutorialspoint.com/cryptography/index.htm.

Usama, Muhammad, Junaid Qadir, Aunn Raza, Hunain Arif, Kok-Lim Alvin Yau, Yehia Elkhatib, Amir Hussain, and Ala Al-Fuqaha. 2017. "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges." *IEEE Access* , September: 65579-65615. doi:10.1109/ACCESS.2019.2916648.

Vaikuntanathan, Vinod. 2011. *Computing Blindfolded: New Developments in Fully Homomorphic Encryption.* Accessed 10 14, 2023. http://cs.toronto.edu/~vinodv/fhe-focs-survey.pdf.

Varatharajan, Brinda, and M Bhuvaneshwari. 2022. "Honesty Factor (HF) based Security Breach Management Technique in Cognitive Radio Network." *Research Square*, July. doi:10.21203/rs.3.rs-1830160/v1.

Various authors [39]. 2020. *Handbook of Research on Blockchain Technology.* 1st edition. Academic Press. doi:10.1016/C2019-0-00935-1.

Warkentin, Merrill, and Craig Orgeron. 2020. "Using the security triad to assess blockchain technology in public sector applications." *International Journal of Information Management*, February. doi:10.1016/j.ijinfomgt.2020.102090.

Whitman, Michael E., and Herbert J. Mattord. 2016. *Principles of Information Security*. Fifth Edition. Cengage Learning. Accessed 10 20, 2023. http://www.mim.ac.mw/books/Principles%20of%20Information%20Security%20(%20PDFDrive%20).pdf.

Wikipedia contributors. 2023. *Cryptography*. Wikipedia, The Free Encyclopedia, 10 18. Accessed 10 20, 2023. https://en.wikipedia.org/w/index.php?title=Cryptography&oldid=1180710842.

Wikipedia contributors. 2023. *Enigma machine.* Wikipedia, The Free Encyclopedia, 10 21. Accessed 10 21, 2023. https://en.wikipedia.org/w/index.php?title=Enigma_machine&oldid=1181179443.

Wikipedia contributors. 2023. *History of cryptography*. Wikipedia, The Free Encyclopedia, September 30. https://en.wikipedia.org/wiki/History_of_cryptography.

Wikipedia contributors. 2023. *World War II cryptography*. Wikipedia, The Free Encyclopedia, January 23. Accessed October 10, 2023. https://en.wikipedia.org/w/index.php?title=World_War_II_cryptography&oldid=1135291497.

Zervopoulos, Panagiotis, and Theodosios Palaskas. 2010. *Εφαρμογή μετρήσεων απόδοσης – αποτελεσματικότητας - αποδοτικότητας στη δημόσια διοίκηση: διεθνής και ελληνική εμπειρία.* Accessed 2024. https://www.researchgate.net/publication/277256127_Epharmoge_metreseon_apodoses_-_apotelesmatikotetas_-_apodotikotetas_ste_demosia_dioikese_diethnes_kai_ellenike_empeiria.

Zhang, Lifang, Zheng Yan, and Raimo Kantola. 2016. "A Review of Homomorphic Encryption and its Applications." *9th EAI International Conference on Mobile Multimedia Communications.* Xi'an, China. 97-106. doi:10.4108/eai.18-6-2016.2264201.

Zhang, Zhenfei. 2014. *Revisiting fully homomorphic encryption schemes and their cryptographic primitives.* Accessed 10 14, 2023. http://ro.uow.edu.au/cgi/viewcontent.cgi?article=5035&context=theses.

Γεωργούλη, Κατερίνα. 2015. *Τεχνητή Νοημοσύνη - Μια εισαγωγική προσέγγιση.* Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών.

10 Ευρετήριο όρων