ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Το πρόβλημα του Cyber Security στα ιατρικά δεδομένα και οι μέθοδοι αντιμετώπισης εναρμονισμένες με το GDPR

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΤΗΛΑ ΚΩΝΣΤΑΝΤΙΝΟΥ

Επιβλέπων : Δημήτριος-Διονύσιος Κουτσούρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Φεβρουάριος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Το πρόβλημα του Cyber Security στα ιατρικά δεδομένα και οι μέθοδοι αντιμετώπισης εναρμονισμένες με το GDPR

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΤΗΛΑ ΚΩΝΣΤΑΝΤΙΝΟΥ

Επιβλέπων : Δημήτριος-Διονύσιος Κουτσούρης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 21η Φεβρουαρίου 2022.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Δημήτριος-Διονύσιος Κουτσούρης Καθηγητής Ε.Μ.Π.	Γεώργιος Ματσόπουλος Καθηγητής Ε.Μ.Π.	Παναγιώτης Τσανάκας Καθηγητής Ε.Μ.Π.

Αθήνα, Φεβρουάριος 2022

(Υπογραφή)

.....

ΠΑΤΗΛΑΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Η παρούσα εργασία έχει ως αντικείμενο την περιγραφή μεθόδων κυβερνοασφάλειας στο χώρο των ιατρικών δεδομένων σε συμμόρφωση με το γενικό κανονισμό προσωπικών δεδομένων (GDPR). Η κυβερνοασφάλεια είναι μια διαδικασία όπου με διάφορες τεχνικές ανιχνεύουμε ψηφιακές απειλές, τις αναλύουμε και τις αντιμετωπίζουμε. Η τεχνολογία της ηλεκτρονικής υγειονομικής περίθαλψης είναι διαδεδομένη σε όλο τον κόσμο και δημιουργεί τεράστιες δυνατότητες βελτίωσης των κλινικών αποτελεσμάτων και αλλαγής της παροχής φροντίδας. Ωστόσο, υπάρχουν αυξανόμενες ανησυχίες σχετικά με την ασφάλεια των δεδομένων και των συσκευών υγειονομικής περίθαλψης. Η αυξημένη συνδεσιμότητα με υπάρχοντα δίκτυα υπολογιστών έχει εκθέσει τις ιατρικές συσκευές σε νέα τρωτά σημεία στον κυβερνοχώρο. Η υγειονομική περίθαλψη είναι ένας ελκυστικός στόχος για το έγκλημα στον κυβερνοχώρο επειδή είναι μια πλούσια πηγή πολύτιμων δεδομένων. Οι παραβιάσεις της ασφάλειας στον κυβερνοχώρο περιλαμβάνουν κλοπή πληροφοριών υγείας και επιθέσεις ransomware σε νοσοκομεία και θα μπορούσαν να περιλαμβάνουν επιθέσεις σε εμφυτευμένες ιατρικές συσκευές. Οι παραβιάσεις μπορούν να μειώσουν την εμπιστοσύνη των ασθενών, να παραλύσουν τα συστήματα υγείας και να απειλήσουν την ανθρώπινη ζωή. Η εργασία αναφέρεται σε τεχνικές κυβερνοασφάλειας ικανές να αντιμετωπίσουν τα ζητήματα ασφαλείας που έχουν προκύψει. Δίνεται έμφαση στην ανωνυμοποίηση, την ψευδωνυμοποίηση και την κρυπτογράφηση ιατρικής εικόνας με τη βοήθεια βαθιάς μάθησης, εναρμονισμένες με τους κανονισμούς προστασίας προσωπικών δεδομένων όπως είναι οι HIPAA και GDPR. Οι προκλήσεις που εμφανίζονται αφορούν τα ποσοστά επιτυχίας των μεθόδων αυτών στα οποία αναφερόμαστε στο τέλος.

Λέξεις Κλειδιά: Κυβερνοασφάλεια, ιατρικά δεδομένα, ανωνυμοποίηση, ψευδωνυμοποίηση, κρυπτογράφηση, βαθιά μάθηση, GDPR

Abstract

The main objective of this thesis is to describe cybersecurity methods in the field of medical data in accordance with the General Regulation of Personal Data (GDPR). Cyber security is a process where with various techniques we detect cyber threats, analyze them and deal with them. Electronic healthcare technology is widespread around the world and creates enormous potential for improving clinical outcomes and changing care delivery. However, there are growing concerns about the security of data and healthcare devices. Increased connectivity to existing computer networks has exposed medical devices to new vulnerabilities in cyberspace. Healthcare is an attractive target for cybercrime because it is a rich source of valuable data. Cyber security breaches include stealing health information and ransomware attacks on hospitals and could include attacks on implanted medical devices. Breaches can reduce patient trust, cripple health systems, and threaten human life. This thesis refers to cyber security techniques capable of dealing with the security issues that have arisen. We emphasize the anonymization, pseudonymization and encryption of medical image with the help of deep learning, harmonized with the regulations of personal data protection such as HIPAA and GDPR. The challenges that arise relate to the success rates of these methods which we refer to in the end.

Keywords: Cyber Security, medical data, anonymization, pseudonymization, cryptography, deep learning, GDPR

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Δημήτριο-Διονύσιο Κουτσούρη, διευθυντή του Εργαστηρίου Βιοϊατρικής Τεχνολογίας της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου, για την ευκαιρία που μου προσέφερε να εκπονήσω την παρούσα διπλωματική εργασία.
Επιπλέον, θα ήθελα να ευχαριστήσω τον υπεύθυνό μου κ. Αθανάσιο Αναστασίου για τη βοήθεια αλλά και την καθοδήγηση που μου παρείχε κατά την υλοποίηση της εργασίας μου.
Τέλος, θα ήθελα να ευχαριστήσω θερμά την οικογένειά μου και τους φίλους μου που στάθηκαν δίπλα μου και με στήριξαν όλα τα χρόνια της φοιτητικής μου ζωής.

Περιεχόμενα

Πίνακας Εικόνων 12
1. Εισαγωγή 15
1.1 Η κυβερνοασφάλεια στον τομέα της υγειονομικής περίθαλψης 15
1.2 Εφαρμογές 18
2. Ανωνυμοποίηση δεδομένων ασθενών 19
2.1 Εισαγωγή 19
2.2 Δομημένα δεδομένα 21
2.3 Δεδομένα συναλλαγών 27
2.3.1 Εφαρμογή παραδοσιακών μεθόδων ανωνυμοποίησης δεδομένων συναλλαγών 29
2.3.2 Απειλές για το απόρρητο κατά τη δημοσίευση δεδομένων συναλλαγών 29
2.4 Μοντέλα απορρήτου: Ανωνυμοποίηση κωδικού διάγνωσης 30
2.5 Αλγόριθμοι ανωνυμοποίησης 36
2.6 Μελέτη περίπτωσης δεδομένων RT: Ανωνυμοποίηση δεδομένων ασθενών 42
2.7 Μοντέλα απορρήτου 43
2.8 Προηγμένοι αλγόριθμοι ανωνυμοποίησης 44
2.9 Μελλοντικές κατευθύνσεις 46
3. Ψευδωνυμοποίηση ιατρικών δεδομένων 49
3.1 Εισαγωγή 49
3.2 Ανάλυση ιατρικών δεδομένων 49
3.3 Ψευδωνυμοποίηση 51
3.3.1 Tokenization 51
3.3.2 Αποτελέσματα σεναρίου υγειονομικής περίθαλψης 56
4. Ένα Δίκτυο κρυπτογράφησης και αποκρυπτογράφησης εικόνας βασισμένο σε βαθιά μάθηση για το Διαδίκτυο ιατρικών πραγμάτων 58
4.1 Εισαγωγή 58
4.2 Αρχιτεκτονική του DeepEDN 60
4.3 Δίκτυο εξόρυξης ROI σε περιβάλλοντα κρυπτογραφημένου κειμένου 65
4.4 Μοντέλο αντιπάλου 66
4.5 Ανάλυση ασφαλείας 67
4.5.1 Εισαγωγή 67
4.5.2 Ανάλυση ασφάλειας κλειδιού 68
4.5.3 Ανάλυση ασφάλειας κρυπτογραφημένου κειμένου 70

4.5.4 Ανάλυση ασφάλειας κάτω από διαφορετικά μοντέλα αντιπάλου 71
4.5.5 Ανάλυση ασφάλειας κάτω από διαφορετικά μοντέλα επίθεσης 73
4.6 Αποτελέσματα πειράματος..... 75
4.6.1 Απόδοση Κρυπτογράφησης και Αποκρυπτογράφησης 75
4.6.2 Απόδοση Δικτύου Εξόρυξης ROI..... 78
4.6.3 Αποδοτικότητα..... 79
5. Εναρμόνιση προσωπικών δεδομένων με το γενικό κανονισμό προσωπικών δεδομένων (GDPR) 81
5.1 Εισαγωγή 81
5.2 Προσωπικά αρχεία υγείας, παγκόσμια πολιτική και ανασκόπηση κανονισμού GDPR 81
5.3 Επικρατείς κανονισμοί προστασίας δεδομένων και οι προκλήσεις τους 84
5.3.1 Γενικές διατάξεις του GDPR..... 84
5.3.2 Νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας (HIPAA)..... 85
5.4 Απαιτήσεις για HIPAA και η λύση συμμόρφωσης GDPR..... 86
5.5 Προτεινόμενη λύση συμμόρφωσης HIPAA και GDPR για την υγειονομική περίθαλψη 87
5.5.1 Κρυπτογράφηση 87
5.5.2 Ψευδωνυμοποίηση..... 88
5.5.3 Ανωνυμοποίηση..... 88
6. Συμπεράσματα 90
Βιβλιογραφία 92

Πίνακας Εικόνων

Εικόνα 1: Κατηγορίες δεδομένων [2].... 20
Εικόνα 2: Πίνακας ασθενών με εφαρμογή διαφορετικής μεθόδου ανωνυμοποίησης[2].... 23
Εικόνα 3: Κατηγοριοποίηση αλγόριθμου k-ανωνυμίας[2] 27
Εικόνα 4: Αρχεία καταγραφής διαγνωστικών με ιατρικό ιστορικό ευαίσθητων αντικειμένων[2].... 28
Εικόνα 5: Ένα παράδειγμα αρχικού συνόλου δεδομένων[2] 30
Εικόνα 6:Περιγραφή του κωδικού ICD 9, ο έντονος κωδικός ICD υποδηλώνει τον ευαίσθητο κωδικό ICD και οι υπόλοιποι είναι οι δημόσιοι κωδικοί ICD[2].... 31
Εικόνα 7: (a) αρχικό σύνολο δεδομένων που περιέχει δημόσια και ευαίσθητα στοιχεία, (b) 2^2-ανώνυμα δεδομένα και (0,5, 6, 2)-συνεκτική εκδοχή της, (c) ιεραρχία γενίκευσης, (d) γενίκευση συνόλου τιμών με βάση το μοντέλο βασισμένο σε κανόνες ειδικά στο (e) και (e) κανόνες PS για το (d)[2]..... 31
Εικόνα 8:Ένα παράδειγμα των (a), (b) δύο ανώνυμων εκδόσεων της εικόνας 7a[2]. 32
Εικόνα 9: Ένα παράδειγμα ανωνυμοποίησης βάσει συνόλου[2]. 35
Εικόνα 10:Σύγκριση αλγορίθμων που προσφέρουν προστασία από επίθεση αποκάλυψης ταυτότητας[2]..... 42
Εικόνα 11:Σύγκριση αλγορίθμων που προσφέρουν προστασία από επίθεση αποκάλυψης ευαίσθητων πληροφοριών[2]. 42
Εικόνα 12:Σύγκριση αλγορίθμων που προσφέρουν προστασία τόσο από την αποκάλυψη ταυτότητας όσο και από την επίθεση αποκάλυψης ευαίσθητων πληροφοριών[2]..... 42
Εικόνα 13:(a) Ένα σύνολο δεδομένων RT με δημογραφικά στοιχεία ασθενών και κωδικούς διάγνωσης, (b) ένα 2^2-ανώνυμο w.r.t. οι συναλλαγές αποδίδουν χρησιμοποιώντας ιεραρχία γενίκευσης που υπάρχει στην εικόνα 6 και (c) η $(2,2^2)$-ανώνυμη έκδοση της εικόνας 13a [2]..... 44
Εικόνα 14:Κατηγοριοποίηση αλγορίθμων για την ανωνυμοποίηση συνόλων δεδομένων RT[2]. 45
Εικόνα 15:Παραδείγματα προβλημάτων κάλυψης και παραβίασης απορρήτου[2]..... 47
Εικόνα 16 Παράδειγμα δεδομένων υγειονομικής περίθαλψης που περιγράφει τύπους γρίπης για ασθενείς. Τα χαρακτηριστικά εκχωρούνται σε κατηγορίες απορρήτου[14]. 50
Εικόνα 17: Αποπροσδιορισμένο σύνολο δεδομένων με εφαρμοσμένη 3-ποικιλομορφία[14]..... 51
Εικόνα 18: Η δομή LPL επεκτείνεται από τα στοιχεία ψευδωνυμοποίησης. Περαιτέρω στοιχεία και χαρακτηριστικά παραλείπονται για το πεδίο εφαρμογής αυτής της εργασίας[14]..... 55
Εικόνα 19: Τροποποιημένες διαδικασίες αποταυτοποίησης βάσει πολιτικής του πλαισίου LPL όταν ζητούνται δεδομένα[14]..... 56
Εικόνα 20: Αποπροσδιορισμένο σύνολο δεδομένων με ψευδωνυμοποίηση. Τα ψευδώνυμα συντέμνονται για καλύτερη αναγνωσιμότητα[14]..... 57
Εικόνα 21: Αντιστοιχίσεις που μπορούν να επαναφέρουν περιεχόμενο που αντικαθίστανται από ψευδώνυμα[14]. 57
Εικόνα 22: Η αρχιτεκτονική του DeepEDN[39]. 60
Εικόνα 23: Η συνολική δομή του DeepEDN[39]..... 61
Εικόνα 24: Διαδικασία δημιουργίας κλειδιού απορρήτου[39]..... 64
Εικόνα 25: Δομή κρυπτογραφημένου και αποκρυπτογραφημένου δικτύου[39]..... 68
Εικόνα 26: Δομή δικτύου εξόρυξης ROI[39]..... 68
Εικόνα 27: Αποτελέσματα κρυπτογράφησης εικόνας[39]..... 69
Εικόνα 28: SSIM μεταξύ 2 κρυπτογραφημένων εικόνων[39]. 69

Εικόνα 29: Κατανομή pixel της αρχικής εικόνας και της κρυπτογραφημένης εικόνας[39]. 70
Εικόνα 30: Αξιολόγηση του αποτελέσματος εντροπίας του δικτύου[39]. 71
Εικόνα 31: Μοντέλο δικτύου διαφορετικών αρχιτεκτονικών[39]. 71
Εικόνα 32: Η απόδοση αποκρυπτογράφησης για διαφορετικά δίκτυα[39]. 71
Εικόνα 33: Η αμοιβαία απόδοση αποκρυπτογράφησης μεταξύ δικτύων υπό εκπαίδευση διαφορετικών κρυφών παραγόντων[39]. 72
Εικόνα 34: Η απόδοση αποκρυπτογράφησης για αυτά τα τέσσερα δίκτυα στην ίδια εικόνα κρυπτογραφημένου κειμένου[39]. 73
Εικόνα 35: Η απόδοση κρυπτογράφησης και αποκρυπτογράφησης της προτεινόμενης μεθόδου[39]. 76
Εικόνα 36: Αξιολόγηση SSIM και PSNR[39]. 77
Εικόνα 37: Η απόδοση του δικτύου εξόρυξης ROI[39]. 78
Εικόνα 38: Πείραμα επίθεσης για το προτεινόμενο δίκτυο εξόρυξης ROI[39]. 79
Εικόνα 39: Η σύγκριση αποτελεσματικότητας μεταξύ της μεθόδου μας και άλλων υπαρχουσών μεθόδων[39]. 80
Εικόνα 40: Μια εννοιολογική επισκόπηση των συστημάτων HER [59]. 82
Εικόνα 41: Απαίτηση συμμόρφωσης HIPAA και GDPR στην υγειονομική περίθαλψη[59]. 89

1. Εισαγωγή

1.1 Η κυβερνοασφάλεια στον τομέα της υγειονομικής περίθαλψης

Η τεχνολογία υγειονομικής περίθαλψης έχει διαδοθεί παντού και δημιουργεί ευκαιρίες για βελτίωση των κλινικών αποτελεσμάτων και παροχής ιατρικής φροντίδας στους ασθενείς. Η αυξημένη συνδεσιμότητα με τα υπάρχοντα δίκτυα υπολογιστών έχει εκθέσει τις ιατρικές συσκευές σε νέες ευπάθειες στον κυβερνοχώρο, με αποτέλεσμα να υπάρχουν αυξανόμενες ανησυχίες σχετικά με την ασφάλεια των δεδομένων και των συσκευών υγειονομικής περίθαλψης. Η υγειονομική περίθαλψη είναι ένας ελκυστικός στόχος για τους hackers για δύο βασικούς λόγους: είναι μια πλούσια πηγή πολύτιμων δεδομένων και οι άμυνές της είναι αδύναμες. Οι παραβιάσεις στον κυβερνοχώρο περιλαμβάνουν κλοπή πληροφοριών για την υγεία και επιθέσεις ransomware στα νοσοκομεία, και θα μπορούσαν να περιλαμβάνουν επιθέσεις σε εμφυτευμένες ιατρικές συσκευές. Οι παραβιάσεις μπορούν να μειώσουν την εμπιστοσύνη των ασθενών, να διαταράξουν τα συστήματα υγείας και να απειλήσουν την ανθρώπινη ζωή. Τελικά, η κυβερνοασφάλεια είναι κρίσιμη για την ασφάλεια των ασθενών, αλλά διαχρονικά είναι αδύναμη. Έχουν θεσπιστεί νέες νομοθετικές και κανονιστικές ρυθμίσεις που διευκολύνουν την αλλαγή. Αυτό απαιτεί την ασφάλεια του κυβερνοχώρου να αποτελέσει αναπόσπαστο τμήμα της ασφάλειας των ασθενών. Απαιτούνται αλλαγές στην ανθρώπινη συμπεριφορά, την τεχνολογία και τις διαδικασίες ως μέρος μιας ολιστικής λύσης [1].

Υπάρχει μια αυξανόμενη ζήτηση για υπηρεσίες υγειονομικής περίθαλψης που προσαρμόζονται στις ανάγκες των ασθενών, ενώ ο προϋπολογισμός για τις υπηρεσίες υγειονομικής περίθαλψης είναι περιορισμένος και πολλές κυβερνήσεις περιορίζουν ακόμη και τις δαπάνες για τη δημόσια υγειονομική περίθαλψη[3].

Οι τεχνολογίες της υγειονομικής περίθαλψης έχουν τη δυνατότητα της επέκτασης και βελτίωσης ζωής. Οι τεχνολογίες που υπάρχουν στις συσκευές αυτές παρέχουν την αποθήκευση ηλεκτρονικών ιατρικών φακέλων (EHR), παρακολουθώντας την υγεία και χορηγώντας φαρμακευτική αγωγή (συμπεριλαμβανομένων των συσκευών γενικής χρήσης και των φορητών ειδών, και της ενσωματωμένης τεχνολογίας στο ανθρώπινο σώμα). Για παράδειγμα, η τεχνολογία τηλεϊατρικής παρέχει φροντίδα εξ αποστάσεως ακόμη και σε όλες τις χώρες. Οι ασθενείς χρησιμοποιούν όλο και περισσότερο τις δικές τους κινητές εφαρμογές, οι οποίες μπορούν τώρα να ενσωματωθούν με την τηλεϊατρική στο ιατρικό διαδίκτυο των πραγμάτων(IoT) [1] για τη συνεργατική διαχείριση της νόσου και τον συντονισμό της περίθαλψης.

Το H-IoT είναι επίσης γνωστό ως το Health IoT, το οποίο αποτελεί ορόσημο στην ανάπτυξη συστημάτων πληροφοριών. Παίζει σημαντικό ρόλο στη διαφώτιση του επιπέδου υγείας των ανθρώπων και αυξάνει την αξία της ζωής. Είναι ένα πολύπλοκο σύστημα, το οποίο περιλαμβάνει συστήματα μικροηλεκτρονικής, ιατρικής και υγείας, επιστήμης υπολογιστών και πολλούς άλλους τομείς. Σύμφωνα με το συνολικό συνδεδεμένο σύστημα υγειονομικής περίθαλψης, η περίοδος από το 2017 έως το 2022 είναι η φάση ανάπτυξης των εφαρμογών υγειονομικής περίθαλψης IoT που επιταχύνουν τις βιομηχανίες υγειονομικής περίθαλψης και διάφορους ενδιαφερόμενους φορείς που εντείνουν τις προσπάθειές τους. Ως εκ τούτου, δεν υπάρχει αμφιβολία ότι το IoT λειτουργεί στον μετασχηματισμό του τομέα της υγειονομικής περίθαλψης επαναπροσδιορίζοντας πλήρως τις συσκευές, τις εφαρμογές και τους ανθρώπους που σχετίζονται μεταξύ τους στις λύσεις υγειονομικής περίθαλψης[4].

Καθώς οι συσκευές υγειονομικής περίθαλψης εξακολουθούν να εξελίσσονται, το ίδιο συμβαίνει και με τη διασύνδεσή τους. Ενώ είναι παραδοσιακά αυτόνομες, πολλές είναι πλέον ενσωματωμένες στο νοσοκομειακό δίκτυο. Για παράδειγμα, σήμερα υπάρχουν 10-15 συνδεδεμένες συσκευές ανά κρεβάτι στα νοσοκομεία των ΗΠΑ. Η διασύνδεση έχει πολλά οφέλη π.χ. την αποδοτικότητα, τη μείωση σφαλμάτων, τον αυτοματισμό και την απομακρυσμένη παρακολούθηση. Αυτά τα οφέλη αλλάζουν τη θεραπεία τόσο των οξειών όσο και των μακροχρόνιων νοσημάτων. Η διασυνδεδεμένη τεχνολογία εκτός του κλινικού περιβάλλοντος επιτρέπει στους επαγγελματίες του τομέα της υγείας να παρακολουθούν και να προσαρμόζουν τις εμφυτευμένες συσκευές χωρίς να χρειάζονται επίσκεψη στο νοσοκομείο ή επεμβατικές διαδικασίες. Τα EHRs μπορούν να βελτιώσουν την περίθαλψη των ασθενών καθιστώντας ευρύτερα διαθέσιμες τις πληροφορίες για την υγεία. Δυστυχώς, η διασύνδεση εισάγει νέες ευπάθειες στον κυβερνοχώρο.

Φυσικά, οι παραβιάσεις της ιδιωτικής ζωής ήταν μια ανησυχία πριν από την εμφάνιση ψηφιακών αρχείων υγείας. Ωστόσο, η διασύνδεση των σημερινών αρχείων παρέχει πολλαπλές πιθανές πύλες πρόσβασης. Όπως, η δυνατότητα πρόσβασης εξ αποστάσεως (ενώ ιστορικά τα χαρτιά θα πρέπει να φυλάσσονται εντός των νοσοκομείων και να είναι προσβάσιμα μόνο μέσω φυσικών παραβιάσεων), η δυνατότητα κλοπής δεδομένων να περνάει απαρατήρητη, και η πρόσβαση σε ένα πληρέστερο αρχείο υγείας που παρέχει τη δυνατότητα για πιθανές επιθέσεις (ενώ τα προηγούμενα ιατρικά αρχεία μπορεί να έχουν διαχωριστεί μεταξύ πολλών διαφορετικών νοσοκομείων / τμημάτων). Ιστορικά, τα χαμένα χαρτιά ή το κλεμμένο laptop μπορεί να έχουν εκθέσει εκατοντάδες ή χιλιάδες ασθενείς σε πιθανή παραβίαση δεδομένων, τώρα που αυτές οι πληροφορίες είναι ηλεκτρονικές και διατίθενται σε πολλά δίκτυα, η παραβίαση της ιδιωτικής ζωής πιθανότατα να επηρεάσει εκατομμύρια ανθρώπους. Για να το καταδείξουμε περαιτέρω, τα αρχεία υγείας διασημοτήτων ήταν πάντοτε στόχος παραβιάσεων [5]. Ωστόσο, πριν από την εμφάνιση ηλεκτρονικών αρχείων, αυτές οι παραβιάσεις περιορίζονταν στο προσωπικό του νοσοκομείου που μπορούσε να αποκτήσει πρόσβαση στα φυσικά έγγραφα. Τώρα τα αρχεία υγείας διασημοτήτων μπορούν δυνητικά να είναι προσβάσιμα εξ' αποστάσεως, αυξάνοντας τις πιθανότητες παραβίασης. Φυσικά, τα ηλεκτρονικά αρχεία έχουν επίσης ένα βασικό πλεονέκτημα για την ιδιωτική ζωή σε σχέση με τα χαρτιά, την ικανότητα παρακολούθησης της πρόσβασης του προσωπικού (μια πρόσφατη έκθεση δείχνει ότι πάνω από το ήμισυ των παραβιάσεων της υγειονομικής περίθαλψης προέρχονται από το εσωτερικό της οργάνωσης [5]).

Οι παραβιάσεις μπορεί να προκύψουν από hacking, κακόβουλο λογισμικό και εσωτερικές απειλές. Το hacking ορίζεται ως μία μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή με σκοπό να αποκτηθούν πληροφορίες ή να προκληθούν διαταραχές. Το κακόβουλο λογισμικό αναφέρεται σε προγράμματα που έχουν σχεδιαστεί για τη διείσδυση σε υπολογιστές χωρίς τη συγκατάθεση των χρηστών και περιλαμβάνει απειλές όπως ιούς και ransomware. Ενώ οι εσωτερικές απειλές είναι ζητήματα που δημιουργούνται από τα λάθη ή τις εσκεμμένες ενέργειες του προσωπικού (π.χ. απάντηση σε ηλεκτρονικά μηνύματα ηλεκτρονικού "phishing" - επίθεση social engineering για εξαγωγή διαπιστευτηρίων σύνδεσης ή εκκίνηση προσβολής κακόβουλου λογισμικού, εσφαλμένες ρυθμίσεις ασφαλείας, κατάχρηση κωδικών πρόσβασης, απώλεια φορητών υπολογιστών και αποστολή μη κρυπτογραφημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου).

Παραδοσιακά, οι άνθρωποι πίστευαν ότι κανένας δεν θα είχε κίνητρο να επιτεθεί σε συστήματα υγειονομικής περίθαλψης και γι' αυτό δεν κρίθηκαν απαραίτητα μέτρα προστασίας. Δεν υπάρχει οργανισμός υγειονομικής περίθαλψης για την παροχή ασφάλειας στον κυβερνοχώρο. Η έμφαση παραδοσιακά ήταν εστιασμένη στη φροντίδα των ασθενών. Υπάρχουν διάφορα ζητήματα που περιπλέκουν την ασφάλεια του κυβερνοχώρου στον τομέα της υγείας και έχουν αυξημένη ευαισθησία

με την πάροδο του χρόνου όπως, η διαρκώς συνδεδεμένη τεχνολογία για την παροχή αποτελεσματικών τρόπων φροντίδας για τους ασθενείς, ιδιαίτερα με χρόνιες παθήσεις. Αυτό παρέχει πολλούς τρόπους σύνδεσης με ιατροτεχνολογικά προϊόντα. Οι συσκευές είναι συχνά εύκολα προσβάσιμες, γεγονός που αυξάνει την πιθανότητα οι εισβολείς να τα βρουν. Μια μεμονωμένη συσκευή θα μπορούσε να παρέχει ένα πιθανό σημείο εισόδου σε μεγαλύτερα νοσοκομειακά δίκτυα, παρακάμπτοντας τα firewalls. Υπάρχει επίσης μια χρονική καθυστέρηση μεταξύ μιας επίθεσης που συμβαίνει και της ανίχνευσης της παραβίασης, συμβάλλοντας στην περαιτέρω αύξηση της ευπάθειας. Περισσότερη εστίαση στη διατήρηση της υγείας των ασθενών οδηγεί σε συνεχή παρακολούθηση των ασθενών εκτός του κλινικού περιβάλλοντος. Περισσότερες συσκευές που χρησιμοποιούνται στο ευρύτερο περιβάλλον υγειονομικής περίθαλψης αυξάνουν την ευπάθεια σε παραβιάσεις. Οι φορητές συσκευές (π.χ. smartphones) υιοθετούνται ευρέως, καθιστώντας δύσκολη την προστασία δεδομένων υγείας από κινδύνους που ενέχουν οι συσκευές γενικής χρήσης.

Ενώ η υγειονομική περίθαλψη έχει ευπάθειες να εκμεταλλευτεί, οι επιτιθέμενοι πρέπει να έχουν κίνητρο να πραγματοποιήσουν επιθέσεις. Το κίνητρο περιλαμβάνει το οικονομικό και πολιτικό κέρδος και ενδεχομένως τη ζωή σε μια μορφή κυβερνο-πολέμου. Το ισχυρότερο από αυτά τα κίνητρα είναι το οικονομικό κέρδος. Τα δεδομένα της υγειονομικής περίθαλψης είναι πολύ πιο πολύτιμα από οποιοδήποτε άλλο. Η αξία για το σύνολο των ιατρικών διαπιστευτηρίων μπορεί να ξεπεράσει τα $1000. Τα κλεμμένα ιατρικά πρόσωπα μπορούν να χρησιμοποιηθούν για να αποκτήσουν υπηρεσίες υγείας και συνταγογραφούμενα φάρμακα, εκμεταλλευόμενοι την ταυτότητα ή τα πιστοποιητικά ασφάλισης κάποιου. Οι χρήσεις επεκτείνονται σε περίπλοκες απάτες που διαπράττονται από το οργανωμένο έγκλημα. Οι απατεώνες έχουν κερδίσει δισεκατομμύρια μέσα σε λίγα χρόνια με την πραγματοποίηση ψευδών ισχυρισμών και τη διανομή ναρκωτικών για πώληση στο dark web. Μερικές φορές υπάρχουν ακόμη επαρκείς πληροφορίες στα ιατρικά αρχεία για το άνοιγμα τραπεζικών λογαριασμών, την εξασφάλιση δανείων ή την απόκτηση διαβατηρίων.

Τα δεδομένα που διατηρούνται στους οργανισμούς υγείας έχουν επίσης πολιτική αξία. Για παράδειγμα, επιτέθηκαν στον Παγκόσμιο Οργανισμό κατά του Ντόπινγκ και δημοσιοποιήθηκαν τα αρχεία διακεκριμένων αθλητών. Η πρόσβαση σε ιστότοπους του NHS γίνεται από εκατομμύρια πολίτες, καθιστώντας τον έναν πρωταρχικό ιστότοπο για τη δημοσίευση προπαγάνδας, κλπ. Για παράδειγμα, οι ιστότοποι του NHS παραβιάστηκαν από τρομοκράτες στον κυβερνοχώρο και μεταφορτώθηκαν εικόνες του εμφυλίου πολέμου της Συρίας.

Εκείνοι με δεξιότητες ασφάλειας στον κυβερνοχώρο απολαμβάνουν την πρόκληση της εύρεσης και της έκθεσης τρωτών σημείων ασφαλείας σε δίκτυα και ιατρικές συσκευές. Για παράδειγμα, το 2016 μια μεμονωμένη σάρωση για την ασφάλεια των ευπαθών μπόρεσε να αποκτήσει πρόσβαση σε ένα αρχείο που περιέχει δεδομένα ατόμων που είχαν εγγραφεί στην υπηρεσία του Εθελοντή Αιμοδότη[1].

Ο νόμος περί φορητότητας και λογοδοσίας για την ασφάλιση υγείας των ΗΠΑ του 1996 εφήρμοσε αρχές για να διασφαλίσει ότι προστατεύονται ορισμένες ηλεκτρονικές πληροφορίες για την υγεία. Ο Κανόνας ασφαλείας απαιτεί από τους υπευθύνους να διατηρούν σύγχρονες και κατάλληλες διοικητικές τεχνικές και φυσικές εφαρμογές για να διασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που δημιουργούν, λαμβάνουν, συντηρούν ή μεταδίδουν. Ο γενικός κανονισμός για την προστασία δεδομένων (GDPR) επίσης τέθηκε σε ισχύ στο Ηνωμένο Βασίλειο τον Μάιο του 2018. Ο GDPR έχει σχεδιαστεί για να εναρμονίσει τους νόμους περί απορρήτου δεδομένων σε ολόκληρη την Ευρώπη για την προστασία από το απόρρητο και τις παραβιάσεις δεδομένων [6]. Ο GDPR στοχεύει να το επιτύχει με την αντιμετώπιση των κενών στην ισχύουσα νομοθεσία, η οποία κυκλοφόρησε τη δεκαετία του 1990 από οργανισμούς που κατέχουν

τεράστια ηλεκτρονικά δεδομένα. Ο GDPR ισχύει για όλα τα προσωπικά δεδομένα που κατέχει ένας οργανισμός. Στο πλαίσιο της νέας νομοθεσίας, όλες οι παραβιάσεις που ενδέχεται να οδηγήσουν σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των λαών πρέπει να αναφέρονται στο γραφείο του Επιτρόπου Πληροφοριών (ICO). Οι παραβιάσεις των δεδομένων υγείας πιθανότατα εμπίπτουν σε αυτήν την κατηγορία, επομένως θα πρέπει να αναφέρονται στον ICO εντός 72 ωρών από την παραβίαση. Το πρόστιμο για τη μη συμμόρφωση φτάνει έως και 20 εκατ. Ευρώ. Άλλες αλλαγές περιλαμβάνουν την ανάγκη όλων των πρακτικών να διαθέτουν ένα γραφείο προστασίας δεδομένων και την εισαγωγή μιας νομοθεσίας περί «διαφάνειας και δίκαιης επεξεργασίας» που πρέπει να συμπεριληφθεί στις ειδοποιήσεις απορρήτου των ασθενών [6]. Αυτή η νέα νομοθεσία θα αυξήσει σημαντικά το κόστος των παραβιάσεων (λόγω υλοποιήσεων) και μπορεί να συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με ζητήματα απορρήτου και την ανάγκη για βελτιωμένη ασφάλεια στον κυβερνοχώρο.

Η ασφάλεια στον κυβερνοχώρο είναι ένας ταχέως αναπτυσσόμενος κλάδος. Με τις απώλειες που σχετίζονται με παραβιάσεις στον κυβερνοχώρο, περισσότερες εταιρείες στρέφονται προς την ασφάλεια. Οι βελτιώσεις ασφαλείας πιθανόν να οδηγούνται από κατάλληλα ασφαλιστικά κίνητρα. Η προστασία έναντι των συνεπειών των διαδικτυακών επιθέσεων ενδέχεται να αποτελεί μέρος των υποχρεώσεων που ασφαλίζονται κατά τον ίδιο τρόπο όπως τα νοσοκομεία είναι ασφαλισμένα έναντι αξιώσεων εγκληματικής αμέλειας[1].

1.2 Εφαρμογές

Παρακάτω θα αναφερθούμε σε μερικές τεχνικές οι οποίες βρίσκουν εφαρμογή στο πρόβλημα της κυβερνοασφάλειας στον τομέα της υγειονομικής περίθαλψης.

1. Η ανωνυμοποίηση είναι μια τεχνική επεξεργασίας δεδομένων, η οποία αποκρύπτει ή τροποποιεί στοιχεία προσωπικής ταυτοποίησης. Με διάφορες τεχνικές όπως το διαφορικό απόρρητο και η γενίκευση δεδομένων, τα δεδομένα αποκτούν ανώνυμη μορφή και δεν μπορούν να συσχετιστούν με οποιοδήποτε άτομο.

2. Η ψευδωνυμοποίηση είναι μια διαδικασία επεξεργασίας δεδομένων με την οποία η ταυτότητα των δεδομένων αποκρύπτεται από τα υπόλοιπα δεδομένα. Αυτό επιτυγχάνεται με την αντικατάσταση πληροφοριών που μπορούν να ταυτοποιήσουν ένα άτομο με ένα ή περισσότερα τεχνητά αναγνωριστικά ή ψευδώνυμα. Η χρήση ψευδωνύμων καθιστά τα δεδομένα λιγότερο αναγνωρίσιμα, ενώ ταυτόχρονα τα δεδομένα παραμένουν κατάλληλα για ανάλυση και επεξεργασία. Στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) η ψευδωνυμοποίηση ορίζεται ως η επεξεργασία δεδομένων προσωπικού χαρακτήρα με τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να οδηγήσουν σε συγκεκριμένο άτομο χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο φυσικό πρόσωπο.

3. Το DeepEDN είναι ένα δίκτυο κρυπτογράφησης και αποκρυπτογράφησης που βασίζεται σε βαθιά μάθηση για να εκπληρώσει τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης της ιατρικής εικόνας. Συγκεκριμένα, στο DeepEDN, το Cycle - Generative Adversarial Network (Cycle-GAN) χρησιμοποιείται ως το κύριο δίκτυο εκμάθησης για τη μεταφορά της ιατρικής εικόνας από

τον αρχικό τομέα στον τομέα στόχο. Ο τομέας στόχος θεωρείται ως ο "Κρυφός Παράγοντας" που καθοδηγεί το μοντέλο εκμάθησης για την πραγματοποίηση της κρυπτογράφησης. Η κρυπτογραφημένη εικόνα επαναφέρεται στην αρχική (απλό κείμενο) εικόνα μέσω ενός δικτύου ανακατασκευής για να επιτευχθεί αποκρυπτογράφηση εικόνας. Προκειμένου να διευκολυνθεί η εξόρυξη δεδομένων απευθείας από το προστατευμένο απόρρητο περιβάλλον, προτείνεται ένα δίκτυο εξόρυξης περιοχής ενδιαφέροντος (ROI) για την εξαγωγή του ενδιαφερόμενου αντικειμένου από την κρυπτογραφημένη εικόνα. Το προτεινόμενο DeepEDN αξιολογείται στο σύνολο δεδομένων ακτίνων Χ θώρακα. Εκτεταμένα πειραματικά αποτελέσματα και ανάλυση ασφάλειας δείχνουν ότι η προτεινόμενη μέθοδος μπορεί να επιτύχει υψηλό επίπεδο ασφάλειας με καλή αποδοτικότητα.

2. Ανωνυμοποίηση δεδομένων ασθενών

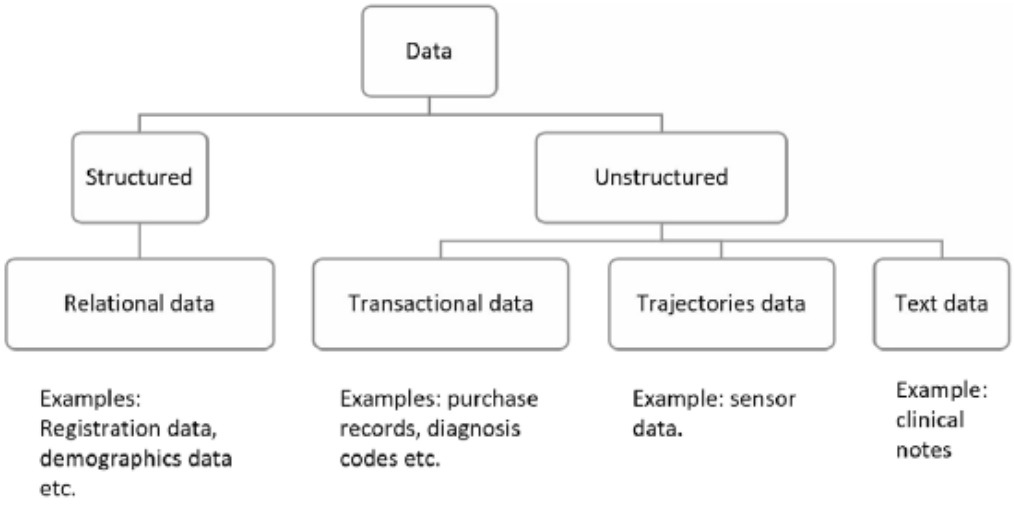
2.1 Εισαγωγή

Κατά τη συγκέντρωση ιατρικών δεδομένων ή κατά την επαναχρησιμοποίησή τους για δευτερεύοντες σκοπούς, τα ζητήματα απορρήτου και οι νομικές απαιτήσεις χρειάζονται προσεκτική εξέταση. Η προστασία της ιδιωτικής ζωής περιλαμβάνει ηθικά, νομικά και κοινωνικά ζητήματα και συνήθως απαιτούνται πολλά επίπεδα τεχνικών και μη τεχνικών μέτρων για την εφαρμογή της. Από τεχνικής πλευράς, το απόρρητο των ασθενών συχνά προστατεύεται από την ανωνυμοποίηση δεδομένων, πράγμα που σημαίνει ότι τα σύνολα δεδομένων τροποποιούνται με τρόπο που αποτρέπει την εκ νέου επιτυχή αναγνώριση. Οι εθνικοί και διεθνείς κανονισμοί απορρήτου αφορούν την ανωνυμοποίηση δεδομένων. Στις Ηνωμένες Πολιτείες, η μέθοδος Safe Harbor του Κανόνα Προστασίας Προσωπικών Δεδομένων του νόμου περί φορητότητας και λογοδοσίας ασφάλισης υγείας (HIPAA) παρέχει έναν κατάλογο χαρακτηριστικών για τα οποία οι τιμές πρέπει να αφαιρεθούν ή να τροποποιηθούν. Επιπλέον, η μέθοδος Expert Determination επιτρέπει τη χρήση επίσημων και στατιστικών μεθόδων για την αξιολόγηση και τη διαχείριση κινδύνων επαναπροσδιορισμού, κάτι παρόμοιο με τον τρόπο με τον οποίο πρέπει να εφαρμοστεί η ανωνυμοποίηση δεδομένων στην Ευρωπαϊκή Ένωση. Η ανωνυμοποίηση δεδομένων είναι μια πολύπλοκη διαδικασία κατά την οποία η προκύπτουσα μείωση των κινδύνων επαναπροσδιορισμού πρέπει να εξισορροπηθεί με τη μείωση της χρησιμότητας των δεδομένων. Μια μεγάλη ποικιλία διαφορετικών μοντέλων και μεθόδων για τον μετασχηματισμό δεδομένων, την εκτίμηση κινδύνου και την εκτίμηση της χρησιμότητας έχει προταθεί για την αντιμετώπιση αυτού του συμβιβασμού[9].

Τις τελευταίες δύο δεκαετίες παρατηρείται αυξανόμενο ενδιαφέρον για μεθόδους απόκρυψης των προσωπικών δεδομένων από τη δημοσίευσή τους. Ορισμένες μέθοδοι έχουν εφαρμοστεί επιτυχώς από διάφορες εφαρμογές στην ιατρική, στα σούπερ μάρκετ και στο ηλεκτρονικό εμπόριο. Η ανάγκη απόκρυψης των δεδομένων είναι απαραίτητη από τη στιγμή που υπάρχει ραγδαία αύξηση της πληροφορίας. Όταν δημοσιεύονται τα δεδομένα που σχετίζονται με ένα άτομο στο διαδίκτυο, αυξάνονται η χρησιμότητα αυτών των δεδομένων, αλλά αυξάνονται και οι ανησυχίες περί απορρήτου. Αυτό ισχύει ιδιαίτερα για τα ιατρικά δεδομένα ασθενών που ενδέχεται να περιέχουν πληροφορίες σχετικές με τα δημογραφικά στοιχεία, το DNA, ή το ιατρικό ιστορικό, όπως τα στοιχεία διαγνώσεων και τα αποτελέσματα εργαστηριακών εξετάσεων. Αυτές οι λεπτομέρειες, αν κοινοποιηθούν, είναι επιρρεπείς σε επιθέσεις, κάτι που είναι αντίθετο με τη νομοθεσία. Μια απλή λύση, για τη διατήρηση της

ιδιωτικής ζωής ενός χρήστη είναι να αποκρύψει το μοναδικό αναγνωριστικό του ασθενή τη στιγμή της δημοσίευσης των δεδομένων. Αυτό το αναγνωριστικό είναι ο αριθμός κοινωνικής ασφάλισης.

Ωστόσο, μόνο η αφαίρεση του αναγνωριστικού δε μπορεί να διατηρήσει το απόρρητο των χρηστών. Μπορεί να υπάρχουν κι άλλα χαρακτηριστικά όπως η ημερομηνία γέννησης, ο ταχυδρομικός κώδικας και το φύλο. Αυτά σε συνδυασμό, μπορούν να αποκαλύψουν την ταυτότητα του χρήστη αν αξιοποιηθούν κατάλληλα από κακόβουλους ανθρώπους. Επομένως, υπάρχει μια απαίτηση για μια πιο εξελιγμένη προσέγγιση στη διατήρηση του απορρήτου. Υπάρχουν τα δομημένα δεδομένα και τα μη δομημένα (Εικόνα 1). Τα δομημένα δεδομένα έχουν μια σταθερή δομή και αναφέρονται σε πληροφορίες που συνίστανται βασικά από στήλες και σειρές δεδομένων σε έναν πίνακα, ή σε περισσότερους, συνδεδεμένους πίνακες. Αντίθετα, τα μη δομημένα δεδομένα είναι πολύ πιο μεταβλητά τόσο σε μορφή όσο και σε περιεχόμενο. Αυτά τα δεδομένα μπορούν περαιτέρω να ταξινομηθούν ως δεδομένα συναλλαγών, δεδομένα τροχιάς και δεδομένα κειμένου. Τα δεδομένα συναλλαγών περιλαμβάνουν ιστορικά συναλλαγών για χρήστες όπως είναι τα αποδεικτικά πληρωμών και οι κωδικοί διάγνωσης. Τα δεδομένα τροχιάς αντιπροσωπεύουν την κινητικότητα αντικειμένων, όπως άνθρωποι, οχήματα, δεδομένα αισθητήρων, ακολουθίες DNA και δεδομένα κειμένου όπως είναι οι κλινικές σημειώσεις. Σε πολλές περιπτώσεις, το σύνολο δεδομένων μπορεί να είναι ένας συνδυασμός των παραπάνω τύπων. Για παράδειγμα, τα δεδομένα ασθενούς περιλαμβάνουν σχεσιακά δεδομένα όπως την εγγραφή και τα δημογραφικά στοιχεία, δεδομένα συναλλαγών που υποδηλώνουν ευρήματα και αιτίες τραυματισμού ή ασθενειών και δεδομένα κειμένου.



Εικόνα 1: Κατηγορίες δεδομένων [2]

Σκοπός είναι να ερευνηθούν δημοφιλείς αλγόριθμοι για την ανωνυμοποίηση σχεσιακών δεδομένων καθώς και δεδομένων συναλλαγών. Αναφορικά με τα σχεσιακά δεδομένα, επιστήμονες έχουν προτείνει πολλές μεθόδους όπως τις k-ανωνυμία, l-ποικιλομορφία, t-εγγύτητα. Θα εστιάσουμε στη γνωστή τεχνική ανωνυμοποίησης που χρησιμοποιείται για την προστασία της σύνδεσης και της ταυτοποίησης των εγγραφών σε ένα σύνολο δεδομένων. Μια επιτυχημένη τεχνική είναι η k-ανωνυμία για σχεσιακά δεδομένα. Αυτή η τεχνική τροποποιεί τις τιμές των οιονεί αναγνωριστικών (Quasi-Identifier-

QID) με τρόπο που σε κάθε εγγραφή στον πίνακα να υπάρχουν τουλάχιστον (k-1) άλλες εγγραφές με την ίδια τιμή για το οιονεί αναγνωριστικό. Αυτό το μοντέλο προστατεύει το απόρρητο ενός χρήστη, όταν απελευθερώνει πληροφορίες για συγκεκριμένο άτομο και περιορίζει τη δυνατότητα χρήσης του οιονεί αναγνωριστικού για την ανάκτηση άλλων σχετικών αλλά εξωτερικών πληροφοριών. Σε περίπτωση μη δομημένων δεδομένων ή δεδομένων συναλλαγών, όπως τα δεδομένα ασθενών, από έναν τεράστιο αριθμό διαθέσιμων διαγνώσεων, μόνο λίγες ισχύουν για ένα άτομο το οποίο καθιστά τα δεδομένα μηδενικά. Επιπλέον κάθε άτομο έχει διαφορετικές διαγνώσεις οπότε δημιουργείται ετερογένεια στα δεδομένα.

2.2 Δομημένα δεδομένα

Η ασφαλής δημοσίευση σχεσιακών δεδομένων απαιτεί την προστασία από τρεις τύπους απειλών προστασίας της ιδιωτικής ζωής όπως είναι η αποκάλυψη ταυτότητας. Στα δημοσιευμένα δεδομένα, μια συγκεκριμένη εγγραφή σχετική με άτομο, οδηγεί σε αποκάλυψη ταυτότητας. Στην περίπτωση δημοσίευσης δεδομένων, οι ασθένειες θεωρούνται ευαίσθητες και τα άτομα δε θα θέλουν να δημοσιευτούν. Άλλα χαρακτηριστικά θεωρούνται δημόσια και δεν επηρεάζονται τα άτομα από την δημοσίευσή τους. Για παράδειγμα, γνωρίζοντας ότι η Μαρία έχει ηλικία 70 ετών και ταχυδρομικό κώδικα 30000 από τις πληροφορίες της λίστας των ψηφοφόρων, ένας εισβολέας μπορεί να τη συνδέσει με την τελευταία εγγραφή της Εικ.2(α), καθώς αυτή είναι η μόνη συναλλαγή με αυτές τις τιμές. Άλλη μια απειλή είναι η αποκάλυψη ιδιότητας μέλους, όπου αυτή επιτρέπει στον εισβολέα να έχει εικόνα των δεδομένων σχετικά με ένα άτομο σε ένα σύνολο δεδομένων. Ο τρίτος τύπος απειλής είναι η γνωστοποίηση χαρακτηριστικών, όπου ένα σύνολο ευαίσθητων στοιχείων μπορεί να συσχετιστεί με ένα άτομο. Για παράδειγμα, ένας εισβολέας γνωρίζει την ηλικίας της Αλίκης και του ταχυδρομικού κώδικα, 65 και 25000 αντίστοιχα. Αν και ο εισβολέας δε μπορεί να συνδέσει την Αλίκη με μια συγκεκριμένη εγγραφή, καθώς υπάρχουν δύο εγγραφές ίδιας τιμής στην Εικ.2(α), μπορεί να συμπεράνει ότι η Αλίκη έχει τη νόσο της γαστρίτιδας διότι και οι δύο συναλλαγές περιέχουν την ίδια ασθένεια.

Σημαντικά μοντέλα απορρήτου που προτάθηκαν είναι η k-ανωνυμία, l-ποικιλομορφία και η t-εγγύτητα. Το μοντέλο k-ανωνυμία χρησιμοποιείται ευρέως για την προστασία του απορρήτου της απελευθέρωσης στατικών δεδομένων. Η k-ανωνυμία μπορεί να μοντελοποιηθεί ως πρόβλημα ομαδοποίησης που χωρίζει τα δεδομένα σε ομάδες (δηλαδή συστάδες) με την αρχή της ελαχιστοποίησης της απώλειας πληροφοριών[10]. Το μοντέλο της k-ανωνυμίας εγγυάται ότι οι πληροφορίες κάθε χρήστη που είναι αποθηκευμένες στο δημοσιευμένο σύνολο δεδομένων, δε μπορούν να διαφοροποιηθούν από τουλάχιστον k-1 εγγραφές που καταγράφονται στο ίδιο σύνολο δεδομένων. Όμως αυτό το μοντέλο μπορεί να αποτύχει για τις εγγραφές που έχουν τις ίδιες ευαίσθητες τιμές εξαιτίας της επίθεσης ομοιογένειας. Η αδυναμία του μοντέλου k-ανωνυμίας αντιμετωπίζεται από το μοντέλο l-ποικιλομορφία, όπου αυτό γίνεται με την εισαγωγή των διαφορετικών τιμών του ευαίσθητου χαρακτηριστικού εντός της ομάδας στον μηχανισμό ανωνυμοποίησης. Το μοντέλο t-εγγύτητα είναι μια περαιτέρω βελτίωση του μοντέλου l-ποικιλομορφίας που χρησιμοποιείται για τη διατήρηση της ιδιωτικής ζωής στα σύνολα δεδομένων, μειώνοντας την ευαισθησία μιας αναπαράστασης δεδομένων. Το μοντέλο αυτό επεκτείνει το μοντέλο l-ποικιλομορφίας με την επεξεργασία των τιμών ενός χαρακτηριστικού ξεχωριστά λαμβάνοντας υπόψη την κατανομή των τιμών δεδομένων για αυτό το χαρακτηριστικό.

Μια άλλη μέθοδος ανωνυμοποίησης είναι η γενίκευση. Η γενίκευση αντικαθιστά την τιμή του QID με τη λιγότερο συγκεκριμένη τιμή, όπως φαίνεται στην Εικ. 2(β). Υπάρχουν διάφορες κατηγορίες αλγορίθμων γενίκευσης.

Α) Ειδίκευση από πάνω προς τα κάτω έναντι γενίκευσης από κάτω προς τα πάνω. Η γενίκευση των δεδομένων πραγματοποιείται με εξειδίκευση ή λεπτομερή περιγραφή του επιπέδου της πληροφορίας από πάνω προς τα κάτω, έως ότου παραβιαστεί μια ελάχιστη απαίτηση απορρήτου και η γενίκευση από κάτω προς τα πάνω ξεκινά από τις εξειδικευμένες τιμές στις λιγότερο εξειδικευμένες, έως ότου παραβιαστεί μια ελάχιστη απαίτηση απορρήτου.

Β) Καθολικό (μονοδιάστατο) έναντι τοπικού (πολυδιάστατο). Ενώ η k-ανωνυμία εφαρμόζεται στα δεδομένα προκειμένου να διατηρηθεί η χρησιμότητα δεδομένων όσο το δυνατόν περισσότερο, η τοπική κωδικοποίηση προτιμάται από την καθολική διότι η καθολική εφαρμόζει την ίδια στρατηγική γενίκευσης για ολόκληρο το σύνολο των δεδομένων σε αντίθεση με την τοπική. Η καθολική κωδικοποίηση μπορεί να οδηγήσει σε απώλεια περισσότερων πληροφοριών και υπεργενίκευση δεδομένων σε σχέση με την τοπική κωδικοποίηση.

Γ) Πλήρης (βέλτιστη) έναντι άπληστη (κατά προσέγγιση). Η άπληστη προσέγγιση βρίσκει ευρετικά μια καθολική βέλτιστη λύση κάνοντας βέλτιστη επιλογή σε κάθε στάδιο, ενώ οι Meyerson και Williams επιβεβαίωσαν ότι η ιδανική k-ανωνυμία είναι ένα πρόβλημα NP-δυσχερές(NP-hard)[2].

Δ) Βάσει ιεραρχίας (καθορίζεται από τον χρήστη) έναντι βάσει διαμερίσματος (αυτόματη). Στον αλγόριθμο βάσει ιεραρχίας, το δέντρο γενίκευσης ορίζεται από τον χρήστη για κάθε χαρακτηριστικό QI, ενώ στον αλγόριθμο βάσει διαμερίσματος, το ίδιο το σύστημα ορίζει το διαμέρισμα των QI χαρακτηριστικών.

Υπάρχουν πολλές άλλες λειτουργίες ανωνυμοποίησης διαθέσιμες για την τροποποίηση ενός πίνακα. Αυτές περιλαμβάνουν την καταστολή, τον ανατομισμό, την παραλλαγή, τη διαταραχή, την κατηγοριοποίηση, τον τεμαχισμό. Η εικόνα 2 δείχνει τον πίνακα ενός ασθενούς με εφαρμογή μεθόδων ανωνυμοποίησης. Η καταστολή αφαιρεί την τιμή του QID όπως φαίνεται στην Εικ.2γ, όπου η τιμή της ηλικίας αφαιρείται. Ο ανατομισμός διαφέρει από τη γενίκευση και την καταστολή. Ο ανατομισμός ούτε τροποποιεί το οιονεί αναγνωριστικό ούτε το ευαίσθητο χαρακτηριστικό, αλλά αποσυνδέει τη σχέση μεταξύ του οιονεί αναγνωριστικού με το ευαίσθητο χαρακτηριστικό. Ο ανατομισμός δημιουργεί δύο ξεχωριστούς πίνακες, έναν πίνακα οιονεί αναγνωριστικών (QID) που αποτελείται από χαρακτηριστικά QID και έναν ευαίσθητο πίνακα (ST) που αποτελείται από ευαίσθητα χαρακτηριστικά και το GroupID είναι το κοινό χαρακτηριστικό και στους δύο πίνακες. Η τιμή του χαρακτηριστικού GroupID θα είναι ίδια για όλες τις εγγραφές στην ίδια ομάδα και στους δύο πίνακες και συνεπώς συνδέονται με τις ευαίσθητες τιμές της ομάδας με τον ίδιο τρόπο.

Id	Age	Sex	Zip	Disease
1	23	M	11000	Pneumonia
2	27	M	13000	Dyspepsia
3	35	M	59000	Dyspepsia
4	59	M	12000	Pneumonia
5	61	F	54000	Flu
6	65	F	25000	Gastritis
7	65	F	25000	Gastritis
8	70	F	30000	Bronchitis

a) Patient table

Age	Sex	Zip	Disease
[21,60]	M	(10001,60000)	Pneumonia
[21,60]	M	(10001,60000)	Dyspepsia
[21,60]	M	(10001,60000)	Dyspepsia
[21,60]	M	(10001,60000)	Pneumonia
[61,70]	F	(10001,60000)	Flu
[61,70]	F	(10001,60000)	Gastritis
[61,70]	F	(10001,60000)	Gastritis
[61,70]	F	(10001,60000)	Bronchitis

b) Generalized table of a

Age	Sex	Zip	Disease
*	M	(10001,60000)	Pneumonia
*	M	(10001,60000)	Dyspepsia
*	M	(10001,60000)	Dyspepsia
*	M	(10001,60000)	Pneumonia
*	F	(10001,60000)	Flu
*	F	(10001,60000)	Gastritis
*	F	(10001,60000)	Gastritis
*	F	(10001,60000)	Bronchitis

c) Suppression of age attribute

id	Age	Sex	Zip	Group-id
1	23	M	11000	1
2	27	M	130	1
3	35	M	59000	1
4	59	M	12000	1
5	61	F	54000	2
6	65	F	25000	2
7	65	F	25000	2
8	70	F	30000	2

d.1) Quasi-identifier table (QIT)

Group-id	Disease	Count
1	Dyspepsia	2
1	Pneumonia	2
2	Bronchitis	1
2	Flu	1
2	Gastritis	2

d.2) Sensitive table (ST)

d) Anatomization

Age	Sex	Zip	Disease
23	M	11000	Dyspepsia
27	M	130	Pneumonia
35	M	59000	Pneumonia
59	M	12000	Dyspepsia
61	F	54000	Bronchitis
65	F	25000	Gastritis
65	F	25000	Gastritis
70	F	30000	Flu

e) Bucketization

(Age, sex)	(Zip, Disease)
(23, M)	(59000, Pneumonia)
(27, M)	(12000, Dyspepsia)
(35, M)	(11000, Dyspepsia)
(59, M)	(13000, Pneumonia)
(61, F)	(54000, Bronchitis)
(65, F)	(25000, Gastritis)
(65, F)	(25000, Gastritis)
(70, F)	(30000, flu)

f) Sliced table

Εικόνα 2: Πίνακας ασθενών με εφαρμογή διαφορετικής μεθόδου ανωνυμοποίησης[2]

Για παράδειγμα, ας εξετάσουμε την απελευθέρωση των δεδομένων ασθενούς στο Σχ.2(α), όπου το ευαίσθητο χαρακτηριστικό είναι “Νόσος” και QID= {Ηλικία, Φύλο}. Το QID που δημιουργείται (εικόνα 2d.1) περιέχει όλες τις εγγραφές από τον αρχικό πίνακα στην Εικ.2α εκτός από το ευαίσθητο χαρακτηριστικό “Νόσος” καθώς αυτό το χαρακτηριστικό αντικαθίσταται από το χαρακτηριστικό GroupID. Στη συνέχεια, δημιουργείται ST (εικόνα 2d.2) που περιέχει τον αριθμό κάθε “Νόσου” για κάθε ομάδα QID. Το QIT και το ST πληρούν την απαίτηση απορρήτου $l \leq 2$, επειδή η πιθανότητα να συναχθεί οποιαδήποτε σχετική τιμή “Νόσου” σε κάθε ομάδα QID στο QIT είναι το πολύ $1/l=1/2=50\%$.

Η παραλλαγή αποσυνδέει τη συσχέτιση του οιονεί αναγνωριστικού και του αριθμητικού ευαίσθητου χαρακτηριστικού. Πρώτα, το σύνολο των εγγραφών δεδομένων χωρίζεται σε ομάδες και στη

συνέχεια σε κάθε ομάδα οι ευαίσθητες τιμές ανακατεύονται. Η διαταραχή αντικαθιστά τις αρχικές τιμές δεδομένων με τις τιμές συνθετικών δεδομένων, έτσι ώστε οι στατιστικές πληροφορίες να μη διαφέρουν σημαντικά από τα αρχικά δεδομένα. Οι εγγραφές στο σύνολο δεδομένων που κυκλοφόρησαν δεν αντιστοιχούν στους κατόχους εγγραφών του πραγματικού κόσμου, επομένως, ένας εισβολέας δε συνδέει ούτε ανακτά τις ευαίσθητες πληροφορίες από τα δημοσιευμένα δεδομένα. Η καδοποίηση χωρίζει τις εγγραφές του συνόλου δεδομένων σε κάδους, και στη συνέχεια, εφαρμόζει τυχαία μετάθεση ευαίσθητου χαρακτηριστικού σε κάθε κάδο για να σπάσει τη σύνδεση του QID και του ευαίσθητου χαρακτηριστικού όπως φαίνεται στην Εικ.2e. Στο τεμαχισμό γίνονται δύο τύποι διαμερισμάτων, ο κάθετος και ο οριζόντιος. Στην κατακόρυφη κατάτμηση, τα συσχετισμένα χαρακτηριστικά ομαδοποιούνται σε στήλες και στη συνέχεια οι εγγραφές ομαδοποιούνται σε κάδους σε οριζόντια διαμέριση. Τέλος, μετατρέποντας τυχαία τις τιμές στηλών σε κάθε κάδο διακόπτεται η σύνδεση μεταξύ διαφορετικών στηλών που φαίνονται στην Εικ.2f.

Για τη διατήρηση του απορρήτου κατά τη διάρκεια της δημοσίευσης δεδομένων, πρώτα απαιτείται k-ανωνυμία. Ακολουθούν οι πιο δημοφιλείς αλγόριθμοι.

Ο μ-Argus είναι ένας αλγόριθμος που ακολουθεί την άπληστη προσέγγιση για τη γενίκευση των τιμών δεδομένων και στη συνέχεια καταστέλλει τα ακραία σημεία προκειμένου να επιτύχει την κατάσταση της k-ανωνυμίας. Προσδιορίζει σπάνιους και μη ασφαλείς συνδυασμούς των 2 και 3 συνδυασμών των τιμών του συνόλου δεδομένων. Οι μη ασφαλείς συνδυασμοί εξαλείφονται με γενίκευση των χαρακτηριστικών εντός του συνδυασμού και με καταστολή κελιών. Το δημοσιευμένο σύνολο δεδομένων περιέχει συνήθως όλες τις πλειάδες και τα χαρακτηριστικά των αρχικών δεδομένων, αν και οι τιμές ενδέχεται να παραλειφθούν σε ορισμένες τοποθεσίες κελιών. Αλλά δεν εξετάζει όλους τους μη ασφαλείς συνδυασμούς των χαρακτηριστικών στο QID, εξετάζονται μόνο 2, 3 συνδυασμοί τιμών δεδομένων. Οι γενικεύσεις που παρέχονται από τον αλγόριθμο ενδέχεται να μην ικανοποιούν πάντα την ιδιότητα k-ανωνυμία και δε δίνουν k-minimal λύση.

Ο Datafly είναι ένας αλγόριθμος που δημιουργεί πρώτα λίστες συχνοτήτων χρησιμοποιώντας άπληστη προσέγγιση και στη συνέχεια γενικεύει επαναληπτικά τους συνδυασμούς τιμών των συνόλων δεδομένων που εμφανίζονται λιγότερο από k-φορές. Μετράει τη συχνότητα πάνω από το σύνολο QID κα εάν η συχνότητα είναι μικρότερη από k, τότε οι πιο διακριτές τιμές χαρακτηριστικών γενικεύονται έως ότου ικανοποιηθεί η k-ανωνυμία. Εξασφαλίζει τη λύση k-ανωνυμία, αλλά δεν παρέχει την ελάχιστη γενίκευση. Το αποτέλεσμα παραμορφώνεται περισσότερο απ' ό,τι χρειάζεται.

Ο Binary Search είναι ένας αλγόριθμος που βασίζεται στη δυαδική αναζήτηση για την επίτευξη της k-minimal γενίκευσης και δίνει μια ελάχιστη γενίκευση. Τα ζητήματα που αυτός ο αλγόριθμος δεν αποδίδει είναι οι πολλαπλές εκδόσεις συνόλων δεδομένων, οι πιθανότητες συμπαιγνίας είτε από πολλαπλούς παραλήπτες είτε από τους ίδιους τους παραλήπτες χρησιμοποιώντας πολλαπλά ερωτήματα και η εφαρμογή στο πιο λεπτομερές επίπεδο του κελιού.

Ο MinGen είναι ένας αλγόριθμος που δίνει ελάχιστη γενίκευση από πολλές ελάχιστες γενικεύσεις βάσει της μέτρησης πληροφοριών που ονομάζεται ακρίβεια. Αντίθετα, η δυαδική αναζήτηση δίνει μία στις δύο γενικεύσεις παρά οποιονδήποτε λόγο. Αλλά το MinGen παρέχει έναν τρόπο προτίμησης μιας γενίκευσης από μια άλλη, η οποία έχει πιο χρήσιμες πληροφορίες που καθορίζονται με τον υπολογισμό της ακρίβειας ενός γενικευμένου πίνακα που δίνει ελάχιστη παραμόρφωση ενός πίνακα. Για τον υπολογισμό της απώλειας πληροφοριών, καθόρισαν μια μέτρηση που καταγράφει το ποσό της παραμόρφωσης σε έναν γενικευμένο πίνακα. Όσον αφορά την πολυπλοκότητα, ο MinGen δεν είναι αποδοτικός, επειδή κάνει εξαντλητική αναζήτηση όλων των πιθανών γενικεύσεων. Ως εκ τούτου,

δεδομένου του πίνακα μετρίου μεγέθους, ο αλγόριθμος παραμένει ανέφικτος και κατά συνέπεια ακατάλληλος για πρακτική εφαρμογή.

Η μέθοδος γενίκευσης από κάτω προς τα πάνω διατηρεί το βοηθητικό πρόγραμμα δεδομένων διατηρώντας παράλληλα το απόρρητο των δεδομένων. Στον προηγούμενο αλγόριθμο, η ποσότητα παραμόρφωσης δεδομένων υπολογίστηκε από τον αριθμό των επιπέδων ιεραρχίας που ανέβηκαν. Ο τρόπος επιλογής της λύσης σύμφωνα με την παραπάνω μέθοδο, δεν εγγυάται την ποιότητα της λύσης. Έτσι, η γενίκευση από κάτω προς τα πάνω προσαρμόζει την απώλεια πληροφοριών με βάση την εντροπία. Ο αλγόριθμος χρησιμοποιεί άπληστη μέθοδο για να ανέβει στην κατάσταση k-ανωνυμίας, επομένως, υπάρχει η πιθανότητα εξεύρεσης τοπικής βέλτιστης λύσης αντί για γενική βέλτιστη λύση. Λειτουργεί μόνο για σαφή χαρακτηριστικά και για συνεχή χαρακτηριστικά και απαιτεί εκ των προτέρων διακριτό δέντρο ταξινόμησης.

Η προσέγγιση από πάνω προς τα κάτω (TDS=Top-Down Specialization) χειρίζεται τόσο τα σαφή χαρακτηριστικά όσο και τα συνεχή. Δημιουργεί δυναμικό δέντρο ταξινόμησης για συνεχή χαρακτηριστικά που επιτρέπει στους χρήστες να σταματούν ανά πάσα στιγμή για να πάρουν έναν γενικευμένο πίνακα που ικανοποιεί την κατάσταση ανωνυμίας. Ο TDS λειτουργεί με συμπιεσμένο πίνακα. Ο συμπιεσμένος πίνακας είναι συνήθως μικρότερος από τον αρχικό πίνακα, ο οποίος μπορεί να τροποποιηθεί σε δεδομένα αποθηκευμένα στο δίσκο (disk-resident).

Η k-optimize είναι μια προσέγγιση από πάνω προς τα κάτω που λαμβάνει είσοδο ένα πλήρως γενικευμένο σύνολο δεδομένων και ειδικεύεται στο σύνολο δεδομένων για να πάρει μια k-ανώνυμη κατάσταση. Η μέθοδος εγγυάται μια βέλτιστη λύση. Χρησιμοποιεί διατεταγμένη διαίρεση καθορισμένης κατάτμησης στην οποία ο τομέας κάθε χαρακτηριστικού αντιπροσωπεύεται ως σύνολο με πλήρη ταξινόμηση. Για παράδειγμα, θεωρούμε την ηλικία = {10,12,25,31,35,45} ως ένα σύνολο κατά σειρά και πιθανό σύνολο διαστημάτων {[10-17,19-23,25-31] [32-41] [18, 42-50]}. Επιπλέον, η ελάχιστη τιμή κάθε διαστήματος μπορεί να χρησιμοποιηθεί για να δηλώσει το διάστημα όπως 1: [10-17, 19-23, 25-31], 2: [32=41] και 3: [18, 42-50].

Η ανώνυμη περιήγηση (incognito) είναι ένας αλγόριθμος που κάνει αναζήτηση από κάτω προς τα πάνω για να κατασκευάσει πλέγματα γενίκευσης για κάθε μεμονωμένο υποσύνολο οιονεί αναγνωριστικών. Δημιουργείται ένα πλέγμα και ελέγχεται αν η στήλη είναι ανώνυμη για την κατάσταση 0. Ο έλεγχος συνεχίζεται έως ότου εντοπίσει την ανώνυμη κατάσταση. Η ανώνυμη περιήγηση παρέχει πλήρη γενίκευση τομέα ενώ η δυαδική αναζήτηση δίνει μία ελάχιστη γενίκευση. Είναι το πρακτικό πλαίσιο για την παροχή ελάχιστων γενικεύσεων πλήρους τομέα, δηλαδή της εφικτής γενίκευσης που ξεπερνά τον προηγούμενο αλγόριθμο σε μεγάλες βάσεις δεδομένων. Η ανώνυμη περιήγηση δίνει αποτέλεσμα σε εκθετικό χρόνο, επομένως, έχουν αναπτυχθεί πολλές βελτιστοποιημένες εκδόσεις της ανώνυμης περιήγησης.

Ο αλγόριθμος Mondrian χρησιμοποιεί πολυδιάστατη μέθοδο κωδικοποίησης στην οποία η κωδικοποίηση στη γενικευμένη τιμή μπορεί να είναι διαφορετική για την ίδια τιμή χαρακτηριστικών, ανάλογα με τις άλλες τιμές των χαρακτηριστικών των οιονεί αναγνωριστικών σε αντίθεση με τη μέθοδο ανωνυμοποίησης μιας διάστασης, όπου η κωδικοποίηση στη γενικευμένη τιμή είναι ίδια για την ίδια τιμή των χαρακτηριστικών. Χρησιμοποιεί τον άπληστο αλγόριθμο για να βρει την κλάση ισοδυναμίας και στη συνέχεια η γενίκευση γίνεται με βάση ερωτήματα φόρτου εργασίας.

Η βέλτιστη ανωνυμοποίηση δικτυωτού πλέγματος (Optimal Lattice Anonymization-OLA) είναι ένας αλγόριθμος που βασίζεται στην προσέγγιση διαίρεσης και κατάκτησης. Χρησιμοποιεί προγνωστική

επισήμανση για να αποσυνθέσει ένα πλέγμα σε μικρότερες δευτερεύουσες συσκευές. Η OLA στοχεύει να βρει τον βέλτιστο κόμβο που είναι k-ανώνυμος με ελάχιστη απώλεια πληροφοριών. Όσον αφορά την εύρεση της γενικής βέλτιστης λύσης αποταυτοποίησης, η OLA βρέθηκε να είναι σταθερά ταχύτερη από την incognito. Αλλά ο χρόνος εκτέλεσης δεν είναι σταθερός, δεν εξαρτάται, από την αλλαγή της σειράς των στηλών στο σύνολο δεδομένων εισόδου. Για παράδειγμα, ένας κόμβος (1,0,0) αντιπροσωπεύει έναν διαφορετικό μετασχηματισμό εάν η πρώτη στήλη αλλάξει με μια άλλη στήλη το σύνολο δεδομένων. Ο χρόνος εκτέλεσης αλλάζει σημαντικά όταν αλλάζει η σειρά των στηλών, αν και σε περίπτωση φυσικής σειράς, η OLA αποδίδει καλύτερα από την ανώνυμη κατάσταση όσον αφορά τον χρόνο εκτέλεσης.

Ο flash είναι ένας σταθερός άπληστος αλγόριθμος. Διασχίζει το δικτυωτό πλέγμα με τον πρώτο προς τα κάτω τρόπο και οι διαδρομές θα δημιουργούνται συνεχώς. Επαναλαμβάνεται σε όλα τα επίπεδα στο πλέγμα, ξεκινώντας από το επίπεδο 0, χρησιμοποιώντας μια άπληστη αναζήτηση πρώτου βάθους προς τον επάνω κόμβο. Ο κόμβος που καθορίζεται από τον αλγόριθμο δυαδικής αναζήτησης ελέγχεται από την k-ανωνυμία. Ανάλογα με το αποτέλεσμα του ελέγχου, ο αλγόριθμος στη συνέχεια προχωρά με το κάτω ή το άνω μισό της διαδρομής. Ο γενικός βέλτιστος κόμβος προσδιορίζεται συγκρίνοντας το τρέχον τοπικό βέλτιστο με το τρέχον γενικό βέλτιστο. Ο χρόνος εκτέλεσης του αλγορίθμου παραμένει ίδιος παρά τη σειρά των στηλών στο σύνολο δεδομένων εισόδου. Η εκτέλεση του αλγόριθμου απαιτεί τα δεδομένα να βρίσκονται στην κύρια μνήμη. Επομένως, μετά την εκτέλεση πειραμάτων από τους δημιουργούς, ο βέλτιστος αριθμός οιονεί αναγνωριστικών για τα σύνολα δεδομένων ήταν 9. Ο υψηλός αριθμός οιονεί αναγνωριστικών οδηγεί σε δυσκολία κράτησης των στοιχείων δεδομένων στην κύρια μνήμη.

Η εικόνα 3 συνοψίζει την κατηγοριοποίηση αυτών των αλγορίθμων με βάση την ταξινόμηση των αλγορίθμων γενίκευσης. Γενικά, η ιδέα είναι να σχηματιστεί περισσότερος αριθμός ομάδων με μικρό μέγεθος ομάδας για να διατηρηθεί η ποιότητα των δεδομένων. Μέχρι τώρα, οι υπάρχοντες αλγόριθμοι επιτυγχάνουν 2k - 1 κατώτατο όριο στο μέγεθος των ομάδων ανωνυμοποίησης. Σε μη ασήμαντες περιπτώσεις, οι Qingming Tang και άλλοι επιτυγχάνουν χαμηλότερο ανώτερο όριο από αυτό του προηγούμενου αλγορίθμου[2]. Προκειμένου να βρουν k-ανώνυμη λύση, υιοθέτησαν προσέγγιση διαίρεσης και κατάκτησης παρόμοια με τον αλγόριθμο Mondrian. Σε κάθε επανάληψη, ο Mondrian χωρίζει την περιοχή σε δύο μέρη όσο το δυνατόν πιο ίσια. Ωστόσο, αυτό οδηγεί στη δημιουργία μικρού αριθμού ομάδων που υποβαθμίζουν την ποιότητα της γενίκευσης. Για παράδειγμα, μια περιοχή περιέχει 4k + 2 σημεία, χωρίζεται περαιτέρω σε δύο υποπεριοχές μεγέθους 2k - 1 και, στη συνέχεια, κάθε περιοχή δε μπορεί να χωριστεί περαιτέρω. Μπορεί να γίνει η καλύτερη έκδοση του διαμερίσματος, όπως (P1, P2, P3) όπου | P1 | = k; | P2 | = k και | P3 | = 2k - 2. Η ιδέα τους ήταν, δεδομένης μιας περιοχής που περιέχει n = ak + b σημεία να μπορεί να χωριστεί σε δύο μέρη, όπως n1 = a1k + b1 και n2 = a2k + b2 αντίστοιχα έτσι ώστε a1 + a2 <= a. Έτσι, για την παραγωγή περισσότερων ομάδων ανωνυμοποίησης στην τελική έκδοση, τα a1 + a2 θα πρέπει να μεγιστοποιηθούν.

Πολλοί αλγόριθμοι k-ανωνυμίας απαιτούν σημαντικό αριθμό προσβάσεων βάσης δεδομένων που μειώνουν την αποτελεσματικότητα του αλγορίθμου. Οι Nergiz και άλλοι πρότειναν έναν αλγόριθμο που χρησιμοποιεί τη δομή περίληψης που διατηρείται ήδη από το σύστημα διαχείρισης βάσης δεδομένων για επιλεκτικότητα ερωτήματος. Επομένως, ο αριθμός των προσβάσεων δεδομένων είναι μικρότερος. Κάνει μονή σάρωση δεδομένων, ενώ άλλοι αλγόριθμοι απαιτούν εκατοντάδες σαρώσεις.

Algorithm	Year	Top-down/bottom-up	Approach	Single dimensional /multidimensional	Feasible	Recoding	Anonymization method	k-minimal solution
μ-Argus	1996	Bottom-up	Greedy	Single	Y	Global	Generalization & suppression	N
Datafly	1997	Bottom-up	Greedy	Single	Y	Global	Generalization	N
Binary search	2001	bottom-up	Divide-conquer	Single	N	Global	Generalization	Single minimal full domain k-anonymization
MinGen	2002	bottom-up	Complete	Single	N	Global	Generalization	All minimal full domain k-anonymization
Bottom-up generalization	2004	Bottom-up	Greedy	Single	Y	Global	Generalization	Single minimal full domain k-anonymization
TDS (Top-Down Specialization)	2005	Top-down	Greedy	Single	Y	Global	Generalization	Single minimal full domain k-anonymization
K-OPTIMIZE	2005	Top-down	Complete	Single	Y	Global	Generalization & suppression	Optimal
Incognito	2005	Bottom-up	Complete	Single	Y	Global	Generalization	Minimal full-domain generalization
Mondrian	2006	Top-down	Greedy	Multi	Y	Local recoding	Generalization	Single multi-dimensional generalization
Ola	2009	Bottom-up	Divide-conquer	Single	Y	Global recoding	Generalization & suppression	Minimal full-domain generalization
Flash	2012	Bottom-up (breadth first)	Greedy	Single	Y	Global	Generalization	Minimal full-domain generalization

Εικόνα 3: Κατηγοριοποίηση αλγόριθμου k-ανωνυμίας[2]

2.3 Δεδομένα συναλλαγών

Τα συγκεκριμένα χαρακτηριστικά των δεδομένων συναλλαγών που διαφέρουν από τα σχεσιακά/δομημένα δεδομένα είναι η υψηλή διάσταση όπου υπάρχει τεράστιος αριθμός δραστηριοτήτων στον κόσμο, γεγονός που αυξάνει τη διάσταση, η αραιότητα όπου από πολλές δραστηριότητες μόνο λίγες ισχύουν για ορισμένα άτομα (ειδικά ασθενείς με μεγάλα προφίλ) και η έλλειψη χαρακτηριστικών οιονεί αναγνωριστικών όπου δεδομένου ότι τα δεδομένα είναι υψηλών διαστάσεων και αραιά, η επιλογή χαρακτηριστικών οιονεί αναγνωριστικών είναι πολύ δύσκολη.

Σε περίπτωση δεδομένων ασθενούς με μεγάλα προφίλ, τα δεδομένα είναι υψηλών διαστάσεων καθώς και αραιά. Χρησιμοποιούνται τα αραιά σχεσιακά σύνολα δεδομένων που διαχειρίζονται από την Ανώνυμη Αντιστοίχιση Δεδομένων Υψηλής Διάστασης (CAHD) χρησιμοποιώντας συσχέτιση μεταξύ αντικειμένων και για την ανωνυμοποίηση ευαίσθητων χαρακτηριστικών, χρησιμοποιείται το καμουφλάρισμα τιμής. Η ανάγκη κατάλληλης μεθόδου ανωνυμοποίησης για αραιό υψηλής διάστασης σύνολο δεδομένων αναγνωρίζεται από τους Narayanan και Shmatikov. Κατασκεύασαν αλγόριθμο απο-ανωνυμοποίησης που εκμεταλλεύεται το γεγονός πολύ μικρών ομοιοτήτων μεταξύ των εγγραφών σε αραιό σύνολο δεδομένων. Ο αλγόριθμος αποανωνυμοποίησε εγγραφές του Netflix για γνωστούς χρήστες και στη συνέχεια έμαθε για τις πολιτικές προτιμήσεις τους με άλλα ευαίσθητα δεδομένα στα προφίλ τους. Η έρευνα κατέληξε στο συμπέρασμα ότι χωρίς την εφαρμογή της κατάλληλης ανωνυμοποίησης, τα σύνολα δεδομένων υψηλών διαστάσεων είναι πολύ ευάλωτα στην ανωνυμοποίηση. Οι Άρης Γκουλαλάς-Διβάνης και άλλοι εντόπισαν την ανάγκη μιας μεθόδου για την προστασία της ιδιωτικής ζωής στα ιατρικά δεδομένα, ικανοποιώντας παράλληλα τον περιορισμό χρησιμότητας.

Το σύνολο δεδομένων συναλλαγών αποτελείται από το σύνολο δεδομένων του πραγματικού κόσμου που περιέχει αυθαίρετο σύνολο στοιχείων που έχουν επιλεγεί από ένα μεγάλο σύμπαν. Αυτά τα δεδομένα έχουν υψηλή διάσταση και δεν έχουν δομή. Για παράδειγμα, από ένα σύμπαν U κάθε άτομο μπορεί να επιλέξει έναν αυθαίρετο αριθμό δραστηριοτήτων (ποτό, κάπνισμα κ.λπ.) και ασθένεια. Στην εικόνα 4, το TID αναφέρεται σε κάθε χρήστη. Τα δεδομένα συναλλαγών έχουν πολλά οφέλη. Για παράδειγμα, οι πληροφορίες που συλλέγουν οι λιανοπωλητές σχετικά με τις αγοραστικές συνήθειες των πελατών έχουν πολύτιμα δεδομένα συναλλαγών που τους επιτρέπουν να προβλέψουν τη συμπεριφορά των αγορών σε διαφορετικές εποχές, η χειμερινή σεζόν θα έχει ως αποτέλεσμα κατακόρυφη αύξηση ηλεκτρικών κουβερτών ή θερμαντήρα δωματίου, οπότε η αποθήκευση σε αυτά τα είδη και η καλή σχεδίαση είναι απαραίτητη, διαφορετικά οι πελάτες θα κοιτάξουν αλλού. Στην υγειονομική περίθαλψη, οι κωδικοί διάγνωσης απαιτούν δημοσίευση για περαιτέρω έρευνα και στατιστικούς σκοπούς. Για παράδειγμα, μετά την κατάργηση του TID, η υπόλοιπη εικόνα 4 πρέπει να δημοσιευτεί για να εξορύξει τις πληροφορίες εάν ορισμένες δραστηριότητες μπορεί να προκύψουν συγκεκριμένες ιατρικές καταστάσεις.

TID	Activities	Medical history
T1 (Bob)	a, c, d, f, g	Diabetes
T2 (David)	a, b, c, f	Hepatitis
T3 (Claire)	b, d, f, x	Hepatitis
T4 (Andrea)	b, c, g, y, z	HIV
T5 (Ellen)	a, c, f, g	HIV

Εικόνα 4: Αρχεία καταγραφής διαγνωστικών με ιατρικό ιστορικό ευαίσθητων αντικειμένων[2]

Εξετάζεται το δημοσιευμένο σύνολο δεδομένων του διαγνωστικού αρχείου καταγραφής στην εικόνα 4, η οποία περιέχει τις πέντε ιατρικές συναλλαγές (το όνομα του ασθενούς διατηρείται ως ιδιωτικό) για την έρευνα σχετικά με τον κύκλο ζωής και την ασθένεια. Το ευαίσθητο στοιχείο είναι το ιατρικό ιστορικό και θεωρείται παραβίαση απορρήτου εάν αυτές οι πληροφορίες μπορούν να συσχετιστούν με ένα συγκεκριμένο άτομο. Παρόμοια με το σχεδόν αναγνωριστικό, οι μη ευαίσθητες δραστηριότητες μπορούν να χρησιμοποιηθούν από έναν εισβολέα για να επαναπροσδιορίσουν τις συναλλαγές του χρήστη. Σκεφτείτε τη συναλλαγή της Claire, η οποία έχει ηπατίτιδα. Ορισμένες από τις δραστηριότητες της Claire μπορούν εύκολα να μαθευτούν από έναν εισβολέα (Εύα), είτε από μια συνομιλία μαζί της, είτε από το να γνωρίζει κάποιες από τις συνήθειές της. Ας υποθέσουμε ότι η Claire μπορεί να παρευρεθεί σε ένα πάρτι, συμπεριλαμβανομένης της Εύας, και πίνει αλκοόλ που αναπαρίσταται ως b και καπνίζει που αναπαρίσταται ως d στην εικόνα 4. Κατά το συνδυασμό αυτών των πληροφοριών με το διαγνωστικό αρχείο καταγραφής, υπάρχει μόνο μία εγγραφή με τις δραστηριότητες b και d. Ως εκ τούτου, η Εύα μπορεί να επαναπροσδιορίσει τη συναλλαγή της Claire και να ανακαλύψει ότι η Claire μπορεί να έχει ηπατίτιδα. Οι διαγνωστικές λεπτομέρειες της Claire αναγνωρίστηκαν από την Εύα και μπορούν να την συνδέσουν με επιτυχία στο ευαίσθητο στοιχείο «Ιατρικό Ιστορικό». Πρέπει να αποτρέψουμε τη σχέση των στοιχείων QID της με ένα συγκεκριμένο ευαίσθητο στοιχείο για την προστασία του απορρήτου της Claire.

2.3.1 Εφαρμογή παραδοσιακών μεθόδων ανωνυμοποίησης δεδομένων συναλλαγών

Για να αποτραπούν οι επιθέσεις επαναπροσδιορισμού σε σχεσιακά δεδομένα, υπάρχουν μοντέλα απορρήτου k-ανωνυμίας και l-ποικιλομορφία. Η κύρια ιδέα είναι να σχηματιστούν "τάξεις ισοδυναμίας" σε ένα οιονεί αναγνωριστικό (QID), καθώς με το σχεσιακό σύνολο δεδομένων έχει έναν σταθερό αριθμό χαρακτηριστικών, είναι δυνατός ο ορισμός οιονεί αναγνωριστικού, π.χ., {Φύλο, ΤΚ, Ημερομηνία γέννησης}, έτσι ώστε οι εγγραφές να μη διακρίνονται στην ίδια κατηγορία ισοδυναμίας. Σε περίπτωση δεδομένων συναλλαγής, το QID θα περιέχει μια τιμή για κάθε δημόσιο στοιχείο του σύμπαντος U, αλλά στο πρακτικό σενάριο το U είναι πολύ μεγάλο για τα δεδομένα συναλλαγής. Ας υποθέσουμε ότι το U περιέχει 10.000 αντικείμενα από αυτά, όπου πολύ μικρό μέρος των στοιχείων ανήκει σε κάθε συναλλαγή, ας πούμε το 1% ή λιγότερο. Για τέτοια αραιότητα του QID, πρέπει να καταστείλουμε κυρίως όλα τα στοιχεία για να σχηματίσουμε κλάσεις ισοδυναμίας. Το ίδιο πρόβλημα αντιμετωπίστηκε από μια προηγούμενη μελέτη όπου φάνηκε ότι όταν τα δεδομένα περιέχουν μεγάλο αριθμό χαρακτηριστικών ως οιονεί αναγνωριστικά, τα δεδομένα φέρουν μεγάλη απώλεια πληροφοριών για την ανωνυμοποίηση των δεδομένων με παραδοσιακές μεθόδους. Ως εκ τούτου, οι μέθοδοι k-ανωνυμίας των σχεσιακών δεδομένων είναι ακατάλληλες για την ανωνυμοποίηση δεδομένων συναλλαγών.

2.3.2 Απειλές για το απόρρητο κατά τη δημοσίευση δεδομένων συναλλαγών

Η ασφαλής δημοσίευση δεδομένων συναλλαγών απαιτεί προστασία από δύο τύπους απειλών για το απόρρητο. Πρώτον είναι η απειλή για την αποκάλυψη ταυτότητας. Στα δημοσιευμένα δεδομένα, μια συγκεκριμένη συναλλαγή σχετίζεται με ένα άτομο, με αποτέλεσμα την αποκάλυψη ταυτότητας. Ας δούμε την απελευθέρωση δεδομένων στην εικόνα 5, η οποία περιέχει τα αρχεία αγορών πολλών ατόμων. Ας υποθέσουμε ότι ορισμένα αντικείμενα είναι ευαίσθητα π.χ. φάρμακο που επισημαίνεται με έντονα γράμματα και μπορεί να μην αρέσει να αγοράζει τέτοια είδη δημόσια. Για τα υπόλοιπα δημόσια αντικείμενα, οι ιδιώτες δεν θα ήθελαν να αποκαλύψουν την αγορά τους. Ας υποθέσουμε ότι ένας εισβολέας γνωρίζει ότι η Μαίρη έχει αγοράσει τα α, β και γ. Στην εικόνα 5, μόνο η πρώτη συναλλαγή περιέχει αυτές τις τιμές, έτσι ένας εισβολέας μπορεί να τη συσχετίσει με την πρώτη συναλλαγή. Ο δεύτερος τύπος επίθεσης είναι η αποκάλυψη χαρακτηριστικών: όταν ένα σύνολο ευαίσθητων στοιχείων πρέπει να συσχετιστεί με ένα άτομο. Ας υποθέσουμε ότι ένας εισβολέας γνωρίζει την αγορά των στοιχείων c και d από τον Tom. Στην εικόνα 5, υπάρχουν δύο συναλλαγές που περιέχουν c και d, επομένως ένας εισβολέας δεν μπορεί να συνδέσει τον Tom με μια συγκεκριμένη συναλλαγή, αλλά ο εισβολέας μπορεί να βρει ότι ο Tom αγόρασε ένα ευαίσθητο στοιχείο g, καθώς το g είναι κοινό και στις δύο συναλλαγές.

Name	Purchased items
Mary	a b c d **g**
Bob	a c e f **h i**
Tom	b c d **g j**
Anne	e f **g h**
Brad	a b d e **j**
Jim	c f **i**

Εικόνα 5: Ένα παράδειγμα αρχικού συνόλου δεδομένων[2]

2.4 Μοντέλα απορρήτου: Ανωνυμοποίηση κωδικού διάγνωσης

Πολλά μοντέλα απορρήτου έχουν προταθεί στο παρελθόν για την προστασία από επιθέσεις αποκάλυψης ταυτότητας κατά την κοινή χρήση κωδικών διάγνωσης. Έστω D = σύνολο N συναλλαγών {T1, . . . , TN } και |D| δηλώνει το μέγεθος του D. T = ⟨Tid,I⟩ = συναλλαγή T πάνω από το στοιχείο I, όπου Tid ένα μοναδικό αναγνωριστικό και το I είναι ένα σύνολο στοιχείων και ⟨Tid,J⟩ = μια συναλλαγή που υποστηρίζει ένα σύνολο στοιχείων I, εάν I ⊆ J. Sup (a,D) = αριθμός συναλλαγών στο D που υποστηρίζουν a (αριθμός συναλλαγών στο D που περιέχουν το στοιχείο a). a = το σύνολο των ευαίσθητων στοιχείων στο I, b = το σύνολο των μη ευαίσθητων στοιχείων στο I όπου a ∪ b = I. Το D' υποδηλώνει την ανώνυμη μορφή του D.

Οι προηγούμενες γνώσεις που απαιτούνται από έναν εισβολέα για να κάνει μια επίθεση είναι: ορισμένα δημόσια στοιχεία b στο D και μία από τις συναλλαγές στο D ανήκει σε ένα άτομο. Αυτή η επίθεση μπορεί να οριστεί ως b-> a, όπου a είναι κάποιο ιδιωτικό στοιχείο και το Sup(b), το μέγιστο του b, υποδηλώνει τον αριθμό των συναλλαγών που περιέχουν το b ως υποσύνολο. Η πιθανότητα μια συναλλαγή να περιέχει a, δεδομένου ότι περιέχει b, είναι P(b− > a) = Sup(b ∪ a)/ Sup(b).

Για παράδειγμα, η εικόνα 7a δείχνει το μικρό στιγμιότυπο του συνόλου δεδομένων που χρησιμοποιεί τον κωδικό ICD 9 και η εικόνα 6 δείχνει την περιγραφή του κώδικα ICD. Ο εισβολέας έχει την προηγούμενη γνώση του κωδικού διάγνωσης b = {716, 924} και σκοπεύει να συναγάγει τον κώδικα διάγνωσης a = 436. Ο εισβολέας βρίσκει ότι, από δύο συναλλαγές που περιέχουν b, η μία περιέχει επίσης a, δηλαδή Sup(b ∪ a,D) = 1 και Sup(b,D) = 2. Επομένως, P(b-> a) = 1/2. Έτσι, υπάρχει 50% πιθανότητα η Τζέιν να έχει διαγνωστεί με κωδικό διάγνωσης 436.

ICD 9 code	Description
716	Other and unspecified arthropathies
924	Accident caused by hot substance or object, caustic or corrosive material, and steam
562	Diverticula of intestine
300	Anxiety, dissociative and somatoform disorders
487	Influenza
309	Adjustment reaction
346	**Migraine**
436	**Acute, but ill-defined, cerebrovascular disease**
429	**Ill-defined descriptions and complications of heart disease**
553	**Other hernia of abdominal cavity without mention of obstruction or gangrene**

Εικόνα 6:Περιγραφή του κωδικού ICD 9, ο έντονος κωδικός ICD υποδηλώνει τον ευαίσθητο κωδικό ICD και οι υπόλοιποι είναι οι δημόσιοι κωδικοί ICD[2]

Πλήρης k-ανωνυμία

Η πλήρης k-ανωνυμία είναι ένα μοντέλο στο οποίο ελάχιστες k εγγραφές έχουν τον ίδιο κωδικό διάγνωσης στο δημοσιευμένο σύνολο δεδομένων και ταυτόχρονα θεωρείται ότι η αποκάλυψη ταυτότητας μπορεί να συμβεί με οποιονδήποτε συνδυασμό κωδικού διάγνωσης. Αλλά η αναγνώριση όλων των κωδικών διάγνωσης σε ένα αρχείο ασθενούς είναι εξαιρετικά δύσκολη. Η πλήρης ανωνυμία μπορεί να βλάψει τη χρησιμότητα δεδομένων.

Δίνεται μια γενικευμένη έκδοση D’ του D και η παράμετρος k ∈ [2, N], εάν υπάρχει συναλλαγή t ∈ D, για κάθε σύνολο στοιχείων b μιας συναλλαγής. Το D’ λέγεται ότι είναι πλήρες k-ανώνυμο αν και μόνο αν Sup(b, D’) >= k.

Για παράδειγμα, στην εικόνα 8a, ο κωδικός διάγνωσης 716–553 έχει αντικατασταθεί από ένα γενικευμένο στοιχείο (716, 924, 562, 300, 487, 309, 346, 436, 429, 553) ώστε να ικανοποιεί την πλήρη εξατομικευμένη ανωνυμία, μήπως η ταυτότητα του ασθενούς συνδέεται με λιγότερες από έξι συναλλαγές σε σχέση με οποιονδήποτε συνδυασμό των κωδικών διάγνωσης 716–553.

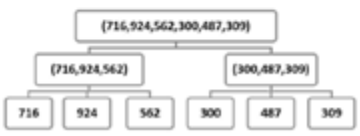
a)

Name	Diagnoses Code
Mary	716 924 562 300 **346 436 429 553**
Bob	487 309 **436 429**
Tom	300 **346 553**
Anne	487 309 **346 436**
Brad	716 924 300 487 **429**
Jim	562 309 **553**

b)

Diagnoses Code
(716,924,562) (300,487,309)**346 436 429 553**
(300,487,309) **436 429**
(300,487,309)**346 553**
(300,487,309) **346 436**
(716,924,562) (300,487,309)**429**
(716,924,562) (300,487,309)**553**

c)



d)

Diagnoses Code
716 (924,562) 300 **346 436 429 553**
487 309 **436 429**
300 **346 553**
487 309 **346 436**
716 (924,562) 300 487 **429**
(924,562)309 **553**

e)

PS-rules
716->553
562 300->346
300->436 429

Εικόνα 7: (a) αρχικό σύνολο δεδομένων που περιέχει δημόσια και ευαίσθητα στοιχεία, (b) 2^2-ανώνυμα δεδομένα και (0,5, 6, 2)-συνεκτική εκδοχή της, (c) ιεραρχία γενίκευσης, (d) γενίκευση συνόλου τιμών με βάση το μοντέλο βασισμένο σε κανόνες ειδικά στο (e) και (e) κανόνες PS για το (d)[2].

a)

Diagnoses Code
(716,924,562,300,487,309,346,436,429,553)
(716,924,562,300,487,309,346,436,429,553)
(716,924,562,300,487,309,346,436,429,553)
(716,924,562,300,487,309,346,436,429,553)
(716,924,562,300,487,309,346,436,429,553)
(716,924,562,300,487,309,346,436,429,553)

b)

Diagnoses Code
(716,924,562) (300,487,309) **346 436 429 553**
(300,487,309) **436 429**
(300,487,309) **346 553**
(300,487,309) **346 436**
(716,924,562) (300,487,309) **429**
(716,924,562) (300,487,309) **553**

Εικόνα 8:Ένα παράδειγμα των (a), (b) δύο ανώνυμων εκδόσεων της εικόνας 7a[2].

K^m-ανωνυμία

Η k^m-ανωνυμία είναι ένα πιο ευέλικτο μοντέλο απορρήτου. Η παράμετρος m χρησιμοποιείται στην ανωνυμία k^m για τη ρύθμιση του μέγιστου αριθμού των κωδικών διάγνωσης που μπορεί να αναγνωριστούν από έναν εισβολέα και κάθε συνδυασμός m κωδικών διάγνωσης απαιτείται να εμφανίζεται σε τουλάχιστον k εγγραφές του συνόλου δεδομένων που κυκλοφόρησε. Αυτό το μοντέλο απορρήτου είναι κατάλληλο για περιπτώσεις όπου οι εκδότες δεδομένων δεν είναι σε θέση (ή δε θέλουν) να αναφέρουν συγκεκριμένα σύνολα κωδικών διάγνωσης που οδηγούν σε επιθέσεις αποκάλυψης ταυτότητας.

Δίνεται μια γενικευμένη έκδοση D’ του D και η παράμετρος $k \in [2, N]$ και $m \in [2, N]$, εάν υπάρχει συναλλαγή $t \in D$, οποιοδήποτε υποσύνολο στοιχείων b μεγέθους m. Το D’ λέγεται ότι είναι k^m-ανώνυμο αν και μόνο αν $Sup(b, D') >= k$.

Για παράδειγμα, στην εικόνα 7a ο συνδυασμός του μη ευαίσθητου κωδικού διάγνωσης 716, 562 εμφανίζεται μόνο σε μία συναλλαγή. Ως εκ τούτου, ο πίνακας δεν είναι 2^2-ανώνυμος. Στην εικόνα 8b, τα στοιχεία 716–562 έχουν αντικατασταθεί από ένα αντικείμενο (716, 924, 562), ενώ τα στοιχεία 300 έως 309 έχουν αντικατασταθεί από (300 487 309). Έτσι, οποιοδήποτε ζεύγος κωδικών διάγνωσης 716-309 περιέχεται από τουλάχιστον δύο συναλλαγές στην εικόνα 8b.

ρ-αβεβαιότητα

Πολλά μοντέλα απορρήτου έχουν προταθεί στο παρελθόν για την παροχή προστασίας από επιθέσεις αποκάλυψης χαρακτηριστικών κατά την κοινή χρήση κωδικών διάγνωσης. Η ρ-αβεβαιότητα περιορίζει την πιθανότητα συσχέτισης ενός ατόμου με οποιονδήποτε κωδικό διάγνωσης σε λιγότερο από ρ. Οι υποθέσεις που κάνει αυτό το μοντέλο είναι ότι ο εισβολέας μπορεί να έχει τη γνώση οποιωνδήποτε κωδικών διάγνωσης και όλοι οι υπόλοιποι κωδικοί διάγνωσης μπορούν να χρησιμοποιηθούν για τη σύνδεση του εάν ο κώδικας είναι ευαίσθητος ή μη. Ως εκ τούτου, αυτό το μοντέλο προστατεύει από ευαίσθητους συσχετισμούς χωρίς να περιορίζει τη φύση της γνώσης ενός αντιπάλου.

Λαμβάνοντας υπόψη ένα γενικευμένο σύνολο δεδομένων D' του D, και τις παραμέτρους ρ ∈ [0,1], εάν υπάρχει οποιαδήποτε συναλλαγή t ∈ D, οποιοδήποτε υποσύνολο στοιχείων b και οποιοδήποτε ευαίσθητο στοιχείο a, το D' λέγεται ότι είναι ρ-αβεβαιότητα εάν και μόνο αν, Sup(b ∪ a, D')/Sup(b, D') <= ρ.

Η ρ-αβεβαιότητα περιορίζει την πιθανότητα συσχέτισης ενός ασθενούς με οποιονδήποτε από τους ευαίσθητους κωδικούς διάγνωσης μικρότερο από ρ. Για παράδειγμα, στην εικόνα 7b, εάν ένας εισβολέας γνωρίζει ότι ένας ασθενής σχετίζεται με τον κωδικό διάγνωσης 716 924 562 300 487 309 και τον ευαίσθητο κωδικό διάγνωσης 429, τότε με πιθανότητα 2/3 (66,7%), μπορεί να συσχετίσει τον ασθενή με έναν άλλο ευαίσθητο κωδικό διάγνωσης 553. Ως εκ τούτου, ο πίνακας δεν ικανοποιεί την αβεβαιότητα 0,5. Αλλά δεν εμποδίζει την αποκάλυψη ταυτότητας. Αρκετά ακατάλληλο όταν η αποκάλυψη ταυτότητας είναι νομική απαίτηση.

(h; k; p)- συνοχή

Ένα άλλο μοντέλο απορρήτου, που ονομάζεται (h; k; p)- συνοχή προστατεύει τόσο από την ταυτότητα όσο και από την αποκάλυψη ευαίσθητων χαρακτηριστικών. Οι μη ευαίσθητοι κωδικοί διάγνωσης σε αυτό το μοντέλο αντιμετωπίζονται με τον τρόπο που αντιμετωπίζονται σε k^m-ανωνυμία και περιορίζουν την πιθανότητα συλλογής ευαίσθητων κωδικών διάγνωσης. Οι παράμετροι k και p είναι ίδιοι με τις k και m στην ανωνυμία k^m και το h περιορίζει την πιθανότητα αποκάλυψης χαρακτηριστικών.

Δίνεται ένα γενικευμένο σύνολο δεδομένων D' του D και των παραμέτρων h∈ [0,1], k∈ [2,N] και p∈ [2,N], εάν υπάρχει συναλλαγή t ∈ D, οποιοδήποτε υποσύνολο στοιχείων b και οποιοδήποτε ευαίσθητο στοιχείο a. Το D' λέγεται ότι είναι (h, k, p)-συνεκτικό αν και μόνο αν Sup(b, D') >= k και Sup(ba, D')/Sup(b, D') <= h.

Για παράδειγμα, δίνεται k = 3, p = 3, h = 80%.

P(300 487 309− > 346) = 3/6 = 1/2 ∗ 100 = 50% < h

P(716 924 562− > 346) = 1/3 = 1/3 ∗ 100 = 33% < h

P(716 924 562− > 436) = 1/3 = 1/3 ∗ 100 = 33% < h

P(300 487 309− > 436) = 3/6 = 1/2 ∗ 100 = 50% < h

P(716 924 562− > 429) = 2/3 = 2/3 ∗ 100 = 66% < h

P(300 487 309− > 429) = 2/3 = 2/3 ∗ 100 = 66% < h

P(716 924 562− > 553) = 2/3 = 2/3 ∗ 100 = 66% < h

P(300 487 309− > 553) = 3/6 = 3/6 ∗ 100 = 50% < h

Η (h, k, p) - συνοχή αποτρέπει τόσο την αποκάλυψη ταυτότητας όσο και την αποκάλυψη ευαίσθητων χαρακτηριστικών. Στην εικόνα 7b είναι (0.8,3,3)-συνοχή που δηλώνει ότι η αναλογία επιτυχίας της αποτροπής ενός εισβολέα να αναγνωρίσει οποιονδήποτε από τους ευαίσθητους κωδικούς διάγνωσης

από 346 έως 553 παρά το γεγονός ότι γνωρίζει οποιοδήποτε ζεύγος κωδικών διάγνωσης 716 έως 309, είναι 0,8. Η υπόθεση στην οποία βασίζεται αυτή η αρχή είναι ότι κάθε συνδυασμός μη ευαίσθητων κωδικών διάγνωσης μπορεί να προκαλέσει επίθεση αποκάλυψης ταυτότητας. Επομένως, κάθε κωδικός διάγνωσης πρέπει να προστατεύεται είτε από αποκάλυψη ταυτότητας είτε από επίθεση αποκάλυψης ευαίσθητων πληροφοριών. Σε εφαρμογές δημοσίευσης ιατρικών δεδομένων, όπου μόνο συγκεκριμένα σύνολα κωδικών διάγνωσης μπορούν να συνδεθούν ή να είναι ευαίσθητα, η εφαρμογή της συνοχής (h, k, p) μπορεί να προκαλέσει μεγάλη απώλεια πληροφοριών που δεν είναι επιθυμητό.

PS- κανόνας (Privacy Sensitive rule) ανωνυμία

Οι παραπάνω προσεγγίσεις έλαβαν πολύ περιοριστική παραδοχή του απορρήτου. Πιο συγκεκριμένα, η προστασία από την αποκάλυψη ταυτότητας απαιτείται όταν ο εισβολέας γνωρίζει είτε όλους τους συνδυασμούς αντικειμένων είτε σύνολα αντικειμένων συγκεκριμένου μεγέθους και προστατεύει όλα τα ευαίσθητα στοιχεία από επίθεση αποκάλυψης ευαίσθητων πληροφοριών. Στην πραγματικότητα, αυτό το σενάριο δεν αναμένεται από έναν επιτιθέμενο. Ωστόσο, στην περίπτωση πραγματικών εφαρμογών (π.χ. βιοϊατρική), μόνο συγκεκριμένα σύνολα αντικειμένων μπορούν να προκαλέσουν επίθεση αποκάλυψης ταυτότητας και έχουν ορισμένα ευαίσθητα στοιχεία. Για παράδειγμα, μόνο οι κοινωνικά στιγματισμένες διαγνώσεις, όπως ο HIV ή ο καρκίνος, θεωρούνται ευαίσθητες. Έτσι, η χρήση ομοιόμορφων υποθέσεων απορρήτου για την ανωνυμοποίηση δεδομένων μπορεί να οδηγήσει σε υπερβολική παραμόρφωση δεδομένων που δεν είναι απαραίτητη. Για παράδειγμα, στην εικόνα 5, εάν τα a, b και c είναι τα μόνα στοιχεία που μπορούν να χρησιμοποιηθούν από έναν εισβολέα για σύνδεση με μια εξωτερική πηγή δεδομένων, τότε μόνο αυτά τα στοιχεία πρέπει να προστατεύονται από επίθεση αποκάλυψης ταυτότητας. Ωστόσο, θα παρέχεται προστασία για όλα τα μη ευαίσθητα αντικείμενα που αποτελούνται από οποιαδήποτε 3 μη ευαίσθητα αντικείμενα χρησιμοποιώντας τις μεθόδους που προτείνονται από τους Takahashi και άλλους που προκαλούν περιττή απώλεια πληροφοριών. Το μοντέλο ανωνυμίας που βασίζεται σε PS κανόνα, σε αυτό μπορούμε να καθορίσουμε λεπτομερείς και ευέλικτες απαιτήσεις απορρήτου. Επιβάλλει την προστασία τόσο από την αποκάλυψη ταυτότητας όσο και από την αποκάλυψη ευαίσθητων πληροφοριών. Σε αυτό το μοντέλο, ο εκδότης δεδομένων μπορεί να αναφέρει λεπτομερείς απαιτήσεις προστασίας και για τους δύο τύπους αποκαλύψεων. Παρόμοια με τους κανόνες συσχέτισης, ο PS κανόνας περιέχει δύο σετ κωδικών διάγνωσης, που ονομάζονται ως προγενέστεροι και ως επακόλουθοι. Το προγενέστερο και το επακόλουθο περιέχουν κωδικούς διάγνωσης που μπορεί να οδηγήσουν σε επιθέσεις αποκάλυψης ταυτότητας και αποκάλυψης ευαίσθητων πληροφοριών, αντίστοιχα. Θεωρούμε έναν κανόνα PS A − > B, όπου το A είναι προγενέστερο και το B είναι επακόλουθο. Σύμφωνα με την ανωνυμία που βασίζεται στον κανόνα PS, τα ανώνυμα δεδομένα πρέπει να ακολουθούν ορισμένες προϋποθέσεις.

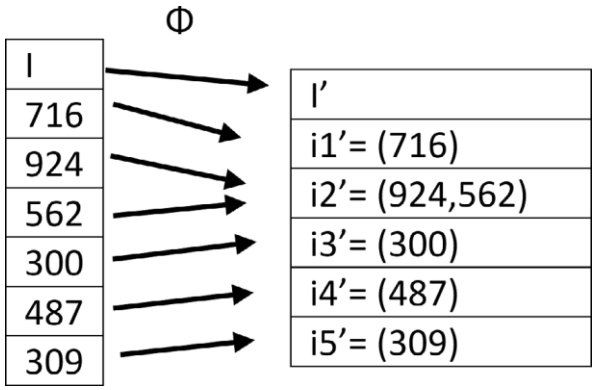
Συνθήκη 1: οι κωδικοί διάγνωσης στο A πρέπει να βρίσκονται σε τουλάχιστον k συναλλαγές του ανώνυμου συνόλου δεδομένων.

Συνθήκη 2: το ποσοστό των συναλλαγών που περιέχουν τους κωδικούς διάγνωσης στο A και περιέχουν επίσης τον κωδικό διάγνωσης στο B, θα πρέπει να είναι το πολύ (c*100)% όπου η παράμετρος c είναι παρόμοια με το όριο εμπιστοσύνης στην εξόρυξη κανόνων συσχέτισης που καθορίζεται από εκδότες δεδομένων. Στην περίπτωση κωδικών διάγνωσης, το μοντέλο έχει πολλά πλεονεκτήματα σε σύγκριση με τα προηγούμενα μοντέλα. Για παράδειγμα, προστατεύει τόσο από τον τύπο ταυτότητας αποκαλύψεων

όσο και από ευαίσθητες πληροφορίες, χρησιμοποιώντας αυτό το μοντέλο οι λεπτομερείς απαιτήσεις απορρήτου μπορούν να καθοριστούν από τους εκδότες δεδομένων και η γενικότητα του μοντέλου είναι μεγαλύτερη από αυτά τα μοντέλα, που αυτά τα μοντέλα είναι εξειδικευμένα σενάρια ανωνυμίας βάσει κανόνων PS.

Ένας κανόνας PS είναι μια συνεπαγωγή I → J, όπου I είναι ένα σύνολο στοιχείων στο P και το J είναι ένα σύνολο στοιχείων στο S. Δίνεται μια γενικευμένη έκδοση ˜D του D, που παράγεται χρησιμοποιώντας το μοντέλο γενίκευσης που βασίζεται σε σύνολο, και τις παραμέτρους k ∈ [2 , N] και c ∈ [0, 1], ένας κανόνας PS b→a προστατεύεται σε ˜D εάν (1) Sup(b, D') ≥ k, και (2) Sup(b ∪ a,D')/Sup(b, D')< = c, P->S όπου η αριστερή πλευρά P είναι η προγενέστερη και η δεξιά πλευρά S είναι η επακόλουθη. Δεδομένου ότι δεν υπάρχουν περιορισμοί στη χρήση των συνόλων στοιχείων για το P και το S, οι αυστηρές απαιτήσεις απορρήτου μπορούν να καθοριστούν και για τους δύο τύπους γνωστοποιήσεων. Οι συναλλαγές ανωνυμοποιούνται χρησιμοποιώντας μοντέλο ανωνυμοποίησης βάσει συνόλου.

Χρησιμοποιώντας ανωνυμοποίηση βάσει συνόλου, ο κατασκευαστής γενικευμένου συνόλου στοιχείων για το σύνολο στοιχείων I αναπαρίσταται ως I' = U ∀i∈ IΦ(i) όπου το U είναι ο κατασκευαστής γενικευμένου συνόλου στοιχείων και το i υποδηλώνει στοιχεία. Για παράδειγμα, ο κωδικός διάγνωσης 716 θα γενικευτεί στο 716, ο κωδικός 924 θα γενικευτεί στο (924, 562), ο κωδικός 562 θα γενικευτεί επίσης στο (924, 562), ο κωδικός 300 θα γενικευτεί στο 300, ο κωδικός 487 στο 487 και ο κωδικός 309 έως 309 όπως φαίνεται στον πίνακα 7d. Ας ελέγξουμε τη δυνατότητα εφαρμογής των κανόνων PS που αναφέρονται στον πίνακα 7e. Παρατηρούμε τον κανόνα PS 562 300→ 346, με προστασία για k = 2 και c = 0,5, καθώς υπάρχουν δύο συναλλαγές που υποστηρίζουν το γενικευμένο προηγούμενο U∀i ∈ {562, 300}, Φ(i) = (924, 562) 300, σύμφωνα με την εικόνα 9 και μόνο ένα από αυτά υποστηρίζει (924, 562)300U346. Αυτό υποδηλώνει ότι εάν ένας εισβολέας γνωρίζει ότι η Mary έχει διαγνωστεί με 562 και 300, δεν μπορεί να συμπεράνει την πραγματική συναλλαγή της Mary επειδή υπάρχουν δύο συναλλαγές που περιέχουν (924, 562)300 ούτε τον ευαίσθητο κωδικό διάγνωσης 346 της Mary με πιθανότητα μεγαλύτερη από 1/2 .



Εικόνα 9: Ένα παράδειγμα ανωνυμοποίησης βάσει συνόλου[2].

Privacy-constrained anonymity (Ανωνυμία που περιορίζεται στο απόρρητο)

Η ανωνυμία που περιορίζεται στο απόρρητο βασίζεται στην έννοια των περιορισμών απορρήτου. Η πολιτική απορρήτου είναι κατασκευασμένη σύμφωνα με τα σύνολα κωδικών διάγνωσης που μπορεί να

γνωρίζει ένας εισβολέας. Σε αυτό το μοντέλο, μόνο εκείνοι οι κωδικοί διάγνωσης που εμφανίζονται στην πολιτική απορρήτου πρέπει να προστατεύονται από επίθεση αποκάλυψης ταυτότητας. Αυτό έχει σημαντικά πλεονεκτήματα σε σχέση με την πλήρη k-ανωνυμία και k^m-ανωνυμία. Για παράδειγμα, δεν προστατεύει υπερβολικά τα δεδομένα και διατηρεί καλύτερα τη χρησιμότητα των δεδομένων. Εφόσον το μοντέλο απαιτεί την προσχεδιασμένη ιδέα των στοχευμένων κωδικών διάγνωσης από έναν εισβολέα, μερικές φορές γίνεται δύσκολο να αποκτηθεί αυτή η γνώση.

Έτσι, μέχρι τώρα οι κανόνες PS φαίνεται να είναι οι καλύτεροι για την ανωνυμοποίηση του κώδικα διάγνωσης, επειδή το μοντέλο είναι πολύ ευέλικτο με χαμηλή απώλεια πληροφοριών, αλλά η πολυπλοκότητα της εφαρμογής των κανόνων PS καθιστά δύσκολη την εφαρμογή. Επομένως, εξαρτάται από τη συνθήκη. Αν υποθέσουμε ότι η προστασία από την αποκάλυψη ταυτότητας απαιτείται μόνο τότε η k^m-ανωνυμία φαίνεται να είναι η καλύτερη, όμως εάν η προστασία από την αποκάλυψη ευαίσθητων πληροφοριών είναι η νομική απαίτηση, τότε η ρ-αβεβαιότητα δίνει το καλύτερο αποτέλεσμα. Εάν το σύνολο δεδομένων απαιτεί προστασία και από τις δύο επιθέσεις, τότε υπάρχουν μόνο δύο επιλογές που έχουμε τη (h, k, p) - συνοχή και τον κανόνα PS. Σε περίπτωση (h, k, p) συνοχής η απώλεια πληροφοριών είναι υψηλή και στην περίπτωση του κανόνα PS, η υπολογιστική πολυπλοκότητα είναι υψηλή επειδή υπάρχει πρόσθετη απαίτηση ελέγχου για τον κίνδυνο αποκάλυψης ευαίσθητων συνόλων στοιχείων, που περιλαμβάνει υπολογισμούς υποστήριξης για μεγάλο αριθμό συνόλων στοιχείων. Αυτό αυξάνει την πολυπλοκότητα του κανόνα PS. Η πολυπλοκότητα στη χειρότερη περίπτωση θα είναι O (αριθμός κανόνων* μέγεθος δεδομένων).

Επομένως, θα πρέπει να αναπτυχθεί ένας αποτελεσματικός αλγόριθμος που θα χρησιμοποιεί δύο διαφορετικές αρχές για να παρέχει προστασία τόσο από την αποκάλυψη ταυτότητας όσο και από την αποκάλυψη ευαίσθητων πληροφοριών. Έτσι, η απόφαση εξαρτάται από τον κάτοχο των δεδομένων και την απαίτηση του συνόλου δεδομένων.

2.5 Αλγόριθμοι ανωνυμοποίησης

Τα δεδομένα συναλλαγών είναι υψηλών διαστάσεων και αραιά. Έτσι, οι αλγόριθμοι που λειτουργούν για την ανωνυμοποίηση σχεσιακών δεδομένων δε μπορούν να εφαρμοστούν στην ανωνυμοποίηση δεδομένων συναλλαγών. Εάν εφαρμοστούν, τα δεδομένα θα υποστούν μεγάλη απώλεια πληροφοριών και θα παρέχουν χαμηλότερη χρησιμότητα δεδομένων. Εάν η k-ανωνυμία εφαρμόζεται στα δεδομένα συναλλαγής, αντιμετωπίζει όλα τα στοιχεία ως οιονεί αναγνωριστικά (QID) που οδηγεί σε σημαντικά χαμηλότερη χρησιμότητα δεδομένων. Για να επιτύχουν k-ανωνυμία στα δεδομένα συναλλαγών, οι Motwani και Nabar εφήρμοσαν τον αλγόριθμο προσέγγισης και τη στρατηγική καταστολής. Η CAHD (Correlation-aware Anonymization of High-dimensional Data), χρησιμοποιεί έναν άπληστο ευρετικό αλγόριθμο και βασίζεται στη συσχέτιση δεδομένων. Οι συναλλαγές οι οποίες ομαδοποιούνται βρίσκονται σε κοντινή απόσταση και αντιπροσωπεύονται στον πίνακα ζώνης. Αυτό οδηγεί σε υψηλότερη χρησιμότητα δεδομένων από την προηγούμενη. Χρησιμοποίησαν τη γενίκευση και την ανατομία για να ανωνυμοποιήσουν τα δεδομένα. Η επεκτασιμότητα των αλγορίθμων ορίζεται ως η αύξηση του χρόνου εκτέλεσης με την αύξηση του μεγέθους του συνόλου δεδομένων ή της τιμής του k. Εάν ο χρόνος εκτέλεσης αυξάνεται γραμμικά με την αύξηση του μεγέθους των δεδομένων ή της τιμής του k, λέμε ότι ο αλγόριθμος είναι επεκτάσιμος, αλλιώς εάν ο χρόνος εκτέλεσης αυξάνεται εκθετικά αυξάνοντας το

μέγεθος του συνόλου δεδομένων ή την τιμή του k, λέμε ότι ο αλγόριθμος δεν είναι επεκτάσιμος. Στη συνέχεια παρουσιάζονται οι σημαντικοί αλγόριθμοι για την ανωνυμοποίηση των δεδομένων συναλλαγών.

Ο Apriori χρησιμοποιεί μια επαναληπτική και από κάτω προς τα πάνω στρατηγική για να επιβάλλει την ανωνυμία των k^m. Βασίζεται στον αλγόριθμο κανόνων συσχέτισης Apriori. Η ιεραρχία διασχίζεται με τρόπο από κάτω προς τα πάνω, με ευρεία εμβέλεια, μέσω ενός μοντέλου παγκόσμιας γενίκευσης που βασίζεται στην ιεραρχία. Με προοδευτικό τρόπο, τα στοιχεία που χρειάζονται προστασία εξετάζονται, δηλαδή από ένα μεμονωμένο στοιχείο σε m σετ στοιχείων για να επιτευχθεί η ανωνυμία k^m, αλλά οδηγεί σε μεγαλύτερη απώλεια πληροφοριών. Ο αλγόριθμος επιλύει το πρόβλημα διαστάσεων των δεδομένων συναλλαγής. Στη χειρότερη περίπτωση, ο αλγόριθμος σαρώνει τη βάση δεδομένων m-φορές. Ο αλγόριθμος κλιμακώνεται καλά με το n πλήθος στοιχείων και συναλλαγών, αλλά υπό περιορισμένη μνήμη ο αλγόριθμος αποτυγχάνει. Η τελική λύση είναι κοντά στη βέλτιστη στις περισσότερες περιπτώσεις.

Ο Xu και άλλοι πρότειναν τον άπληστο (Greedy) αλγόριθμο που λειτουργεί με βάση την αρχή της συνοχής (h, k, p). Προστατεύει τα δεδομένα τόσο από τον τύπο ταυτότητας επιθέσεων όσο και από την αποκάλυψη ευαίσθητων χαρακτηριστικών. Εάν ο αλγόριθμος εφαρμόζεται για την προστασία του κώδικα διάγνωσης, μπορεί να προκαλέσει σημαντική απώλεια πληροφοριών, επειδή χρησιμοποιείται καταστολή στον αλγόριθμο που προκαλεί μεγαλύτερη απώλεια πληροφοριών σε σύγκριση με τη γενίκευση, και στη δημοσίευση ιατρικών δεδομένων απαιτείται το λεπτομερές απόρρητο, για το οποίο η (h, k, p) συνοχή δε λαμβάνεται υπόψη. Η επεκτασιμότητα του αλγορίθμου δεν έχει συζητηθεί.

Ο Suppress Control είναι ένας άπληστος, παγκόσμιος αλγόριθμος βασισμένος σε καταστολή ο οποίος επιβάλλει την ρ-αβεβαιότητα. Η καταστολή εφαρμόζεται τόσο σε ευαίσθητα όσο και σε μη ευαίσθητα είδη, διατηρώντας τον κανόνα συσχέτισης ευαίσθητου χαμηλότερου από ρ ενώ η απώλεια ελαχιστοποιείται. Καταστέλλει σχεδόν το 90% των ευαίσθητων στοιχείων και το 60% των μη ευαίσθητων στοιχείων στην περίπτωση του συνόλου δεδομένων BMS-WebView1. Με την αύξηση του μεγέθους των δεδομένων, ο χρόνος εκτέλεσης του αλγορίθμου αυξάνεται εκθετικά. Ως εκ τούτου, ο αλγόριθμος δεν είναι επεκτάσιμος.

Ο TDControl είναι ένας άπληστος αλγόριθμος που βασίζεται σε καθολική γενίκευση, καλύτερος αλγόριθμος για την επίτευξη ρ-αβεβαιότητας από το Suppress Control. Γενικεύει γενικά τα μη ευαίσθητα στοιχεία και καταστέλλει εκείνα τα ευαίσθητα στοιχεία που παραβιάζουν την συνθήκη της ρ-αβεβαιότητας. Επομένως, η απώλεια πληροφοριών είναι μικρότερη από τον αλγόριθμο Suppress Control. Καταστέλλει μόνο το 80% των ευαίσθητων στοιχείων και γενικεύει τα μη ευαίσθητα στοιχεία στην περίπτωση του συνόλου δεδομένων BMS-WebView1, επομένως η απώλεια πληροφοριών είναι μικρότερη από το Suppress Control. Ο χρόνος εκτέλεσης του αλγορίθμου αυξάνεται γραμμικά με την αλλαγή του μεγέθους των δεδομένων. Ως εκ τούτου, ο αλγόριθμος είναι επεκτάσιμος.

Η ανωνυμοποίηση συναλλαγών βάσει κανόνων (Rule-Based Anonymization of Transactions = RBAT) προτάθηκε από τον Loukides και άλλους και είναι ένα μοντέλο βασισμένο σε κανόνες. Σε αυτό το μοντέλο, οι κάτοχοι δεδομένων μπορούν να διατυπώσουν λεπτομερώς τις απαιτήσεις απορρήτου, επειδή δε γίνεται διάκριση μεταξύ δημόσιων και ευαίσθητων στοιχείων που χρειάζονται προστασία. Το μοντέλο βασίζεται στον κανόνα PS. Σύμφωνα με πειράματα που πραγματοποιήθηκαν από τους συγγραφείς, το RBAT επιτυγχάνει αποτέλεσμα που είναι σημαντικά καλύτερο από τον αλγόριθμο Apriori όσον αφορά τη χρησιμότητα των δεδομένων, διασφαλίζοντας ταυτόχρονα ότι οι ευαίσθητες

πληροφορίες προστατεύονται και δεν αποκαλύπτονται. Ο χρόνος εκτέλεσης του αλγορίθμου δεν επηρεάζεται σημαντικά από την τιμή του k. Επομένως, μπορούμε να πούμε ότι ο αλγόριθμος είναι επεκτάσιμος.

Ο Loukides και άλλοι πρότειναν τον αλγόριθμο Utility-Guided Anonymization of Clinical Profiles (UGACLIP) που παρέχει προστασία από την αποκάλυψη ταυτότητας, ενώ διατηρεί τη χρησιμότητα για την επικύρωση του GWAS (genome wise association studies = γονιδιωματικές μελέτες συσχέτισης). Η GWAS είναι η μελέτη για την εύρεση της σχέσης μεταξύ του κώδικα διάγνωσης και της αλληλουχίας DNA για την εύρεση πολλών διαταραχών. Ο UGACLIP χρησιμοποιεί επαναληπτική μέθοδο για να ικανοποιήσει κάθε περιορισμό απορρήτου. Ως πρώτο βήμα, επιλέγεται ο περιορισμός της ιδιωτικής ζωής που συνδέεται με τους περισσότερους ασθενείς. Δεύτερον, ο ασυνήθιστος κώδικας ICD γενικεύεται επαναληπτικά με γενικευμένο κώδικα ICD για να ικανοποιηθεί ο περιορισμός. Επιπλέον, η καταστολή χρησιμοποιείται για την ικανοποίηση περιορισμών απορρήτου, εάν δε μπορεί να ικανοποιηθεί με γενίκευση. Ο αλγόριθμος πηγαίνει στην επόμενη επανάληψη, εάν ο περιορισμός απορρήτου παραμείνει ανικανοποίητος, διαφορετικά η διαδικασία τερματίζεται. Το κατάλληλο επίπεδο προστασίας απορρήτου επιλέγεται από τον κάτοχο των δεδομένων. Αλλά αυτό το έργο μπορεί να είναι δύσκολο, επειδή απαιτείται η πρόβλεψη της αντίθετης γνώσης. Ο αλγόριθμος δεν εγγυάται ότι η απώλεια πληροφοριών είναι ελάχιστη σε ανώνυμα δεδομένα για να ικανοποιεί την καθορισμένη πολιτική βοηθητικών προγραμμάτων. Η επεκτασιμότητα της προσέγγισης δεν έχει αξιολογηθεί. Η άλλη μέθοδος διερευνήθηκε για τον περιορισμό της σύνδεσης στον κώδικα διάγνωσης και στην αλληλουχία DNA, αλλά εξακολουθεί να μην εγγυάται την ελάχιστη απώλεια πληροφοριών που προκύπτει.

Ανωνυμοποίηση συναλλαγών βάσει περιορισμών (COAT): Ο Loukides και άλλοι εντόπισαν την ανάγκη ανωνυμοποίησης των δεδομένων συναλλαγών σύμφωνα με τις συγκεκριμένες ανάγκες της εφαρμογής και τις απαιτήσεις χρησιμότητας. Οι απαιτήσεις έχουν μοντελοποιηθεί με τη μορφή περιορισμών. Χρησιμοποιεί ανωνυμοποίηση που βασίζεται σε σύνολο. Για να αυξηθεί η χρησιμότητα δεδομένων και να δημιουργηθούν λιγότερα παραμορφωμένα στοιχεία, καθορίστηκαν οι λεπτομερείς περιορισμοί απορρήτου και χρησιμότητας. Παράγει ανώνυμα δεδομένα που αποτρέπουν την αποκάλυψη ταυτότητας με χαμηλή απώλεια πληροφοριών σε σύγκριση με το Apriori. Η χειρότερη πολυπλοκότητα χρόνου εκτέλεσης του αλγορίθμου είναι O (|P| ×M ×(M + |P| ×|p| + N)) όπου |p| είναι το μέγεθος του περιορισμού απορρήτου που προσπαθεί να προστατεύσει το COAT στην τρέχουσα επανάληψη και |P| ο αριθμός των καθορισμένων περιορισμών απορρήτου, το M είναι το μέγεθος του περιορισμού του βοηθητικού προγράμματος, το N είναι το μέγεθος δεδομένων. Ως εκ τούτου, ο χρόνος εκτέλεσης του COAT εξαρτάται γραμμικά με το μέγεθος της βάσης δεδομένων, επομένως, κλιμακώνεται καλά σε σχέση με το μέγεθος του συνόλου δεδομένων. Σε σύγκριση με τον Apriori, ο χρόνος εκτέλεσης είναι 2,5 φορές ταχύτερος με το μέγεθος του συνόλου δεδομένων.

Ανωνυμοποίηση δεδομένων συναλλαγών βάσει ομαδοποίησης περιορισμένης ιδιωτικότητας (PCTA): Οι Gkoulalas-Divanis και άλλοι πρότειναν έναν αλγόριθμο που βασίζεται σε ομαδοποίηση και παράγει ανώνυμα δεδομένα με χαμηλή απώλεια πληροφοριών. Ο αλγόριθμος μπορεί να αποδώσει σημαντικά καλύτερο αποτέλεσμα από τις προηγούμενες μεθόδους (Apriori, COAT) όσον αφορά τη χρησιμότητα των δεδομένων. Αυτή η μέθοδος είναι επεκτάσιμη, δηλαδή μπορεί να ικανοποιηθεί ο πραγματικός περιορισμός της ιδιωτικής ζωής και της χρησιμότητας. Η πολυπλοκότητα χρόνου εκτέλεσης του αλγορίθμου είναι O(|P| × |p| × (N + |I|2)) όπου I είναι ο συνολικός αριθμός των στοιχείων. Ο χρόνος εκτέλεσης του αλγορίθμου εξαρτάται γραμμικά από το μέγεθος δεδομένων. Επομένως, κλιμακώνεται καλά σε σχέση με το μέγεθος δεδομένων.

Local Recoding Anonymization (LRA): Ο Terrovitis και άλλοι πρότειναν έναν αποτελεσματικό αλγόριθμο βασισμένο στον Apriori για την ελαχιστοποίηση της απώλειας πληροφοριών και χρησιμοποιεί τοπικό σχήμα επανακωδικοποίησης. Αρχικά, το αρχικό σύνολο δεδομένων διαμερίζεται και, στη συνέχεια, χρησιμοποιώντας τον αλγόριθμο Apriori, κάθε διαμέρισμα ανωνυμοποιείται ανεξάρτητα. Η κατάτμηση γίνεται με σύστημα ταξινόμησης κωδικών Gray. Έτσι, για να έχουμε k^m-ανώνυμη βάση δεδομένων, κάθε διαμέρισμα θα πρέπει να είναι k^m-ανώνυμο. Σύμφωνα με τα πειράματα που πραγματοποιήθηκαν από τους συγγραφείς, ο χρόνος εκτέλεσης μειώνεται με την αύξηση της τιμής του k. Η επεκτασιμότητα της προσέγγισης είναι καλύτερη με το μέγεθος του συνόλου δεδομένων από αυτό του αλγόριθμου Apriori επειδή τα δεδομένα μπορούν να κατατμηθούν σύμφωνα με τη διαθέσιμη μνήμη.

Ο αλγόριθμος κάθετης κατάτμησης (VPA) χρησιμοποιεί ιεραρχία, καθολική γενίκευση για να αντιμετωπίσει το ζήτημα της LRA. Δημιουργεί ισορροπημένα διαμερίσματα χωρίζοντας τη βάση δεδομένων κατακόρυφα, δηλαδή δημιουργεί υποδιαιρέσεις που περιέχουν στοιχεία με κοινό πρόγονο που υπάρχει σε ένα ορισμένο επίπεδο στην ιεραρχία. Ο Apriori εφαρμόζεται σε κάθε διαμέρισμα για τη γενίκευση της βάσης δεδομένων. Ωστόσο, οι LRA και VPA χρησιμοποιούν γενίκευση βάσει ιεραρχίας για την επιβολή της ανωνυμίας των k^m, η οποία είναι μάλλον ακατάλληλη για την ανωνυμοποίηση κωδικών διάγνωσης, όπου η προστασία από την αποκάλυψη ευαίσθητων πληροφοριών είναι επίσης η νομική απαίτηση μαζί με την προστασία από την αποκάλυψη ταυτότητας. Σύμφωνα με πειράματα που πραγματοποιήθηκαν, ο αλγόριθμος απαιτεί λιγότερο χρόνο εκτέλεσης από αυτόν των LRA και Apriori για όλα τα σύνολα δεδομένων στα οποία διεξήγαγαν τα πειράματα. Η μέθοδος είναι επεκτάσιμη με το μέγεθος του συνόλου δεδομένων και η απώλεια πληροφοριών είναι παρόμοια με την Apriori.

Gray-TSP: Ο Xue και άλλοι πρότειναν μια προσέγγιση στην οποία δεν απαιτείται ιεραρχία γενίκευσης αντί αυτού χρησιμοποιεί γενικευμένους bitmaps. Για να γενικεύσει τα QID, αντιστοιχίζει κάθε εγγραφή με καθορισμένη τιμή σε ένα bitmap με έναν μη αμοιβαίο τρόπο επανακωδικοποίησης. Η απώλεια πληροφοριών μειώνεται με επιτυχία. Αλλά έχει μεγάλο χρόνο εκτέλεσης και υψηλή πολυπλοκότητα, επειδή χρησιμοποιεί γενετική προσέγγιση για να προσδιορίσει το σύνολο των συναλλαγών για ανωνυμοποίηση. Το βοηθητικό πρόγραμμα δεδομένων διατηρείται καλύτερα από αυτό του CAHD. Σύμφωνα με τα πειράματα που διεξήχθησαν, δείχνει παρόμοια επεκτάσιμη τάση ανάπτυξης όπως του CAHD σε σχέση με το μέγεθος δεδομένων.

Ανωνυμοποιητής που βασίζεται σε ομαδοποίηση (CBA): Ο CBA (Clustering-Based Anonymizer) χρησιμοποιεί προσέγγιση που βασίζεται σε ομαδοποίηση και γενικεύει κάθε κώδικα ICD ή γενικευμένο στοιχείο. Αυτή η προσέγγιση είναι καλύτερη από τον UGACLIP όσον αφορά τη διατήρηση της χρησιμότητας δεδομένων, επειδή όταν η μέθοδος γενίκευσης δεν είναι αρκετή για να ικανοποιήσει τον περιορισμό της χρησιμότητας, ο CBA χρησιμοποιεί μέθοδο καταστολής μόνο για εκείνους τους κωδικούς ICD που απαιτείται για τη διασφάλιση του απορρήτου, ενώ ο UGACLIP καταστέλλει όλους τους κωδικούς ICD στο τον περιορισμό του βοηθητικού προγράμματος, ο οποίος μπορεί να αφαιρέσει τους κωδικούς ICD χωρίς λόγο. Ο CBA παίρνει χρόνο $O(|P| \times |p| \times (N + |I|2))$, εδώ το N είναι το μέγεθος δεδομένων, $|p|$ είναι ο συνολικός αριθμός των κωδικών ICD και $|P|$ αριθμός κωδικών που χρειάζονται προστασία. Ο χρόνος εκτέλεσης εξαρτάται γραμμικά από το μέγεθος δεδομένων. Ως εκ τούτου, μπορούμε να πούμε ότι ο αλγόριθμος είναι επεκτάσιμος σε σχέση με το μέγεθος δεδομένων.

Αποσύνδεση (Disassociation): Ο Loukides και άλλοι πρότειναν μια προσέγγιση βασισμένη στην αποσύνδεση για την ανωνυμοποίηση των κωδικών διάγνωσης. Η προσέγγιση διασφαλίζει το απόρρητο, διατηρώντας παράλληλα σημαντικά χαμηλότερες απώλειες στο βοηθητικό πρόγραμμα δεδομένων. Η

προδιαγραφή των κωδικών διάγνωσης που μπορεί να οδηγήσει σε αποκάλυψη ταυτότητας, δεν απαιτείται από τους κατόχους δεδομένων. Όπως οι μέθοδοι αναφέρθηκαν από τους συγγραφείς, οι κάτοχοι δεδομένων πρέπει να καθορίσουν κωδικούς διάγνωσης που οδηγούν σε χαμηλότερη χρησιμότητα δεδομένων με υψηλή απώλεια πληροφοριών σε περίπτωση ιατρικών δεδομένων. Ο αλγόριθμος εκτελεί οριζόντια κατάτμηση, κάθετη κατάτμηση και διύλιση. Ο οριζόντιος διαχωρισμός σχηματίζει συστάδες παρόμοιων εγγραφών σε σχέση με τους κωδικούς διάγνωσης και στη χειρότερη περίπτωση, η πολυπλοκότητα χρόνου εκτέλεσης είναι O(|D|2) όπου |D| αντιπροσωπεύει το μέγεθος δεδομένων. Η κατακόρυφη κατάτμηση δημιουργεί κομμάτια αποσυνδέοντας τους συνδυασμούς των κωδικών διάγνωσης και παίρνει χρόνο O(|T|p!) όπου p είναι το σύμπλεγμα και |T|p είναι ο τομέας του συμπλέγματος p. Το μέγεθος του συμπλέγματος μπορεί να ρυθμιστεί, επομένως η τιμή |T|p είναι μικρή στην πράξη. Η τελευταία λειτουργία διύλισης μειώνει περαιτέρω την απώλεια πληροφοριών και βελτιώνει τη χρησιμότητα δεδομένων και απαιτεί χρόνο O(|D|2). Καθώς το μέγεθος των δεδομένων αυξάνεται, ο χρόνος εκτέλεσης αυξάνεται εκθετικά, επομένως, συνάγεται ότι η προσέγγιση δεν είναι επεκτάσιμη σε σχέση με το μέγεθος δεδομένων. Ωστόσο, η απώλεια πληροφοριών είναι χαμηλή καθώς, κατά την ανωνυμοποίηση, τα δεδομένα δεν αλλάζουν. Μόνο η σύνδεση μεταξύ των δεδομένων σπάει.

Μερική καταστολή (Partial Suppression) είναι μια μέθοδος μερικής καταστολής για την επιβολή ρ-αβεβαιότητας, η οποία είναι καλύτερη από τη μέθοδο καθολικής καταστολής που διαγράφει περιττά στοιχεία. Προκειμένου να ελαχιστοποιηθεί ο αριθμός των διαγραφών στοιχείων για να επιτευχθεί το ίδιο επίπεδο απορρήτου, απέστειλαν τα στοιχεία που παραβιάζουν την συνθήκη της ρ-αβεβαιότητας χρησιμοποιώντας την προσέγγιση διαίρει και βασίλευε. Η προσέγγισή τους διατηρεί τη διανομή δεδομένων καλύτερα από αυτή του TDControl διατηρώντας παράλληλα χρήσιμους συσχετισμούς στα δεδομένα. Σύμφωνα με τα πειράματα που διεξήχθησαν, οι αλγόριθμοι δείχνουν υπεργραμμική επιτάχυνση με το μέγεθος δεδομένων εισόδου. Ως εκ τούτου, ο αλγόριθμος δεν είναι επεκτάσιμος.

Gray Sort Clustering (GSC): Ο Wang και άλλοι πρότειναν έναν αλγόριθμο για την παροχή ανωνυμίας σε σύνολα δεδομένων συναλλαγών που περιέχουν ευαίσθητα στοιχεία. Για συναλλαγές με μη ευαίσθητα στοιχεία δεν απαιτείται ανωνυμοποίηση. Ο αλγόριθμος που προτείνεται εδώ έχει υψηλότερο επίπεδο απορρήτου από αυτό των αλγορίθμων που προτείνονται από τους Ghinita, Wang και άλλους. Για να επιτευχθεί το επίπεδο απορρήτου, η λειτουργία προσθήκης/διαγραφής χρησιμοποιείται στο QID και μόνο η λειτουργία προσθήκης σε ευαίσθητα στοιχεία. Η χρονική πολυπλοκότητα του αλγορίθμου είναι O(|D| |QID|) + O(|D| log|D|) + |ST| [2ak*O(|QID|)] + O(|D|*|I|) όπου |ST| είναι ο αριθμός των ευαίσθητων συναλλαγών, a είναι παράμετρος που ορίζεται από το χρήστη, k είναι παράμετρος ανωνυμίας και |I| είναι ο συνολικός αριθμός στοιχείων. Ο χρόνος εκτέλεσης του αλγορίθμου αυξάνεται γραμμικά με την αύξηση της τιμής του k. Προκύπτει εύλογη απώλεια πληροφοριών από τον αλγόριθμο.

PTA: ένα σύστημα που αποτελείται από τρεις ενότητες P (μονάδα προεπεξεργασίας) T (μονάδα TSP) A (μονάδα ανωνυμοποίησης), εφαρμόζεται η μία μετά την άλλη. Αρχικά, ταξινομεί όλες τις συναλλαγές χρησιμοποιώντας τον κωδικό Grey για να ομαδοποιήσει τις παρόμοιες συναλλαγές. Η δεύτερη ενότητα εφαρμόζει ένα πρόβλημα ταξιδιωτικού πωλητή (Traveling Salesman problem = TSP) σε κάθε ομάδα για να βρει έναν κυκλικό βρόχο μεταξύ των συναλλαγών (μια τοπική κατά προσέγγιση λύση). Τρίτον, η ενότητα ανωνυμοποίησης χρησιμοποιεί προσέγγιση χαρτογράφησης και πλειοψηφίας για να βρει ένα κεντρικό σημείο κάθε ομάδας. Στη συνέχεια, η απώλεια πληροφοριών υπολογίζεται αντικαθιστώντας όλες τις συναλλαγές ανά κεντρικό σημείο σε κάθε ομάδα. Η ομάδα με την ελάχιστη απώλεια πληροφοριών θεωρείται τότε ως κλάση ισοδυναμίας. Όλες οι συναλλαγές που ανήκουν στην κατηγορία ισοδυναμίας αντικαθίστανται από το κεντρικό σημείο της. Η διαδικασία επαναλαμβάνεται για να

δημιουργηθούν περισσότερες κλάσεις ισοδυναμίας. Οι εκκρεμείς συναλλαγές που δεν έχουν κατανεμηθεί σε καμία κατηγορία ισοδυναμίας κατανέμονται στη συνέχεια στην πιο συγκρίσιμη κατηγορία ισοδυναμίας όσον αφορά την απόσταση Hamming. Στο σύστημα PTA α) τα δεδομένα συναλλαγής με χαμηλή απώλεια πληροφοριών είναι ανώνυμα, β) η υπολογιστική πολυπλοκότητα της διαδικασίας ανωνυμοποίησης μειώνεται, γ) ο χρόνος εκτέλεσης του αλγορίθμου είναι O(|D|3) όπου D είναι το μέγεθος δεδομένων και η απώλεια πληροφοριών του συστήματος PTA είναι πολύ μικρότερο από αυτό της τελευταίας τεχνολογίας (grey-TSP , GSC).

Ανωνυμοποίηση βάσει δέντρων: Ο Loukides και άλλοι πρότειναν μια προσέγγιση γενίκευσης από πάνω προς τα κάτω χρησιμοποιώντας προστασία από κανόνες PS. Πρώτα, αντιστοιχίζει όλα τα δημόσια στοιχεία του συνόλου δεδομένων σε ένα πιο γενικευμένο στοιχείο και, στη συνέχεια, το στοιχείο χωρίζεται όσο το δυνατόν περισσότερο για να βελτιωθεί η χρησιμότητα. Η χειρότερη χρονική πολυπλοκότητα του αλγορίθμου είναι O(2|P| ×|S| × N) όπου |P| είναι το μέγεθος προηγούμενων και |S| είναι το μέγεθος της συνέπειας στους κανόνες P-> S και N είναι το μέγεθος δεδομένων. Ο χρόνος εκτέλεσης αυξάνεται γραμμικά με την αύξηση του μεγέθους των δεδομένων. Ως εκ τούτου, ο αλγόριθμος είναι επεκτάσιμος και, στα πειράματα, η ανωνυμοποίηση βάσει δέντρων είναι έως και 10,3 φορές αποτελεσματική από τον Apriori.

Ανωνυμοποίηση βάσει δείγματος: Ο Loukides και άλλοι πρότειναν έναν αλγόριθμο που είναι πιο επεκτάσιμος από την ανωνυμοποίηση που βασίζεται σε δέντρα, επειδή ο έλεγχος κανόνων είναι πολύ πιο γρήγορος από αυτόν της ανωνυμοποίησης βάσει δέντρων. Χρησιμοποιεί τον συνδυασμό στρατηγικής από πάνω προς τα κάτω και από κάτω προς τα πάνω. Το γενικευμένο σύνολο δεδομένων κατασκευάστηκε γρήγορα χρησιμοποιώντας τεχνική δειγματοληψίας που ικανοποιεί τους περισσότερους κανόνες PS. Για τους υπόλοιπους κανόνες, πρέπει να τροποποιήσουμε ελαφρώς ορισμένα από τα στοιχεία. Πρώτον, ο αλγόριθμος αντιστοιχίζει όλα τα στοιχεία με ένα πιο γενικευμένο στοιχείο και στη συνέχεια προχωρά σε τρία βήματα: (i) φάση κατάτμησης βάσει δείγματος, στην οποία δημιουργείται ένα δέντρο γενίκευσης σταδιακά παρόμοιο με την ανωνυμοποίηση βάσει δέντρων, (ii) από πάνω προς τα κάτω φάση αναθεώρησης περικοπής, για τη βελτίωση της χρησιμότητας, τα γενικευμένα δεδομένα διαχωρίζονται περαιτέρω και (iii) η φάση αναθεώρησης περικοπής από κάτω προς τα πάνω, για να διασφαλιστεί το απόρρητο, τα γενικευμένα στοιχεία συγχωνεύονται επαναληπτικά. Η πολυπλοκότητα χρόνου εκτέλεσης του αλγορίθμου είναι ίδια με αυτή της ανωνυμοποίησης βάσει δέντρων O(2|P| × | S| × N) αλλά στα πειράματα το Sample-based αποδείχθηκε ότι ήταν πιο κλιμακωτό στην πράξη.

Η εικόνα 10 δίνει τη σύγκριση των αλγορίθμων που προσφέρουν προστασία από επίθεση αποκάλυψης ταυτότητας, η εικόνα 11 δίνει τη σύγκριση των αλγορίθμων που προσφέρουν προστασία από την επίθεση αποκάλυψης ευαίσθητων πληροφοριών και η εικόνα 12 δίνει τη σύγκριση αλγορίθμων που προσφέρουν προστασία από αποκάλυψη ταυτότητας καθώς και αποκάλυψη ευαίσθητων πληροφοριών επίθεση.

Privacy models	Algorithm	Year	Scalability	Information loss	Anonymization method	Approach
Complete k-anonymity	Gray-TSP	2012	Scalable (Similar to CAHD)	Lower than CAHD [30]	Generalization	Genetic
	GSC	2014	Scalable	Moderate	Addition/deletion	Heuristic/Clustering
	PTA	2016	Not Scalable	Lower than GSC	Generalization	Divide & Conquer
K^m-anonymity	Apriori	2008	Scales well with number of items and transactions	High information loss	Generalization	Bottom-up
	COAT	2011	Better than Apriori with the size of dataset	Lower than Apriori	Generalization & suppression	Heuristic
	PCTA	2011	Scales well w.r.t. dataset size	Lower than Apriori and COAT	Generalization	Clustering based approach
	Local Recoding Anonymization (LRA)	2011	Scales better than Apriori with the size of dataset and value of k	Lower than Apriori	Generalization	Bottom-up hierarchy based
	Virtual Partitioning Algorithm (VPA)	2011	Scales better than LRA with the size of dataset and value of k	Similar to Apriori	Generalization	Bottom-up hierarchy based
	Disassociation	2014	Not Scalable	Very low	Bucketization	Clustering
Privacy constrained anonymity	UGACLIP	2010	Not discussed	High information loss	Generalization & suppression	Iterative
	CBA	2013	Scalable w.r.t dataset size	Lower than UGAClip	Generalization & suppression	Clustering

Εικόνα 10:Σύγκριση αλγορίθμων που προσφέρουν προστασία από επίθεση αποκάλυψης ταυτότητας[2].

Privacy models	Algorithm	Year	Scalability	Information loss	Anonymization method	Approach
ρ-uncertainty	Suppress control	2010	Not scalable	High	Suppression	Greedy
	TD control	2010	Scalable	Lower than suppressControl	Suppression & generalization	Greedy
	Partial suppression	2014	Not Scalable	Low	Suppression	Divide & conquer

Εικόνα 11:Σύγκριση αλγορίθμων που προσφέρουν προστασία από επίθεση αποκάλυψης ευαίσθητων πληροφοριών[2].

Privacy models	Algorithm	Year	Scalability	Information loss	Anonymization method	Approach
(h,k,p)-coherence	Greedy	2008	Not discussed	Significant information loss	Suppression	Greedy
PS-rule based anonymity	RBAT	2010	Scalable (w.r.t. k)	Data utility better than Apriori	Generalization	Top-down
	Tree-based anonymization	2013	Scalable (better than Apriori)	Lower than greedy	Generalization	Top-down
	Sample-based anonymization	2013	Scalable (better than tree-based anonymization)	Lower than tree based anonymization	Generalization	Combination of top-down and bottom-up strategy

Εικόνα 12:Σύγκριση αλγορίθμων που προσφέρουν προστασία τόσο από την αποκάλυψη ταυτότητας όσο και από την επίθεση αποκάλυψης ευαίσθητων πληροφοριών[2].

2.6 Μελέτη περίπτωσης δεδομένων RT: Ανωνυμοποίηση δεδομένων ασθενών

Τα δεδομένα ασθενών περιέχουν πληροφορίες ασθενών με κωδικούς διάγνωσης όπου τα δημογραφικά στοιχεία του ασθενούς αποθηκεύονται σε δομημένη μορφή και τα στοιχεία διάγνωσης αποθηκεύονται ως δεδομένα συναλλαγής. Σύμφωνα με τις προσεγγίσεις που συζητήθηκαν παραπάνω, αρχικά τα δημογραφικά δεδομένα και τα διαγνωστικά δεδομένα μπορούν να διαχωριστούν και στη συνέχεια μπορεί να εφαρμοστεί ο κατάλληλος αλγόριθμος ανωνυμοποίησης για την ανωνυμοποίηση του καθενός. Αλλά αυτή η διαδικασία είναι χρονοβόρα. Ας εξετάσουμε το σύνολο δεδομένων RT που φαίνεται στην εικόνα 13a, στην οποία κάθε εγγραφή αντιστοιχεί σε έναν ασθενή. Η ηλικία, το φύλο και η φυλή είναι σχεσιακά χαρακτηριστικά, ενώ ο κώδικας διάγνωσης είναι ένα χαρακτηριστικό συναλλαγής που περιέχει σύνολο στοιχείων. Η εφαρμογή τέτοιου τύπου δεδομένων απαιτείται όπου πρέπει να

βρούμε όλους τους ασθενείς ηλικίας κάτω των 30 ετών που διαγνώστηκαν με τη νόσο 487 και 309. Η άλλη εφαρμογή μπορεί να είναι σε σούπερ μάρκετ, όπου πολλές μελέτες μάρκετινγκ απαιτούν να βρούμε τα δημογραφικά στοιχεία των πελατών και τα προϊόντα που αγοράστηκαν μαζί. Ένα σύνολο δεδομένων RT D αποτελείται από εγγραφές που περιέχουν σχεσιακά χαρακτηριστικά R1, . . . , Rv, που περιέχουν μεμονωμένες τιμές και ένα χαρακτηριστικό συναλλαγής T, που περιέχει τιμές συνόλου. Έχει γίνει κάποια βελτίωση προς αυτή την κατεύθυνση για την αποτελεσματική ανωνυμοποίηση του συνδυασμού τέτοιων δεδομένων. Πολλές μέθοδοι έχουν αναπτυχθεί για τη διατήρηση του απορρήτου δεδομένων των συνόλων δεδομένων που περιέχουν είτε σχεσιακές ιδιότητες είτε ιδιότητες συναλλαγής μόνο όπως συζητήθηκε σε προηγούμενες ενότητες. Εάν κάθε τύπος χαρακτηριστικού ανωνυμοποιηθεί ξεχωριστά χρησιμοποιώντας τις υπάρχουσες μεθόδους, δεν θα αποφέρει το απαιτούμενο αποτέλεσμα επειδή οι πληροφορίες που αφορούν τόσο τον τύπο των χαρακτηριστικών σχεσιακό όσο και με τη συναλλαγή ενδέχεται να προκαλέσουν αποκάλυψη ταυτότητας. Παρατηρώντας την εικόνα 13a, το μικρό στιγμιότυπο του συνόλου δεδομένων INFORMS που έχει το φύλο, τη φυλή, τον μήνα γέννησης και το έτος γέννησης ως σχεσιακά χαρακτηριστικά και τον κωδικό διάγνωσης ως χαρακτηριστικό συναλλαγής, έχουμε υπολογίσει την ηλικία από το χαρακτηριστικό μήνα και γέννηση. Και οι δύο τύποι δεδομένων ανωνυμοποιούνται χωριστά, όπως φαίνεται στην εικόνα 13b. Ένας εισβολέας, ο οποίος γνωρίζει ότι ο Μπομπ είναι ένας 25χρονος άνδρας που δεν συνάντησε κανένα ατύχημα τα προηγούμενα χρόνια, το οποίο ορίζεται από τον κωδικό 924, μπορεί να συσχετίσει τον Μπομπ με το ID 2 στην εικόνα 13b. Η προστασία από την αποκάλυψη ταυτότητας είναι σημαντική για την εκπλήρωση της νομικής απαίτησης, π.χ. Κανόνας απορρήτου HIPAA, και για να βοηθήσει τη μελλοντική συλλογή δεδομένων.

2.7 Μοντέλα απορρήτου

Η (k, k^m)-ανωνυμία είναι η προστασία από την αποκάλυψη ταυτότητας στο RTdataset. Όταν ένας εισβολέας έχει τη γνώση οποιουδήποτε συνδυασμού δημογραφικών στοιχείων του ασθενούς και οποιουδήποτε συνδυασμού m κωδικών διάγνωσης. Ένας εισβολέας δεν μπορεί να διακρίνει μια εγγραφή από τουλάχιστον k-1 άλλες εγγραφές χρησιμοποιώντας τις παραπάνω γνώσεις, τότε το σύνολο δεδομένων RT είναι (k, k^m) ανώνυμο. Η ανωνυμία (k, k^m) προσφέρει το ίδιο επίπεδο προστασίας με την k-ανωνυμία και την k^m-ανωνυμία για δημογραφικά χαρακτηριστικά και χαρακτηριστικά συναλλαγής αντίστοιχα. Ωστόσο, το αντίστροφο δεν ισχύει. Συγκεκριμένα, ένα σύνολο δεδομένων RT μπορεί να είναι k και k^m ανώνυμο αλλά όχι (k, k^m)-ανώνυμο όπως φαίνεται στην εικόνα 13b.

Id	Name	Relational attributes			Transaction attributes
		Age	Sex	Race	Diagnoses
1	Mary	29	M	White	716 924 562 300 **346 436 429 553**
2	Bob	25	M	Black	487 309 **436 429**
3	Tom	38	M	Asian	300 **346 553**
4	Anne	46	M	American	487 309 **346 436**
5	Brad	61	F	Black	716 924 300 487 **429**
6	Jim	65	F	White	562 309 **553**

a)

Id	Relational attributes			Transaction attributes
	Age	Sex	Zip	Diagnoses
1	[20-30]	M	All	(716,924,562) (300,487,309) **346 436 429 553**
2	[20-30]	M	All	(300,487,309) **436 429**
3	[31-51]	M	All	(300,487,309) **346 553**
4	[31-51]	M	All	(300,487,309) **346 436**
5	[60-70]	F	All	(716,924,562) (300,487,309) **429**
6	[60-70]	F	All	(716,924,562) (300,487,309) **553**

b)

Id	Relational attributes			Transaction attributes
	Age	Sex	Zip	Diagnoses
1	[20-50]	All	All	(716,924,562) (300,487,309) **346 436 429 553**
2	[20-50]	All	All	(300,487,309) **436 429**
3	[20-50]	All	All	(300,487,309) **346 553**
4	[20-50]	All	All	(300,487,309) **346 436**
5	[60-70]	F	All	(716,924,562) (300,487,309) **429**
6	[60-70]	F	All	(716,924,562) (300,487,309) **553**

c)

Εικόνα 13:(a) Ένα σύνολο δεδομένων RT με δημογραφικά στοιχεία ασθενών και κωδικούς διάγνωσης, (b) ένα 2^2-ανώνυμο w.r.t. οι συναλλαγές αποδίδουν χρησιμοποιώντας ιεραρχία γενίκευσης που υπάρχει στην εικόνα 6 και (c) η $(2,2^2)$-ανώνυμη έκδοση της εικόνας 13a [2].

2.8 Προηγμένοι αλγόριθμοι ανωνυμοποίησης

Differentially Private Data Algorithm: Ο Jiang και άλλοι πρότειναν μια μέθοδο που επιβάλλει το διαφορικό απόρρητο, μια ισχυρή αρχή απορρήτου, έχει την ιδιότητα, η παρουσία ή η απουσία των πληροφοριών ενός ατόμου στο σύνολο δεδομένων να μην επηρεάζει το αποτέλεσμα της ανάλυσης που εφαρμόζεται στο σύνολο δεδομένων. Με άλλα λόγια, οποιαδήποτε ερμηνεία που γίνεται από έναν εισβολέα για ένα άτομο θα είναι (περίπου) ανεξάρτητη από το εάν η εγγραφή του ατόμου υπάρχει στο σύνολο δεδομένων ή όχι. Η μέθοδος κατασκευάζει ένα γενικευμένο πίνακα έκτακτης ανάγκης για την επιβολή διαφορικού απορρήτου. Διατηρεί την καταμέτρηση όλων των συνδυασμών τιμών δεδομένων και, στη συνέχεια, προστίθεται θόρυβος στις μετρήσεις για να ικανοποιήσει το διαφορικό απόρρητο. Για τη δημιουργία ενός ταξινομητή, η μέθοδος διατηρεί όσο το δυνατόν περισσότερες πληροφορίες. Τα πειράματα που διεξήχθησαν κατέληξαν στο συμπέρασμα ότι ο αλγόριθμος είναι επεκτάσιμος για να χειρίζεται μεγάλα σύνολα δεδομένων.

RM_{RT}: Ο Poulis και άλλοι πρότειναν ένα πλαίσιο για την επιβολή της ανωνυμίας (k, k^m) σε σχεσιακά και καθορισμένα χαρακτηριστικά. Ο αλγόριθμος γενικεύει τα δημογραφικά χαρακτηριστικά με τέτοιο τρόπο ώστε η απώλεια πληροφοριών να παραμένει χαμηλότερη από ένα δεδομένο όριο και γενικεύει τον κώδικα διαγνώσεων χρησιμοποιώντας γενίκευση συνόλου τιμών. Ο χρόνου εκτέλεσης της ανωνυμοποίησης είναι O(F + |C|2 · (KR + KT)), όπου F είναι το κόστος για τον αρχικό σχηματισμό συμπλέγματος, |C| ο αριθμός των συστάδων στο D, και τα KR και KT τα κόστη γενίκευσης του σχεσιακού και συναλλακτικού τμήματος ενός συμπλέγματος.

Ο Takahashi και άλλοι επιβάλλουν την k-ανωνυμία χρησιμοποιώντας γενίκευση που βασίζεται στην ιεραρχία. Σε μια δεδομένη ιεραρχία, κάθε ομάδα αξιών αντικαθίσταται με τον πλησιέστερο κοινό πρόγονό τους. Επιπλέον, ορισμένες τιμές γενικεύονται με έναν προκαθορισμένο τρόπο που επιλέγεται από τους κατόχους δεδομένων. Ως αποτέλεσμα, ο χώρος της πιθανής λύσης είναι μικρότερος από αυτόν του ART_{UC} και προκαλεί μεγάλη απώλεια πληροφοριών. Αυτό συμβαίνει επειδή οι τιμές των χαρακτηριστικών είναι προγενικευμένες, ακόμη και η γενίκευση μπορεί να γίνει χρησιμοποιώντας πιο συγκεκριμένες τιμές που προκαλούν μικρότερη απώλεια πληροφοριών και για τη γενίκευση του κώδικα διάγνωσης, χρησιμοποιείται το μοντέλο γενίκευσης που βασίζεται στην ιεραρχία που προσφέρει χαμηλότερα δεδομένα χρησιμότητα από αυτή του μοντέλου γενίκευσης που βασίζεται σε σύνολο.

ART_{UC}: Προηγούμενοι αλγόριθμοι για την ανωνυμοποίηση συνόλων δεδομένων RT προκαλούν μεγαλύτερη απώλεια πληροφοριών, επειδή τα δημογραφικά στοιχεία ή/και οι κωδικοί διάγνωσης δέχονται κάθε είδους αλλαγές στους αλγόριθμους που οδηγούν σε ανακριβείς μελέτες για τον αριθμό των περιπτώσεων. Για την επίλυση αυτού του ζητήματος έχει προταθεί περιορισμός του βοηθητικού προγράμματος. Ο Poulis και άλλοι πρότειναν έναν αλγόριθμο που χρησιμοποιεί (k, k^m)- ανωνυμία. Χρησιμοποιώντας την προσέγγιση από κάτω προς τα πάνω, ο αλγόριθμος δημιουργεί πρώτα συμπλέγματα με παρόμοιες τιμές σε δημογραφικά χαρακτηριστικά με βάση τους περιορισμούς χρησιμότητας. Στη συνέχεια, οι τιμές στα δημογραφικά στοιχεία και στον κώδικα διάγνωσης γενικεύονται ξεχωριστά σε κάθε ομάδα. Στο τέλος, τα συμπλέγματα που περιέχουν τις παρόμοιες γενικευμένες τιμές συγχωνεύονται. Προσφέρει καλύτερη χρησιμότητα δεδομένων από αυτή των προηγούμενων αλγορίθμων επειδή τα συμπλέγματα σχηματίζονται χρησιμοποιώντας αλγόριθμους ανωνυμοποίησης από κάτω προς τα πάνω που εξερευνούν μεγαλύτερο χώρο πιθανών λύσεων. Ο αλγόριθμος κλιμακώνει καλά το w.r.t. μέγεθος δεδομένων και τις τιμές k και m. Η εικόνα 14 δίνει την κατηγοριοποίηση των αλγορίθμων για την ανωνυμοποίηση συνόλων δεδομένων RT.

Anonymization algorithm	Year	Privacy model	Anonymization method	Support of utility constraints	Information loss	Scalability	Approach
Differentially private data algorithm	2013	Differential privacy	Generalization	N	High	Scalable (w.r.t. dataset size)	Top-down fashion
RM_{RT}	2013	(k,k^m)-anonymity	Generalization	N	Low	Scalable	Clustering and hierarchy based generalization
ART_{UC}	2017	(k, k^m)-anonymity	Generalization and suppression	Y	Lower than above	Scalable (w.r.t. dataset size and anonymization parameters	Set based generalization

Εικόνα 14:Κατηγοριοποίηση αλγορίθμων για την ανωνυμοποίηση συνόλων δεδομένων RT[2].

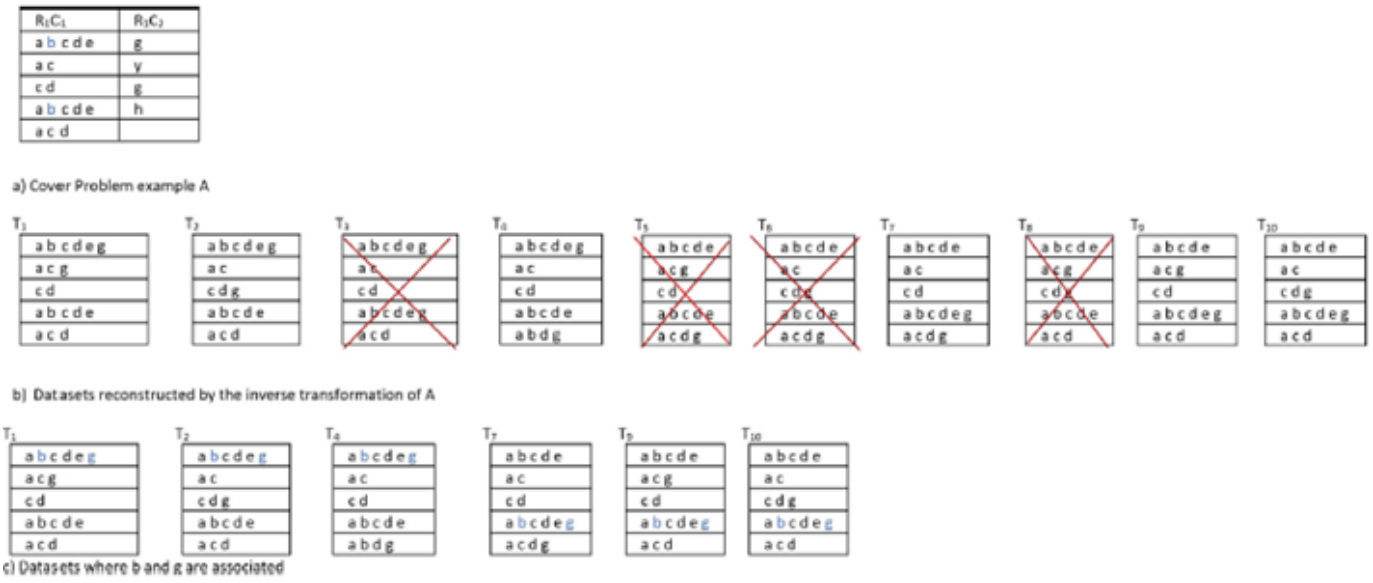
2.9 Μελλοντικές κατευθύνσεις

Οι ακόλουθες κατευθύνσεις μελλοντικής εργασίας που έχουν προσδιοριστεί με βάση την έρευνα είναι:

Βελτίωση στην υπάρχουσα τεχνική.

Η μέθοδος bucketization διατηρεί τη χρησιμότητα διατηρώντας τις τιμές ανέπαφες χωρίς καμία αλλαγή, επομένως, η αποσύνδεση που πραγματοποιείται με bucketization ξεπερνά τις προσεγγίσεις του CBA και του UGACLIP όσον αφορά την απώλεια πληροφοριών με το ίδιο επίπεδο απορρήτου. Η αποσύνδεση διαχωρίζει το σύνολο δεδομένων σε συστάδες τμημάτων εγγραφής σε k^m ανώνυμων και τμημάτων στοιχείων. Ταξινομεί τις εγγραφές με βάση τα πιο συχνά στοιχεία και στη συνέχεια τις ομαδοποιεί οριζόντια σε μικρότερα χωριστά συμπλέγματα. Τα συμπλέγματα χωρίζονται κατακόρυφα σε k^m ανώνυμα κομμάτια εγγραφής και οι σπάνιοι συνδυασμοί διαχωρίζονται. Όμως, χρησιμοποιώντας το πρόβλημα κάλυψης συνόλου, ένας εισβολέας με κάποια γνώση του παρασκηνίου των αντικειμένων μπορεί να ταιριάζει με το σύνολο και να μπορεί να βρει την πλήρη γνώση του συνόλου που ταιριάζει με τη γνώση υποβάθρου που ονομάζεται πρόβλημα κάλυψης.

Τυπικά, το πρόβλημα κάλυψης ορίζεται ως εξής: ''Δίνεται ένα σύνολο στοιχείων σε RiCj−1 (j ≥ 2) που έχουν υποστήριξη μεγαλύτερη ή ίση με την υποστήριξη ενός στοιχείου xi, j ∈RiCj, Ii, j−1 = {y : y ∈ RiCj−1 και s(y, RiCj−1) ≥ s(xi, j, RiCj)}, υπάρχει πρόβλημα κάλυψης αν ∃yi, j−1 ∈ Ii, j−1 τέτοιο ώστε s(yi, j−1, RiCj−1) = s(Ii, j−1, RiCj−1) = min ∀y∈Ii, j−1 s(y, RiCj−1)'' όπου το RiCj αντιπροσωπεύει το κομμάτι εγγραφής που δημιουργήθηκε με την τεχνική αποσύνδεσης. Έτσι, εάν υπάρχει μια σχέση μεταξύ m ήδη γνωστών στοιχείων για ένα άτομο με λιγότερες από k εγγραφές όλων των συνόλων δεδομένων που ανακατασκευάστηκαν από τον αντίστροφο μετασχηματισμό που καθιερώθηκε από έναν εισβολέα, τότε λέγεται ότι συμβαίνει παραβίαση απορρήτου. Για παράδειγμα, στην εικόνα 15a, εάν τα στοιχεία 'g' και 'b' αναζητήθηκαν από ένα άτομο που είναι γνωστό από έναν εισβολέα, ο εισβολέας μπορεί να τον συνδέσει με τα στοιχεία 'a', 'c', 'd' και 'g' σε όλα τα ανακατασκευασμένα σύνολα δεδομένων με τον αντίστροφο μετασχηματισμό του A που φαίνεται στην εικόνα 15c. Τα δεδομένα T3, T5, T6 και T8 που φαίνονται στην εικόνα 15b δεν είναι δυνατά λόγω της τεχνικής αποσύνδεσης. Επομένως, απαιτείται να αναπτυχθεί ένας αλγόριθμος που μπορεί να παρέχει κάποια άλλη μέθοδο μαζί με τη δημιουργία κάδου σε διαχωρισμένα δεδομένα και να αξιολογήσει το κέρδος στη χρησιμότητα που παρέχει το διαχωρισμένο σύνολο δεδομένων.



Εικόνα 15:Παραδείγματα προβλημάτων κάλυψης και παραβίασης απορρήτου[2].

Προστασία από διάφορους τύπους επιθέσεων

Η ισχυρή μορφή επιθέσεων, που ονομάζονται συνεργατικές επιθέσεις, περιλαμβάνει μια επίθεση σε δεδομένα όπου η γνώση δύο ή περισσότερων εισβολέων συνδυάζεται ή/και η γνώση του ιστορικού πολλαπλών εγγραφών στα δεδομένα στοχεύει στην εκ νέου αναγνώριση ενός ατόμου ή μιας οντότητας από τα δημοσιευμένα δεδομένα. Οι αλγόριθμοι ανωνυμίας πρέπει να αξιολογηθούν για αποτελεσματική προστασία από αυτές τις επιθέσεις. Χρησιμοποιώντας ισχυρότερες αρχές απορρήτου, όπως το διαφορικό απόρρητο, μπορούν να αντιμετωπιστούν τέτοιες ισχυρές επιθέσεις. Ωστόσο, η χρησιμότητα δεδομένων μειώνεται χρησιμοποιώντας αυτές τις αρχές.

Σε περίπτωση ανωνυμοποίησης κωδικού διάγνωσης, η πλήρης k-ανωνυμία και η k^m-ανωνυμία παρέχουν προστασία έναντι της αποκάλυψης ταυτότητας και η ρ-αβεβαιότητα παρέχει προστασία έναντι της αποκάλυψης ευαίσθητων πληροφοριών. Η (h, k, p)- συνοχή και ο PS κανόνας παρέχουν προστασία έναντι και των δύο τύπων επιθέσεων, αλλά η (h, k, p)- συνοχή προκαλεί υπερβολική απώλεια και η υπολογιστική πολυπλοκότητα του επόμενου είναι πολύ υψηλή, αν και οι αλγόριθμοι χρησιμοποιούν στρατηγική κλαδέματος για να μειώσουν την πολυπλοκότητα των PS κανόνων. Προτείνεται να αναπτυχθεί αποτελεσματικός αλγόριθμος για να παρέχει προστασία τόσο από την αποκάλυψη ταυτότητας όσο και από την αποκάλυψη ευαίσθητων πληροφοριών.

Κατά τη δημοσίευση δεδομένων συναλλαγών, η προστασία από την ταυτότητα και η αποκάλυψη ευαίσθητων πληροφοριών είναι οι κύριες ανησυχίες, ενώ μπορεί επίσης να εξεταστεί η ανάγκη αποτροπής της επίθεσης αποκάλυψης μελών.

Οι μέθοδοι που συζητήθηκαν παραπάνω για την ανωνυμοποίηση των συνόλων δεδομένων RT εξετάζουν ένα μη ταξινομημένο σύνολο κωδικών διάγνωσης. Υπάρχουν ορισμένες εφαρμογές, όπως οι διαχρονικές μελέτες, που απαιτούν την ταξινόμηση των κωδικών διάγνωσης να παραμένει ανέπαφη. Σε

αυτή την περίπτωση, πρέπει να διατηρήσουμε τη διαδοχικότητα των δεδομένων σε ανώνυμα δεδομένα. Έχει γίνει κάποια εργασία για διαδοχικά δεδομένα αλλά αυτές οι μέθοδοι είναι για μεμονωμένα ευαίσθητα στοιχεία (σχεσιακά δεδομένα) και όχι για πολλαπλά ευαίσθητα στοιχεία (δεδομένα συναλλαγών).

3. Ψευδωνυμοποίηση ιατρικών δεδομένων

3.1 Εισαγωγή

Η επιβολή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) στις 25 Μαΐου 2018 ενισχύει το απόρρητο στην Ευρώπη. Οι νομικές αρχές του Privacy by Design και Privacy by Default υποστηρίζουν ότι το απόρρητο πρέπει να λαμβάνεται υπόψη κατά τον σχεδιασμό όλων των τεχνικών συστημάτων και οι προεπιλεγμένες ρυθμίσεις (π.χ. πολιτική απορρήτου σε ένα ηλεκτρονικό σύστημα) πρέπει να είναι φιλικές προς το απόρρητο από προεπιλογή. Ειδικές κατηγορίες προσωπικών δεδομένων, π.χ. δεδομένα που αφορούν την υγεία ή τα γενετικά δεδομένα, προστατεύονται ιδιαίτερα και δεν πρέπει να υποβάλλονται σε επεξεργασία εκτός εάν πληρούνται ειδικοί όροι όπως νομική βάση ή ρητή συγκατάθεση. Η Layered Privacy Language (LPL), συμπεριλαμβανομένου του γενικού πλαισίου της, σκοπεύει να μοντελοποιήσει και να επιβάλλει πολιτικές απορρήτου «από τη συναίνεση έως την επεξεργασία» [11]. Με το παρόν, η LPL μοντελοποιεί πολιτικές απορρήτου, οι οποίες παρουσιάζονται και ενδεχομένως εξατομικεύονται από το μεμονωμένο ζήτημα δεδομένων. Εάν δοθεί συμφωνία ή/και συναίνεση σχετικά με την πολιτική απορρήτου, θα υποβληθεί σε προεπεξεργασία και αποθήκευση. Τις περισσότερες φορές στη βιβλιογραφία, η ανωνυμοποίηση χρησιμοποιείται συνώνυμα με την αποταυτοποίηση, η οποία είναι μια έννοια που χρησιμοποιείται από τον κανόνα απορρήτου των ΗΠΑ για τη φορητότητα και τη λογοδοσία της ασφάλισης υγείας (HIPPA) για ιατρικά δεδομένα[15]. Κατόπιν αιτήματος προσωπικών δεδομένων για συγκεκριμένο σκοπό, διεξάγεται η διαδικασία αποταυτοποίησης βάσει πολιτικής. Αυτό καθορίζει εάν η αιτούσα οντότητα είναι εξουσιοδοτημένη να ζητήσει τα δεδομένα και, εάν είναι απαραίτητο, ανωνυμοποιεί τα δεδομένα. Έτσι, τεχνικές ανωνυμοποίησης όπως η γενίκευση, η καταστολή και η διαγραφή χρησιμοποιούνται για την επιβολή μοντέλων απορρήτου όπως η k-ανωνυμία, η l-ποικιλομορφία ή το διαφορικό απόρρητο, όπως είδαμε και σε προηγούμενο κεφάλαιο. Παρακάτω θα αναφερθεί η ανάλυση δεδομένων με την ψευδωνυμοποίηση αυτών. Στον GDPR, η ψευδωνυμοποίηση ορίζεται ως η επεξεργασία προσωπικών δεδομένων κατά τρόπο που δεν μπορεί πλέον να αποδοθεί σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών. Ως εκ τούτου, μπορεί κανείς να υποστηρίξει ότι οποιαδήποτε επεξεργασία που επιτρέπει τη χρήση πρόσθετων, άμεσων ή έμμεσων αναγνωριστικών/χαρακτηριστικών, για την εκ νέου αναγνώριση του υποκειμένου των δεδομένων εμπίπτει στην κατηγορία της ψευδωνυμοποίησης. Αυτό σημαίνει ότι η αποταυτοποίηση είναι πιο κοντά στην έννοια της ψευδωνυμοποίησης παρά στην ανωνυμοποίηση[15].

3.2 Ανάλυση ιατρικών δεδομένων

Στην υγειονομική περίθαλψη, τα προσωπικά δεδομένα των ασθενών αποθηκεύονται και υφίστανται επεξεργασία για διαφορετικούς σκοπούς, όπως χρέωση, ανάλυση ή έρευνα. Ειδικά, πληροφορίες για την κατάσταση των ασθενών, π.χ. σάκχαρο αίματος, συμπτώματα, ασθένειες και θεραπείες, που εμπίπτουν στις ειδικές κατηγορίες προσωπικών δεδομένων, αποθηκεύονται μαζί με κανονικά προσωπικά δεδομένα όπως όνομα, ηλικία ή διεύθυνση ασθενών. Στη συνέχεια, υποθέτουμε ένα σενάριο στο οποίο ένα σύνολο δεδομένων αναλύεται για τον εντοπισμό μιας πιθανής επιδημίας. Εδώ, η γρίπη, κοινώς γνωστή ως «γρίπη», χωρίζεται σε διαφορετικούς τύπους. Ο τύπος Α είναι γενικά υπεύθυνος για μεγάλες επιδημίες γρίπης, ο τύπος Β είναι λιγότερο επιβλαβής και ο τύπος C δεν προκαλεί επιδημίες. Υπάρχουν επιπλέον υποτύποι, οι οποίοι είναι άσχετοι με αυτό το παράδειγμα.

Υποθέτουμε ένα σύνολο δεδομένων υγειονομικής περίθαλψης όπως φαίνεται στην εικόνα 16, που αποτελείται από χαρακτηριστικά διαφορετικών κατηγοριών απορρήτου. Γενικά, τα δεδομένα

ταξινομούνται σε τέσσερις κατηγορίες. Ρητά αναγνωριστικά (Explicit Identifiers=EI), χαρακτηριστικά που προσδιορίζουν ένα άτομο μοναδικά, οιονεί αναγνωριστικά (Quasi Identifiers=QI) που σε συνδυασμό προσδιορίζουν ένα άτομο, ευαίσθητα δεδομένα (Sensitive Data=SD), που αποτελούνται από ευαίσθητες αλλά μη αναγνωρίσιμες πληροφορίες σχετικά με τον κάτοχο της εγγραφής και μη ευαίσθητα δεδομένα (NSD), δεδομένα που δεν ανήκουν σε καμία από τις παραπάνω κατηγορίες. Με βάση αυτήν την ταξινόμηση, η οποία υπάρχει επίσης στη LPL, τα μοντέλα απορρήτου ανωνυμοποιούν ένα σύνολο δεδομένων. Υποθέτουμε ότι σε αυτήν την περίπτωση θέλουμε να προστατεύσουμε την ταυτότητα και τις ευαίσθητες πληροφορίες, οι οποίες θα μπορούσαν επίσης να χρησιμοποιηθούν κακόβουλα για αποταυτοποίηση. Επομένως, ένα μοντέλο απορρήτου όπως η l-ποικιλομορφία θα μπορούσε να επιλεγεί και να εφαρμοστεί στο σύνολο δεδομένων.

Name (*EI*)	**Age** (*QI*)	**Zip Code** (*QI*)	**Virus** (*SD*)
John	28	94032	Flu Type C
Max	25	94032	Flu Type C
Mary	22	94034	Flu Type A
Harry	20	94032	Flu Type B
Theresa	24	94034	Flu Type C

Εικόνα 16 Παράδειγμα δεδομένων υγειονομικής περίθαλψης που περιγράφει τύπους γρίπης για ασθενείς. Τα χαρακτηριστικά εκχωρούνται σε κατηγορίες απορρήτου[14].

Το EI στην l-ποικιλομορφία ανωνυμοποιείται με διαγραφή (συμβολίζεται με «*»). Τα QI και SD είναι ανώνυμα, έτσι ώστε κάθε ομάδα (ηλικία, ταχυδρομικός κώδικας και σύμπτωμα) να περιέχει τουλάχιστον τρεις ίδιες εγγραφές. Οι τιμές για το χαρακτηριστικό «ηλικία» γενικεύονται κατά δεκαετίες, γεγονός που οδηγεί σε γενίκευση κάθε τιμής (π.χ. «20» σε «20 – 29»). Για τον ταχυδρομικό κώδικα, η κατάργηση εφαρμόζεται ξεκινώντας από τον τελευταίο χαρακτήρα, ο οποίος είναι κατάλληλος για γερμανικούς ταχυδρομικούς κώδικες. Τέλος, το χαρακτηριστικό «virus» γενικεύεται από ειδική σε γενικότερη περιγραφή, π.χ. «Γρίπη τύπου Α» έως «γρίπη».

Το προκύπτον ανώνυμο σύνολο δεδομένων (βλ. εικόνα 17) μπορεί να ερμηνευθεί ως επιδημία στη γενική περιοχή του 9403*, παρόλο που τα αρχικά δεδομένα δείχνουν μόνο ένα κρούσμα γρίπης Τύπου Α στην περιοχή 94034 και ένα κρούσμα γρίπης Τύπου Β στο 94032. Επομένως, τα αρχικά δεδομένα δεν υποδεικνύουν ξέσπασμα επιδημίας, αλλά τα ανώνυμα δεδομένα ενδέχεται να υποδεικνύουν ξέσπασμα γρίπης (ποιος τύπος είναι απροσδιόριστος). Αν και δεν φαίνεται ρητά σε αυτό το παράδειγμα, η EI είναι ιδιαίτερα σημαντική σε δεδομένα χρονοσειρών στα οποία ο ίδιος ασθενής πρέπει να αναγνωριστεί σε πολλές εγγραφές. Αυτά θα καταστρέφονταν εντελώς ή θα είχαν παραποιηθεί με τεχνικές ανωνυμοποίησης.

Name (*EI*)	Age (*QI*)	Zip Code (*QI*)	Virus (*SD*)
*	20 - 29	9403*	Flu
*	20 - 29	9403*	Flu
*	20 - 29	9403*	Flu
*	20 - 29	9403*	Flu
*	20 - 29	9403*	Flu

Εικόνα 17: Αποπροσδιορισμένο σύνολο δεδομένων με εφαρμοσμένη 3-ποικιλομορφία[14].

Αυτό οδηγεί στο συμπέρασμα ότι οι τεχνικές ανωνυμοποίησης δεν επαρκούν αποκλειστικά. Οι τεχνικές ψευδωνυμοποίησης, στις οποίες δίνουμε μια ευρεία επισκόπηση στην επόμενη ενότητα, απαιτούνται και πρέπει να διερευνηθούν για το LPL.

3.3 Ψευδωνυμοποίηση

Γενικά, το αρχικό σύνολο δεδομένων D είναι ψευδωνυμοποιημένο σε D'. Αποτελείται από κατηγορίες δεδομένων που αναφέρθηκαν προηγουμένως.

D = (EI, QI, SD, NSD)

Στο D' τα χαρακτηριστικά αντικαθίστανται με μοναδικά αναγνωρίσιμα ψευδώνυμα. Ανάλογα με την περίπτωση χρήσης, μόνο το EI πρέπει να είναι ψευδωνυμοποιημένο. Η εφαρμογή των διαφορετικών κατηγοριών δεδομένων εξαρτάται από την περίπτωση χρήσης. Τυπικά, τα EI και QI είναι ψευδωνυμοποιημένα. Ωστόσο, τα SD και NSD μπορεί να είναι ψευδωνυμοποιημένα

D’ = (EI', QI’ SD’, NSD’).

Στη συνέχεια παρουσιάζεται επισκόπηση των μεθόδων ψευδωνυμοποίησης.

3.3.1 **Tokenization**

Το tokenization είναι ο μηχανισμός διαχωρισμού ή κατακερματισμού των προτάσεων και των λέξεων στο πιθανό μικρότερο μόρφημα που ονομάζεται token. Το token είναι η μικρότερη δυνατή λέξη μετά την οποία δεν μπορεί να σπάσει περαιτέρω[16]. Το tokenization ανταλλάσσει διαφορετικές τιμές με ένα διακριτικό(token). Η δημιουργία του token μπορεί να ποικίλλει και μπορεί να περιλαμβάνει μια ψευδοτυχαία φύτρα(seed) ή κλειδιά διευκόλυνσης. Γίνεται διάκριση μεταξύ εξαρτημένου και ανεξάρτητου tokenization. Το εξαρτημένο tokenization διατηρεί μια σχέση με τα αρχικά δεδομένα σε αντίθεση με το ανεξάρτητο tokenization.

Independent: TokenGenerator → Token
Dependent: TokenGenerator(Value) → Token

Ως αποτέλεσμα, τα ψευδώνυμα που βασίζονται σε ανεξάρτητα token είναι πιο ασφαλή, επειδή δεν είναι δυνατή η εκ νέου ταυτοποίηση μόνο με συγκεκριμένα ψευδώνυμα (π.χ. επιθέσεις με έγχυση). Γενικά, η δημιουργία token βασίζεται σε τυχαίες φύτρες, κρυπτογραφικές μεθόδους ή κατακερματισμό. Μια επισκόπηση δίνεται στη συνέχεια.

*Τυχαίες φύτρες(**Random Seeds)***

Ένα ψευδώνυμο μπορεί να δημιουργηθεί με βάση ψευδοτυχαίες φύτρες. Εδώ, είναι απαραίτητο να αποφευχθούν οι συγκρούσεις tokens. Για να υπάρξει περισσότερη ιδιωτικότητα, η τυχαία φύτρα μπορεί να συνδυαστεί με μυστικά κλειδιά. Ένα παράδειγμα είναι η γεννήτρια ταυτότητας ασθενούς από τον K. Pommerening.

Μέθοδοι κρυπτογράφησης

Οι προσεγγίσεις κρυπτογράφησης είναι είτε συμμετρικές είτε ασύμμετρες. Οι συμμετρικές προσεγγίσεις χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Για παράδειγμα, οι Heurix-Neubauer και άλλοι χρησιμοποιούν DES και AES. Οι ασύμμετρες προσεγγίσεις κρυπτογραφούν με δημόσιο κλειδί και αποκρυπτογραφούν με ιδιωτικό κλειδί. Ο Rottondi και άλλοι παρουσίασαν ψευδωνυμοποίηση με βάση το RSA. Τα κλειδιά πρέπει να αποθηκεύονται με ασφάλεια για να διατηρηθεί η σκοπιμότητα αυτής της προσέγγισης. Για να αποτραπεί οριστικά η αποψευδωνυμοποίηση, το ιδιωτικό κλειδί μπορεί να απορριφθεί. Γενικά, το μειονέκτημα των κρυπτογραφικών μεθόδων είναι το αυξημένο υπολογιστικό κόστος. Επιπλέον, το token που δημιουργείται μπορεί να μην έχει σταθερό μήκος και μπορεί να είναι πολύ υπερβολικό.

Κατακερματισμός

Μια συνάρτηση κατακερματισμού συνήθως αντιστοιχίζει ένα σύνολο εισόδου σε ένα μικρότερο σύνολο στόχων. Έτσι, οι περισσότερες συναρτήσεις κατακερματισμού δεν είναι ενέσιμες. Σε αντίθεση με τις κρυπτογραφικές μεθόδους, τα tokens που δημιουργούνται έχουν το ίδιο μέγεθος ανεξάρτητα από το μήκος των εισαγωγών. Ωστόσο, λόγω της φύσης της συνάρτησης κατακερματισμού, διαφορετικές είσοδοι μπορεί να γίνουν το ίδιο ψευδώνυμο. Επομένως, οι -ανθεκτικοί σε σύγκρουση- αλγόριθμοι κατακερματισμού προτιμώνται για την ψευδωνυμοποίηση. Επιπλέον, οι μέθοδοι κατακερματισμού μπορούν να ταξινομηθούν σε κατακερματισμό με κλειδί και χωρίς κλειδί. Οι Noumeir, Brekne και άλλοι χρησιμοποιούν αλγόριθμους SHA-X και MDX χωρίς κλειδί. Το μειονέκτημα του κατακερματισμού χωρίς κλειδί είναι ότι τα tokens που δημιουργούνται μπορούν να συνδεθούν μεταξύ διαφορετικών συνόλων δεδομένων εάν χρησιμοποιείται η ίδια συνάρτηση κατακερματισμού. Οι μέθοδοι με κλειδί επεκτείνουν τους κατακερματισμούς που βασίζονται σε κρυπτογράφηση με ένα κλειδί, π.χ. Κωδικός ελέγχου ταυτότητας μηνύματος κατακερματισμού (HMAC). Υποθέτοντας ότι το κλειδί παραμένει μυστικό, αποτρέπονται επιθέσεις λεξικού ή παρόμοιες επιθέσεις.

Τεχνικές Διατήρησης Αξίας

Υπάρχουν ορισμένες περαιτέρω μέθοδοι για το tokenization, οι οποίες διατηρούν συγκεκριμένες λειτουργίες σε μη αναγνωρισμένα σύνολα δεδομένων αυξάνοντας τη χρησιμότητα. Αυτοί οι αλγόριθμοι έχουν αναπτυχθεί για συγκεκριμένες περιπτώσεις χρήσης. Παραδείγματα είναι η ανωνυμοποίηση διεύθυνσης IP με διατήρηση προθέματος και η ψευδωνυμοποίηση με διατήρηση της απόστασης.

Πρότυπα Υλοποίησης

Για να αποκτηθούν πρόσθετα χαρακτηριστικά, όπως αυξημένος βαθμός απορρήτου ή δυνατότητα αποψευδωνυμοποίησης, το tokenization μπορεί να συνδυαστεί με πρόσθετες μεθόδους. Ας λάβουμε υπόψη ότι οι ακόλουθες μέθοδοι έχουν συγκριτικά πολύ αδύναμη απόδοση εάν χρησιμοποιούνται αποκλειστικά από άποψη ασφάλειας, ειδικά για μικρά σύνολα δεδομένων. Επομένως, θα πρέπει πάντα να συνδυάζονται με άλλες προσεγγίσεις.

Μια διπλή αντιστοίχιση αποθηκεύει το παραγόμενο token και την αρχική τιμή.

Value ↔ Token

Έτσι, επιτρέπει την εξουσιοδοτημένη αποψευδωνυμοποίηση του token. Επομένως, η αποθήκευση πρέπει να είναι κρυπτογραφημένη για να αποφευχθεί η μη εξουσιοδοτημένη ψευδωνυμοποίηση. Όταν προστίθενται νέες εγγραφές δεδομένων στο D, οι οποίες πρέπει να έχουν ψευδώνυμα, τότε κάθε τιμή θα αναζητηθεί στον κρυπτογραφημένο χώρο αποθήκευσης χαρτογράφησης και θα αντικατασταθεί από το αντίστοιχο token. Εάν δεν βρεθεί αντίστοιχο token δημιουργείται και προσαρτάται νέα αντιστοίχιση. Επομένως, το D με λιγότερες διακριτές τιμές επεξεργάζεται ταχύτερα από το D με διάφορες διακριτές τιμές. Η απόδοση της επεξεργασίας κατά την απονομή ψευδωνυμίας εξαρτάται από τη δομή δεδομένων που χρησιμοποιείται για αποθήκευση.

Η περιορισμένη παραγωγή tokens μιμείται τις αρχικές τιμές υπολογίζοντας αποκλειστικά ψευδώνυμα με το ίδιο σύνολο χαρακτήρων και την ίδια δομή. Ως αποτέλεσμα, το απόρρητο αυξάνεται. Για παράδειγμα, μια ημερομηνία θα προκύψει επίσης δομημένη ως ημερομηνία μετά την ψευδωνυμοποίηση. Η αντιμετάθεση δεδομένων ανταλλάσσει καταχωρήσεις με βάση τη συνάρτηση αντιμετάθεσης. Για κάθε νέα καταχώρηση, οι αλλαγές πρέπει να παρακολουθούνται με απλή αντιστοίχιση ή με ενημέρωση της λειτουργίας. Η ψευδωνυμοποίηση μπορεί να αναστραφεί εάν είναι γνωστή η αντιμετάθεση. Η προσθήκη θορύβου χρησιμοποιείται για να αποκτήσει περισσότερο απόρρητο προσθέτοντας έναν ψευδοτυχαίο θόρυβο στις καταχωρήσεις εισόδου. Ωστόσο, η ανίχνευση ανωμαλιών ή παρόμοιες τεχνικές μπορεί να αντιμετωπίσουν τον θόρυβο. Το αλάτισμα προσθέτει εντροπία στη διαδικασία δημιουργίας διακριτικών για να αυξήσει το κόστος υπολογισμού των επιθέσεων από λεξικά εμπιστευτικών πληροφοριών και επομένως μειώνει τον κίνδυνο αποψευδωνυμοποίησης. Η τιμή του άλατος μπορεί είτε να δημιουργηθεί ντετερμινιστικά από μια δεδομένη καταχώρηση όπως στο PBKDF2 (κατακερματισμός) είτε ως τυχαία τιμή όπως στην τροποποίηση RSA-OAEP (κρυπτογράφηση). Για ίσες τιμές το αλάτι επαναχρησιμοποιείται.

Συλλογισμός για διάφορες μεθόδους ψευδωνυμοποίησης

Η μέθοδος ψευδωνυμοποίησης πρέπει να επιλεγεί με βάση την προβλεπόμενη χρήση. Εδώ, πρέπει να ληφθούν υπόψη διάφορες πτυχές. Ξεκινώντας με τις ιδιότητες της τιμής δεδομένων, την απαιτούμενη χρησιμότητα του token και τη χρήση μεθόδων κατακερματισμού και κρυπτογράφησης. Θα πρέπει επίσης να ληφθεί υπόψη η απαίτηση για μεταγενέστερη απουσία ψευδωνυμοποίησης με χρήση διπλών αντιστοιχίσεων ή χρήση μονόδρομης ψευδωνυμοποίησης για αυξημένη ασφάλεια. Επιπλέον, μπορούν να προστεθούν πολλές τεχνικές για να επιτευχθεί το επιθυμητό επίπεδο απορρήτου/ασφάλειας. Λόγω των διαφόρων δυνατοτήτων για ψευδωνυμοποίηση, καταλήξαμε στην απαίτηση για μια γενική προδιαγραφή των μεθόδων ψευδωνυμοποίησης εντός του LPL και του γενικού πλαισίου απορρήτου του, το οποίο συζητάμε παρακάτω.

Ενσωμάτωση σε Layered Privacy Language (LPL)

Η Layered Privacy Language (LPL) προορίζεται για τη μοντελοποίηση πολιτικών απορρήτου που συνδυάζει τόσο τις νομικές απόψεις όσο και τις απόψεις της επιστήμης των υπολογιστών σχετικά με το απόρρητο. Η αρχική LPL [11] έχει επεκταθεί περαιτέρω από μια επέκταση διεπαφής χρήστη για να υποστηρίζει εικονίδια απορρήτου για τη διεπαφή χρήστη προσωπικής πολιτικής απορρήτου [12] και την επέκταση GDPR [13]. Επιπλέον, η LPL συνοδεύεται από ένα γενικό πλαίσιο απορρήτου που επιτρέπει την αποταυτοποίηση βάσει πολιτικής, χρησιμοποιώντας μεθόδους ανωνυμοποίησης και μοντέλα απορρήτου. Για τη διευκόλυνση των διαφόρων μεθόδων ψευδωνυμοποίησης εντός της LPL, πρέπει να επεκταθεί τόσο η πολιτική όσο και η διαδικασία αποταυτοποίησης βάσει πολιτικής. Αυτό φαίνεται στα παρακάτω.

Επέκταση ψευδωνυμοποίησης για LPL

Στη συνέχεια, περιγράφουμε την επέκταση ψευδωνυμοποίησης για LPL με βάση την αρχική επισημοποίηση από τον Gerl και άλλους[11]. Να σημειωθεί ότι η επέκταση διεπαφής χρήστη [12] και η επέκταση GDPR[13] δεν λαμβάνεται υπόψη καθώς δεν παρεμβαίνει στην ενσωμάτωση της ψευδωνυμοποίησης στην LPL. Το ριζικό στοιχείο της LPL είναι το LayeredPrivacyPolicy-element lpp, το οποίο παραμένει αμετάβλητο.

lpp = (version, name, lang, ppURI, upp, ds, P)

Αποτελείται από τον αριθμό έκδοσης LPL, το όνομα πολιτικών απορρήτου, τη γλώσσα που ορίζεται για την εμφάνιση περιγραφών, τον σύνδεσμο προς τη νομική πολιτική απορρήτου, το στοιχείο UnderlyingPrivacyPolicy, το στοιχείο DataSource και ένα σύνολο στοιχείων σκοπού.

Το στοιχείο Purpose-p επεκτείνεται επιτρέποντας τον ορισμό μεθόδων ψευδωνυμοποίησης σε συγκεκριμένα σύνολα δεδομένων.

p = (name, optOut, required, descr, DR, r, pm, D, PSM)

Επομένως, το p αποτελείται από το όνομά του, τη σημαία κατάστασης που προσδιορίζει εάν ο χρήστης μπορεί να εξαιρεθεί ή να επιλέξει τον σκοπό, μια σημαία εάν ο σκοπός πρέπει να γίνει αποδεκτός, περιγραφή σε καθορισμένη γλώσσα γλώσσας, σύνολο στοιχείων DataRecipient dr, Retention στοιχείο r, PrivacyModel στοιχείο pm, και ένα σύνολο στοιχείων d. Επίσης το σύνολο της μεθόδου ψευδωνυμοποίησης psm, το οποίο θα αναλυθεί περαιτέρω.

Μια μέθοδος ψευδωνυμοποίησης psm αντιπροσωπεύει μία διαμόρφωση ψευδωνυμοποίησης, η οποία θα εφαρμοστεί στο σύνολο δεδομένων.

psm = (name, attrName, NOD, descr, header, PSMA)

Είναι μια πλειάδα με τα ακόλουθα χαρακτηριστικά:

- name: Ορίζει την προσέγγιση ψευδωνυμοποίησης. Αποτελείται προκαθορισμένο σύνολο διαθέσιμων μεθόδων.
- attrName: Κειμενική αναπαράσταση ονόματος για νέο χαρακτηριστικό, το οποίο περιέχει ψευδώνυμα.
- NOD: Σύνολο NameOfData στοιχείων, το οποίο αντιπροσωπεύει χαρακτηριστικά για να ψευδωνυμοποιηθούν. Αναφέρεται στο χαρακτηριστικό όνομα του στοιχείου δεδομένων. Πρέπει τουλάχιστον να αποτελείται από ένα έγκυρο όνομα.
- descr: Αναγνώσιμη από τον άνθρωπο περιγραφή της ψευδωνυμοποίησης σε καθορισμένη γλώσσα lang .
- header: Αναγνώσιμη από τον άνθρωπο κεφαλίδα ψευδωνυμοποίησης σε καθορισμένη γλώσσα γλώσσα lang.
- PSMA: Σύνολο στοιχείων χαρακτηριστικών μεθόδου ψευδωνυμοποίησης psma που περιγράφει περαιτέρω διαμορφώσεις της προσέγγισης ψευδωνυμοποίησης.

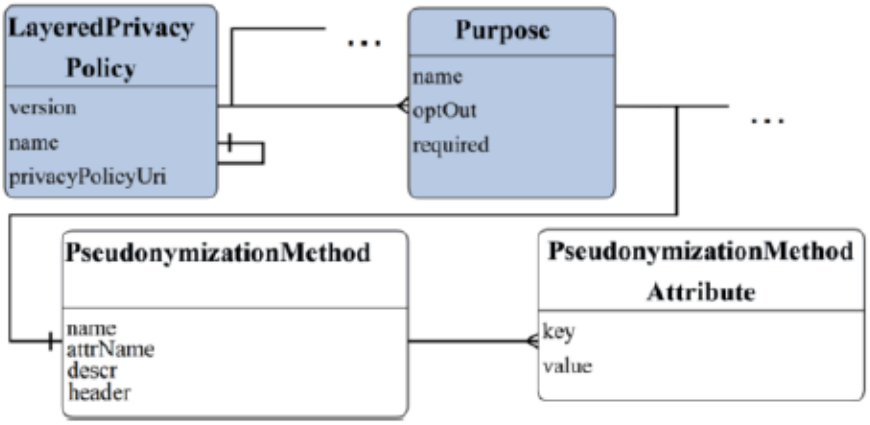
Κάθε στοιχείο μεθόδου ψευδωνυμοποίησης χαρακτηριστικού psma διαμορφώνει την καθορισμένη προσέγγιση:

psma = (key; value)

Αυτή η πλειάδα κλειδιού-τιμής ορίζει χαρακτηριστικά απαραίτητα για όλες τις πιθανές μεθόδους.

Η LPL έχει επεκταθεί με την προσθήκη του στοιχείου της μεθόδου ψευδωνυμοποίησης psm και του στοιχείου της μεθόδου ψευδωνυμοποίησης χαρακτηριστικού psma, το οποίο επιτρέπει τον ορισμό διαφόρων μεθόδων ψευδωνυμοποίησης (βλ. Εικόνα 18). Στην τρέχουσα κατάσταση, η επέκταση υποστηρίζει διάφορες προσεγγίσεις κατακερματισμού (SHA-X, MDX), κατακερματισμό με κλειδί (HMAC SHA-X), κατακερματισμό με κλειδί με εντροπίες και χαρτογράφηση (PBKDF2 HMAC SHA-X), συμμετρική κρυπτογραφία (AES, DES, 3DES , RC4, Blowfish) και τυχαίες φύτρες με χαρτογράφηση. Περαιτέρω προσεγγίσεις μπορούν εύκολα να προστεθούν ορίζοντας τες ως στοιχεία psm και psma.

Τα μυστικά, τα οποία μπορεί να οδηγήσουν σε επαναπροσδιορισμό, δεν αποθηκεύονται στο μοντέλο LPL. Σύμφωνα με τον GDPR, αυτές οι πληροφορίες πρέπει να αποθηκεύονται χωριστά. Η συγκεκριμένη διαχείριση κλειδιού και μυστικού ανήκει στον ελεγκτή, την οντότητα που διαχειρίζεται τα αποθηκευμένα δεδομένα.



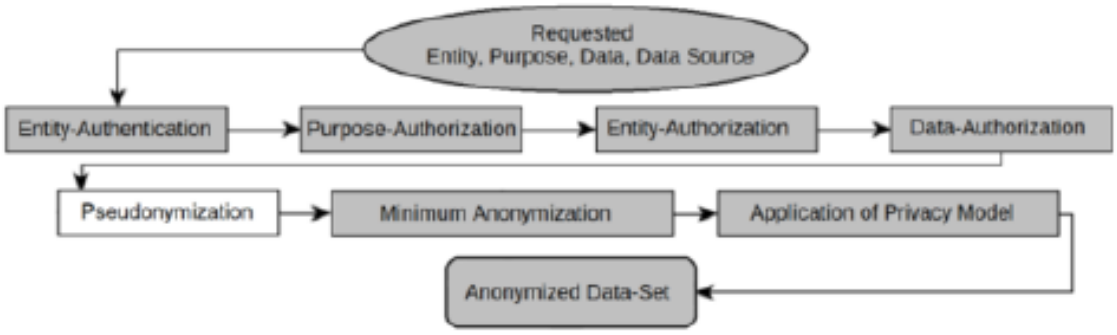
Εικόνα 18: Η δομή LPL επεκτείνεται από τα στοιχεία ψευδωνυμοποίησης. Περαιτέρω στοιχεία και χαρακτηριστικά παραλείπονται για το πεδίο εφαρμογής αυτής της εργασίας[14].

Αποταυτοποίηση βάσει πολιτικής

Η αποταυτοποίηση βάσει πολιτικής βασισμένη στην LPL απαιτεί από την αιτούσα οντότητα να παρέχει τον σκοπό, ένα σύνολο δεδομένων και ένα σύνολο πηγών δεδομένων για το αίτημα. Στη συνέχεια, η αιτούσα οντότητα θα επαληθευτεί. Ο σκοπός, η οντότητα και το σύνολο δεδομένων θα εξουσιοδοτηθούν έναντι των ιδιοτήτων των αντίστοιχων πολιτικών απορρήτου lpp των πηγών δεδομένων. Κατά τη διάρκεια της ελάχιστης ανωνυμοποίησης θα εφαρμόζονται εξατομικευμένες ρυθμίσεις απορρήτου για κάθε πηγή δεδομένων. Τέλος, ένα κοινό μοντέλο απορρήτου προέρχεται από όλα τα σχετικά lpp και εφαρμόζεται στο σύνολο δεδομένων.

Αυτή η αλυσίδα διεργασιών θα επεκταθεί προσθέτοντας τη διαδικασία ψευδωνυμοποίησης πριν από την ελάχιστη ανωνυμοποίηση (βλ. Εικόνα 19). Με ανεστραμμένη σειρά, η ανωνυμοποίηση πριν από την ψευδωνυμοποίηση, θα είχε ως αποτέλεσμα τη λιγότερη διατήρηση της χρησιμότητας, λόγω της πιθανής ανωνυμοποίησης των τιμών που θα πρέπει να διατηρηθούν με tokenization αμφιμονοσήμαντης

αντιστοιχίας. Κάθε στοιχείο δεδομένων με ψευδώνυμα θα τροποποιηθεί μετά την ψευδωνυμοποίηση. Για παράδειγμα, η ταξινόμηση θα αλλάξει σε NDS για να αποφευχθεί οποιαδήποτε περαιτέρω ανωνυμοποίηση από μεταγενέστερες διαδικασίες.



Εικόνα 19: Τροποποιημένες διαδικασίες αποταυτοποίησης βάσει πολιτικής του πλαισίου LPL όταν ζητούνται δεδομένα[14].

3.3.2 Αποτελέσματα σεναρίου υγειονομικής περίθαλψης

Με την επέκταση ψευδωνυμοποίησης μπορούμε τώρα να αποταυτοποιήσουμε το σύνολο δεδομένων της γρίπης (βλ. εικόνα 16) και ταυτόχρονα να προσθέσουμε τη δυνατότητα επαναπροσδιορισμού χρησιμοποιώντας διπλές αντιστοιχίσεις. Τα ονόματα ασθενών και ο τύπος του ιού στο παράδειγμα της γρίπης θα αποθηκευτούν ως ψευδώνυμα ή αναγνωριστικά. Για παράδειγμα, εάν προκύψουν νέες γνώσεις σχετικά με την υγεία των ασθενών, τα αναγνωριστικά μπορούν να αφαιρεθούν από ψευδωνυμία για να παραδίδουν αυτές τις νέες πληροφορίες στους επηρεαζόμενους ασθενείς αποκτώντας την ταυτότητά τους και τις πληροφορίες για τον ιό.

Η ακόλουθη διαμόρφωση, χρησιμοποιώντας τον αλγόριθμο HMAC-SHA-1 και τη γεννήτρια αναγνωριστικών ασθενούς σε συνδυασμό με αντιστοιχίσεις, θα επιτύχει μια τέτοια ψευδωνυμοποίηση:

psm_0 = (“HMAC-SHA-1”, “Name -ID”, {“Name”},
“Description_0”, “HMAC-SHA-1 pseudonymization”, {})
psm_1 = (“PID”, “Virus-ID”, {“Virus”}, “Description_1”,
“PID pseudonymization”, {})

Αξίζει να σημειωθεί ότι το κλειδί, που είναι απαραίτητο για το HMAC, και η χαρτογράφηση δεν ορίζονται στην πολιτική απορρήτου LPL για συμμόρφωση με τον GDPR.

Τα αποτελέσματα της ψευδωνυμοποίησης, που εφαρμόζονται στα ανεπεξέργαστα δεδομένα (βλ. εικόνα 16), που ορίζονται από τα psm_0 και psm_1, δίνονται στην εικόνα 20, στην οποία έχει πρόσβαση ο αναλυτής δεδομένων. Στην εικόνα 20 δεν εφαρμόζονται μοντέλα ανωνυμοποίησης ή απορρήτου. Οι αντιστοιχίσεις, που είναι απαραίτητες για την εκ νέου αναγνώριση, μπορούν να εξεταστούν στην εικόνα 21, η οποία θα πρέπει να είναι ασφαλισμένη και να είναι προσβάσιμη μόνο από εξουσιοδοτημένο προσωπικό. Η επέκταση υποστηρίζει επίσης μια κρυπτογράφηση AES για αντιστοιχίσεις για την αύξηση των ιδιοτήτων ασφαλείας.

Name-ID (*NSD*)	Age (*QI*)	Zip Code (*QI*)	Virus-ID (*NSD*)
EA4B255	28	94032	KM93N2O
ADE0D85	25	94032	KM93N2O
2412F8F	22	94034	93I8M72
FF85768	20	94032	0O9INMW
71624DB	24	94034	KM93N2O

Εικόνα 20: Αποπροσδιορισμένο σύνολο δεδομένων με ψευδωνυμοποίηση. Τα ψευδώνυμα συντέμνονται για καλύτερη αναγνωσιμότητα[14].

Name-ID	Name
EA4B255	John
ADE0D85	Max
2412F8F	Mary
FF85768	Harry
71624DB	Theresa

Virus-ID	Virus
93I8M72	Flu Type A
0O9INMW	Flu Type B
KM93N2O	Flu Type C

Εικόνα 21: Αντιστοιχίσεις που μπορούν να επαναφέρουν περιεχόμενο που αντικαθίστανται από ψευδώνυμα[14].

Εάν τώρα συγκρίνουμε ανωνυμοποιημένα δεδομένα (βλ. εικόνα 17) και ψευδωνυμοποιημένα δεδομένα (βλ. εικόνα 20), δε μπορούμε πλέον να κάνουμε λανθασμένο συμπέρασμα. Μπορεί να παρατηρηθεί ότι υπάρχουν διαφορετικοί τύποι ιών, οι οποίοι μπορούν να αποδοθούν μοναδικά σε άτομα. Ωστόσο, μπορεί να φανεί ότι υπάρχει ομαδοποίηση. Όμως, με τις διπλές χαρτογραφήσεις μπορεί να αποδειχθεί ότι ο συχνά εμφανιζόμενος ιός KM93N2O είναι η σχετικά αβλαβής γρίπη τύπου C. Επομένως, μπορεί να εξαχθεί το συμπέρασμα ότι δεν υπάρχει επιδημία γρίπης. Επιπλέον, η ψευδωνυμοποίηση του SD μπορεί να μετριάσει τη σύνδεση χαρακτηριστικών, την αναγνώριση με ευαίσθητο χαρακτηριστικό. Λόγω της ψευδωνυμοποίησης, ο εισβολέας δεν μπορεί να συναγάγει το απόρρητο αναγνωρίζοντας άτομα με μοναδικά ευαίσθητα χαρακτηριστικά ή να χρησιμοποιεί εξωτερικές γνώσεις, επειδή οι παρεχόμενες πληροφορίες δεν είναι αναγνώσιμες από τον εισβολέα.

4. Ένα Δίκτυο κρυπτογράφησης και αποκρυπτογράφησης εικόνας βασισμένο σε βαθιά μάθηση για το Διαδίκτυο ιατρικών πραγμάτων

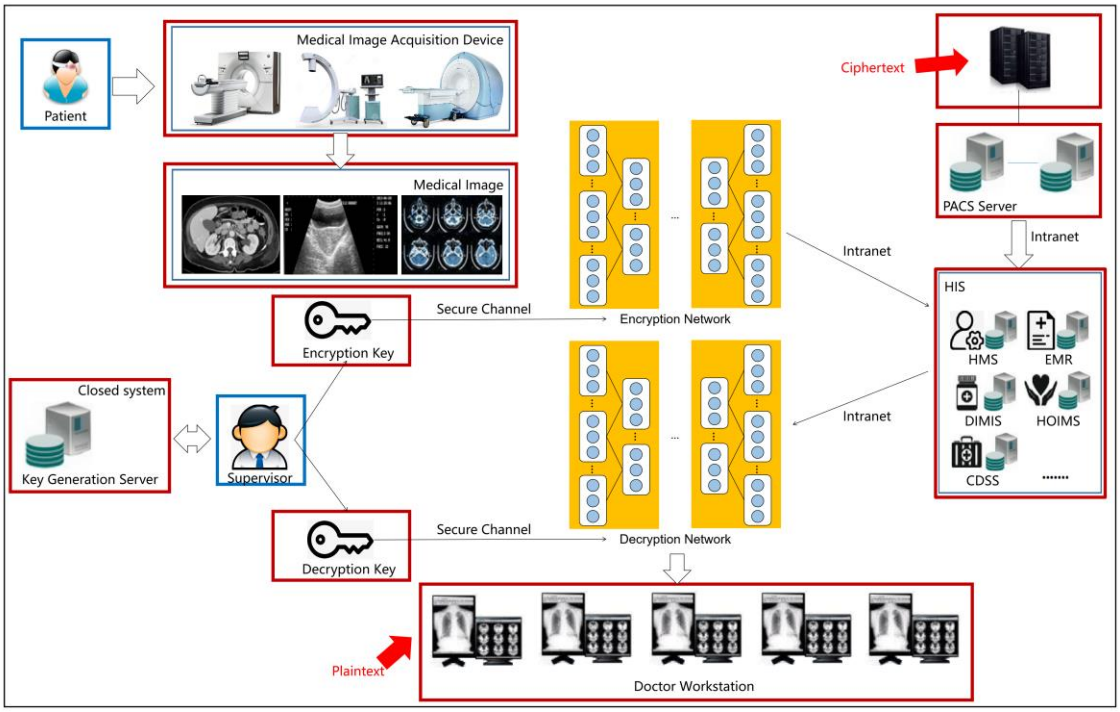
4.1 Εισαγωγή

Το Internet of Medical Things (IoMT) είναι ένας διεπιστημονικός τομέας που υιοθετεί τις τεχνολογίες Διαδικτύου των Πραγμάτων (IoT) στον τομέα της ιατρικής [17]. Με την ανάπτυξη του IoMT, πολλοί ιατρικοί εξοπλισμοί απεικόνισης συνδέονται ευρέως για να διευκολύνουν τη διαδικασία διάγνωσης και θεραπείας για τους γιατρούς, π.χ. η μαγνητική τομογραφία εγκεφάλου (MRI) για τη διάγνωση όγκων εγκεφάλου και η υπολογιστική τομογραφία (CT) πνεύμονα για ανίχνευση οζιδίου πνεύμονα. Στο IoMT, η διαχείριση των ιατρικών εικόνων γίνεται συνήθως από ένα σύστημα που ονομάζεται Συστήματα Αρχειοθέτησης και Επικοινωνίας Εικόνων (PACS) [19]. Όταν ένας ασθενής σαρώνεται από τον ιατρικό εξοπλισμό απεικόνισης, οι ιατρικές εικόνες που δημιουργούνται θα αποθηκευτούν πρώτα στο PACS. Όταν ο γιατρός αρχίσει να εξετάζει τον ασθενή, το PACS θα ανακτήσει τις απαραίτητες εικόνες από τη βάση δεδομένων και θα μεταφέρει τις εικόνες στο σταθμό εργασίας των γιατρών που λειτουργεί με τις πληροφορίες του ασθενούς από το Σύστημα Πληροφοριών του Νοσοκομείου (HIS). Αν και το PACS και το HIS λειτουργούν σε περιβάλλον intranet, εξακολουθούν να υπάρχουν ορισμένα κρίσιμα ζητήματα ασφάλειας κατά την αποθήκευση, τη μεταφορά και την αξιολόγηση ιατρικών εικόνων, τα οποία διατηρούν ευαίσθητες πληροφορίες απορρήτου των ασθενών. Εάν ένας εισβολέας, είτε εσωτερικός είτε εξωτερικός εισβολέας, έχει τη δυνατότητα να εισβάλει στο PACS ή στο HIS, γίνεται πολύ εύκολο να κρυφακούει αυτές τις ιατρικές εικόνες, με αποτέλεσμα τη σοβαρή διαρροή πληροφοριών απορρήτου των ασθενών [22].

Για την προστασία του συστήματος IoMT και την προστασία του απορρήτου των ασθενών, μπορεί να πραγματοποιηθεί κρυπτογράφηση και αποκρυπτογράφηση σε ιατρικές εικόνες, π.χ. Πρότυπο κρυπτογράφησης δεδομένων (DES), Προηγμένο Πρότυπο Κρυπτογράφησης (AES) και Συνάρτηση κατακερματισμού (Hash function). Επιπλέον, η κρυπτογράφηση εικόνας που βασίζεται σε χαοτικά συστήματα χρησιμοποιείται επίσης στη βιβλιογραφία [23]. Ωστόσο, αυτές οι μέθοδοι είναι δύσκολο να επιτύχουν μια καλή ισορροπία μεταξύ της απόδοσης ασφάλειας και της αποτελεσματικότητας κρυπτογράφησης. Η βαθιά μάθηση (deep learning) έχει επίσης μεγάλες δυνατότητες για την αντιμετώπιση αυτού του ζητήματος, όπου τα πολυεπίπεδα νευρωνικά δίκτυα εξάγουν μια ιεραρχία χαρακτηριστικών από ακατέργαστες εικόνες εισόδου. Το Συνελικτικό Νευρωνικό Δίκτυο (CNN) [24] έχει αποδείξει τα σημαντικά πλεονεκτήματα στην όραση υπολογιστή [25][30] καθώς και στη μεταφορά τομέα εικόνας [31]. Η μεταφορά της εικόνας από έναν τομέα σε έναν άλλο μπορεί να θεωρηθεί ως πρόβλημα μεταφοράς λεπτομέρειας όπου ο στόχος είναι να μάθουμε τη σχέση αντιστοίχισης μεταξύ μιας εικόνας εισόδου και μιας εικόνας εξόδου από ένα σύνολο στοιχισμένων ζευγών εικόνων. Μία από τις πιο δημοφιλείς μεθόδους μετασχηματισμού εικόνας σε εικόνα είναι τα Cycle-Consistent Adversarial Networks, τα οποία εισάγουν απώλειες συνοχής δύο κύκλων που μετατρέπουν την εικόνα από τον έναν τομέα στον άλλο και στη συνέχεια ανακατασκευάζουν ξανά την αρχική εικόνα. Στην πραγματικότητα, ο αλγόριθμος βαθιάς μάθησης έχει επίσης υιοθετηθεί για την επίλυση του προβλήματος της αποθορυβοποίησης εικόνας [32].

Εμπνευσμένο από τα παραπάνω έργα, σε αυτό το κεφάλαιο, προτείνεται ένα δίκτυο κρυπτογράφησης και αποκρυπτογράφησης εικόνων που βασίζεται σε βαθιά μάθηση (DeepEDN) για μετασχηματισμό εικόνας σε εικόνα και αποθορυβοποίηση εικόνας. Η νέα ιδέα βασίζεται στις ακόλουθες δύο σημαντικές ιδέες: (1) Εάν η ιατρική εικόνα μπορεί να μεταφερθεί σε άλλο τομέα εικόνας που είναι πολύ διαφορετικός από τον αρχικό, αυτή η ιατρική εικόνα μπορεί να θεωρηθεί ως κρυπτογραφημένη και (2) η διαδικασία αποκρυπτογράφησης ιατρικών εικόνων μπορεί να υλοποιηθεί με τον τρόπο αποθορυβοποίησης ή ανακατασκευής εικόνας. Στο DeepEDN, το δίκτυο Cycle-GAN χρησιμοποιείται ως το κύριο δίκτυο εκμάθησης για την υλοποίηση του μετασχηματισμού εικόνας σε εικόνα. Υπάρχουν δύο τομείς στη διαδικασία κρυπτογράφησης: ο τομέας της αρχικής ιατρικής εικόνας και ο τομέας προορισμού, όπου ο τομέας προορισμού θεωρείται ως "ο κρυφός παράγοντας" που καθοδηγεί το μοντέλο εκμάθησης για την υλοποίηση της διαδικασίας κρυπτογράφησης. Το δίκτυο κρυπτογράφησης, αποτελείται από ένα δίκτυο παραγωγής και ένα δίκτυο διαχωρισμού. Ο πρώτος θα δημιουργήσει την εικόνα παρόμοια με τον τομέα προορισμού, ενώ ο δεύτερος θα προωθήσει το δίκτυο παραγωγής για να δημιουργήσει τις ίδιες εικόνες με τον τομέα προορισμού προσδιορίζοντας τις δημιουργούμενες εικόνες. Επομένως, μετά την επεξεργασία με τη χρήση του δικτύου κρυπτογράφησης, η αρχική ιατρική εικόνα μπορεί να μετατραπεί στον τομέα προορισμού και να γίνει το κρυπτογραφημένο κείμενο. Η διαδικασία αποκρυπτογράφησης είναι παρόμοια με τις παραδοσιακές μεθόδους κρυπτογράφησης-αποκρυπτογράφησης, η οποία είναι η αντίστροφη λειτουργία της διαδικασίας κρυπτογράφησης. Στην πράξη, ένα δίκτυο ανακατασκευής, το οποίο είναι στην πραγματικότητα μια διαδικασία αποκρυπτογράφησης, χρησιμοποιείται για την επαναφορά της κρυπτογραφημένης εικόνας στην αρχική. Στο DeepEDN, οι παράμετροι του δικτύου παραγωγής θεωρούνται ως το ιδιωτικό κλειδί για την κρυπτογράφηση ενώ οι παράμετροι του δικτύου ανακατασκευής θεωρούνται ως το ιδιωτικό κλειδί για την αποκρυπτογράφηση. Επιπλέον, το DeepEDN υιοθετεί την μάθηση χωρίς επίβλεψη για να εκπαιδεύσει το δίκτυο εκμάθησης και δεν χρειάζεται πολλά δείγματα με ετικέτα. Ξεπερνά τα ζητήματα δεδομένων στην εκπαίδευση και είναι ευεργετικό για την εφαρμογή της βαθιάς μάθησης σε αρχεία κρυπτογραφίας.

Με βάση το DeepEDN, το σύστημα PACS βελτιώνεται με τη χρήση ενός διακομιστή παραγωγής κλειδιών. Όπως φαίνεται στην εικόνα 22, ο διακομιστής παραγωγής κλειδιών είναι υπεύθυνος για την εκπαίδευση του δικτύου κρυπτογράφησης και του δικτύου αποκρυπτογράφησης. Το σύστημα PACS μπορεί να καλέσει το δίκτυο κρυπτογράφησης για να κρυπτογραφήσει την ιατρική εικόνα και στη συνέχεια να αποθηκεύσει αυτές τις εικόνες κρυπτογραφημένου κειμένου στη βάση δεδομένων εικόνων. Κατά την αναθεώρηση, το σύστημα HIS θα υιοθετήσει το δίκτυο αποκρυπτογράφησης για την αποκρυπτογράφηση της εικόνας κρυπτογραφημένου κειμένου στην αρχική. Το δίκτυο κρυπτογράφησης και το δίκτυο αποκρυπτογράφησης θα μεταφερθούν μέσω του ασφαλούς καναλιού. Επιπλέον, προτείνεται ένα δίκτυο εξόρυξης ROI για την άμεση εξαγωγή του ROI (όργανο ή ιστό) από την κρυπτογραφημένη ιατρική εικόνα χωρίς αποκρυπτογράφηση. Πιο συγκεκριμένα, κατά την εισαγωγή μιας κρυπτογραφημένης ιατρικής εικόνας στο δίκτυο εξόρυξης ROI, το ενδιαφερόμενο τμηματοποιημένο αντικείμενο μπορεί να εξαχθεί απευθείας χωρίς να αποκαλύπτονται άλλα μέρη των πληροφοριών του ασθενούς.



Εικόνα 22: Η αρχιτεκτονική του DeepEDN[39].

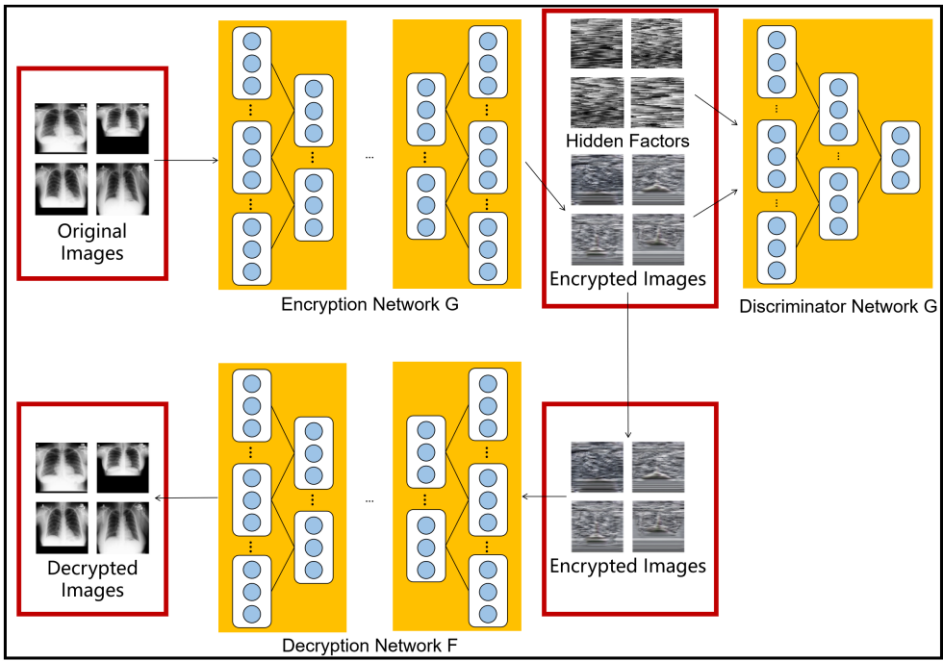
4.2 Αρχιτεκτονική του DeepEDN

Το παραδοσιακό δίκτυο που βασίζεται στο GAN που χρησιμοποιείται για εκμάθηση μεταφοράς τομέα μπορεί να μετατρέψει μόνο την αρχική εικόνα στην εικόνα του τομέα προορισμού. Ωστόσο, αντιμετωπίζοντας την κρυπτογράφηση και την αποκρυπτογράφηση εικόνας, εκτός από τη μετατροπή της αρχικής ιατρικής εικόνας σε εικόνα κρυπτογραφημένου κειμένου, πρέπει επίσης να επαναφέρουμε την εικόνα κρυπτογραφημένου κειμένου στην αρχική εικόνα, δηλαδή την ανακατασκευή εικόνας. Μπορεί να διαπιστωθεί ότι το δίκτυο Cycle-Gan επιτυγχάνει καλή απόδοση στον τομέα του μετασχηματισμού τομέα και της ανακατασκευής εικόνας μέσω της δημιουργίας αντίθετης απώλειας και της κυκλικής συνεπούς απώλειας. Ως εκ τούτου, το Δίκτυο Cycle Gan υιοθετείται ως το δίκτυο εκμάθησης σε αυτήν την εργασία.

Όπως φαίνεται στην εικόνα 23, το DeepEDN αποτελείται κυρίως από τρία υποδίκτυα: το δίκτυο κρυπτογράφησης G, το δίκτυο διαχωρισμού D και το δίκτυο αποκρυπτογράφησης F. Το δίκτυο κρυπτογράφησης G χρησιμοποιείται για την κρυπτογράφηση των αρχικών εικόνων εισόδου, το δίκτυο αποκρυπτογράφησης F είναι υπεύθυνο για επαναφορά των κρυπτογραφημένων εικόνων στην αρχική (αποκρυπτογράφηση της εικόνας) και το δίκτυο διαχωρισμού D έχει σχεδιαστεί κυρίως για τη βελτίωση της απόδοσης του δικτύου κρυπτογράφησης διακρίνοντας τις παραγόμενες εικόνες από τις εικόνες στον τομέα προορισμού (Hiding Factors). Στις μεθόδους βαθιάς μάθησης, η συνάρτηση απώλειας χρησιμοποιείται συνήθως για την εκπαίδευση του μοντέλου. Η συνολική απώλεια L του προτεινόμενου μοντέλου δίνεται ως εξής:

$$L = LG + LD + LR; \qquad (1)$$

όπου το LG υποδεικνύει την απώλεια του δικτύου κρυπτογράφησης G, το LD δηλώνει την απώλεια του δικτύου διαχωρισμού D και το LR υποδεικνύει την απώλεια του δικτύου αποκρυπτογράφησης F.



Εικόνα 23: Η συνολική δομή του DeepEDN[39].

Το δίκτυο κρυπτογράφησης G χρησιμοποιείται για τη μετατροπή των αρχικών ιατρικών εικόνων στον τομέα-στόχο για κρυπτογράφηση ιατρικής εικόνας. Το δίκτυο G ξεκινά με ένα αρχικό στάδιο συνέλιξης για τη χωρική μείωση δειγματοληψίας και κωδικοποίηση των εικόνων, και τα χρήσιμα χαρακτηριστικά που λαμβάνονται σε αυτό το στάδιο θα χρησιμοποιηθούν για τον επόμενο μετασχηματισμό. Στη συνέχεια, εκτελούνται εννέα υπολειπόμενα μπλοκ για την κατασκευή της πολλαπλής και των χαρακτηριστικών περιεχομένου. Οι εικόνες εξόδου ανακατασκευάζονται με δύο επάνω μπλοκ συνέλιξης που περιέχουν ένα διασκελισμένο επίπεδο συνέλιξης και ο διασκελισμός ορίζεται στο 2. Τέλος, η πρόβλεψη εξάγεται από έναν πυρήνα συνέλιξης 7 x 7. Επιπλέον, η δομή του δικτύου αποκρυπτογράφησης F είναι ίδια με το δίκτυο κρυπτογράφησης G.

Το προτεινόμενο μοντέλο περιλαμβάνει δύο αντιστοιχίσεις G : X →Y και Φ : N → X. Ο στόχος της αντιστοίχισης της συνάρτησης G είναι να μάθει πώς να μετασχηματίζει τις αρχικές ιατρικές εικόνες X στις εικόνες Y στον τομέα προορισμού και να εξαπατήσει το δίκτυο διαχωρισμού D. Όταν το δίκτυο διαχωρισμού D δε μπορεί να διακρίνει με επιτυχία εάν μια εικόνα δημιουργείται από το δίκτυο κρυπτογράφησης G ή πραγματικός τομέας εικόνας κρυπτογραφημένου κειμένου Y , σημαίνει ότι το δίκτυο κρυπτογράφησης G μετατρέπει τον αρχικό τομέα εικόνας ασθενούς X σε έναν τομέα εικόνας κρυπτογραφημένου κειμένου Y με επιτυχία. Η απώλεια LG του κρυπτογραφημένου δικτύου G είναι:

$$LG = \min_G(E_{x\sim pdata(x)}\log(1 - D(G(x)))); \qquad (2)$$

όπου το G αντιπροσωπεύει ένα δίκτυο κρυπτογράφησης και το D αντιπροσωπεύει το δίκτυο διαχωρισμού. Ο στόχος της LG είναι να ελαχιστοποιήσει το ποσοστό επιτυχίας του δικτύου διαχωρισμού

D για την ανίχνευση του κρυπτογραφημένου κειμένου που δημιουργείται από το δίκτυο κρυπτογράφησης G. Εκτός από την κρυπτογράφηση, ένας άλλος στόχος της προτεινόμενης μεθόδου είναι να διασφαλίσει ότι η αποκατασταθείσα εικόνα διατηρεί τις πληροφορίες το αρχικό ακόμα και κρυπτογραφημένο. Όπως φαίνεται στην εικόνα 23, για κάθε εικόνα x από τον τομέα X, η απώλεια ανακατασκευής μετρά τη διαφορά μεταξύ του G(x) και της αρχικής εικόνας, δηλ., x→ G(x) → F(G(x)) ≈ x. Η απώλεια ανακατασκευής L ορίζεται ως:

$$LR = E_{x\sim pdata(x)} ||F(G(X) - X||_1$$

$$= \mathrm{Ex}\sim\mathrm{pdata(x)} \sum_{i=1}^{n} |F(G(xi) - xi| \qquad (3)$$

Το δίκτυο διαχωρισμού D χρησιμοποιείται για να αξιολογήσει εάν η εικόνα εξόδου του δικτύου κρυπτογράφησης ανήκει στον τομέα προορισμού. Για το δίκτυο διάκρισης D, μετά από επεξεργασία με αρχικά συνελικτικά στρώματα, υιοθετούνται δύο γραμμικά συνελικτικά μπλοκ για να μειωθεί η ανάλυση της εικόνας και να κωδικοποιηθούν βασικά τοπικά χαρακτηριστικά για επακόλουθη διάκριση. Στη συνέχεια, το δίκτυο χρησιμοποιεί ένα μπλοκ κατασκευής χαρακτηριστικών και ένα συνελικτικό στρώμα 3 x 3 για να αποκτήσει το τελικό αποτέλεσμα. Επιπλέον, για κάθε συνελικτικό επίπεδο, υιοθετείται το Leaky ReLU (LReLU) με α = 0.2 και ακολουθείται από ένα στρώμα κανονικοποίησης παρτίδας (BN).

Η εκπαίδευση του δικτύου διαχωρισμού D είναι να ταξινομεί τις εικόνες και να ελέγχει εάν προέρχεται από τον τομέα κρυπτογραφημένου κειμένου Y ή δημιουργείται από το δίκτυο κρυπτογράφησης G. Το δίκτυο κρυπτογράφησης G προσπαθεί να δημιουργήσει μια εικόνα G(x) παρόμοια με την εικόνα στον τομέα Y , ενώ το δίκτυο διάκρισης D στοχεύει να βρει τη διαφορά μεταξύ μετασχηματισμένων δειγμάτων από το G(x) και πραγματικών δειγμάτων στο Y . Η ελαχιστοποίηση της απώλειας L_D του δικτύου διαχωρισμού D ισοδυναμεί με τη μεγιστοποίηση της ακρίβειας ταξινόμησης του δικτύου διακρίσεων D, η οποία είναι αντίθετη με τον στόχο του δικτύου κρυπτογράφησης G. Η απώλεια L_D δίνεται ως εξής:

$$L_D=E_{x\sim pdata(x)}\log D(x)+E_{x\sim pdata(x)}\log(1-D(G(x))) \quad (4)$$

όπου το G αντιπροσωπεύει το κρυπτογραφημένο δίκτυο και το D το δίκτυο διαχωρισμού. Η L_D και η L_G στο δίκτυο GAN σχηματίζουν μια αντίπαλη σχέση. Όταν τα δύο δίκτυα φτάσουν σε κατάσταση ισορροπίας, το δίκτυο διάκρισης D μπορεί να επιτύχει ακρίβεια ταξινόμησης 50% τόσο για την εικόνα κρυπτογραφημένου κειμένου που δημιουργείται όσο και για την εικόνα τομέα πραγματικού κρυπτοκειμένου Y . Με άλλα λόγια, η εικόνα κρυπτογραφημένου κειμένου που δημιουργείται από το δίκτυο κρυπτογράφησης G είναι τόσο παρόμοια με τον τομέα πραγματικού κρυπτογραφημένου κειμένου Y, έτσι ώστε το δίκτυο διάκρισης D να μην μπορεί να τα διακρίνει.

Στο DeepEDN, οι τελικές παράμετροι του δικτύου G μπορούν να θεωρηθούν ως το ιδιωτικό κλειδί για κρυπτογράφηση ενώ οι παράμετροι του δικτύου F θεωρούνται ως το ιδιωτικό κλειδί για αποκρυπτογράφηση. Για κρυπτογράφηση, οι παράμετροι για κάθε συνελικτικό επίπεδο αρχικοποιούνται αρχικά τυχαία ως εξής:

$$W_n = \mathrm{random}[w_{n,1}, w_{n,2}, \ldots., w_{n,j}, \ldots], \quad (5)$$

όπου w_n είναι το n^{th} συνελικτικό στρώμα και $w_{n,j}$ είναι η j-th παράμετρος ενός συνελικτικού στρώματος. Επομένως, το ιδιωτικό κλειδί W για κρυπτογράφηση αποτελείται στην πραγματικότητα από όλες τις παραμέτρους κάθε συνελικτικού επιπέδου και ορίζεται ως εξής:

$$W = consist[W_1, W_2, \ldots, W_n, \ldots] \quad (6)$$

Κατά την εκπαίδευση του δικτύου κρυπτογράφησης, το ιδιωτικό κλειδί για την κρυπτογράφηση ενημερώνεται συνεχώς και βελτιώνεται με διαφορετικές εικόνες εισόδου μέσω της διαδικασίας εκπαίδευσης διάδοσης προς τα εμπρός. Η αντίθετη απώλεια L_{gan} υπολογίζεται για να μετρήσει τη διαφορά μεταξύ του προβλεπόμενου αποτελέσματος και του στόχου στους "Κρυφούς Παράγοντες", καθοδηγώντας έτσι το δίκτυο να εκπαιδεύσει και να ενημερώσει το ιδιωτικό κλειδί για κρυπτογράφηση.

Εκτός από τη διάδοση προς τα εμπρός, ο αλγόριθμος ανάστροφης διάδοσης (BP) χρησιμοποιείται επίσης για να μεταβιβάσει την απώλεια ολόκληρου του δικτύου πίσω στα συνελικτικά επίπεδα. Στην πραγματικότητα πρόκειται για μια κλίση κατάβασης, η οποία μπορεί να ενημερώσει περαιτέρω τις παραμέτρους σε κάθε επίπεδο για να επιτύχει καλύτερη απόδοση. Η βαθμιδωτή κάθοδος μπορεί να περιγραφεί ως εξής:

$$\begin{aligned}
\theta_j =& \theta_j - \alpha \vee J(\theta) = \theta_j - \alpha \frac{\delta}{\theta_j} J(\theta) \\
=& \theta_j - \alpha \frac{\delta}{\theta_j} \frac{1}{2m} \sum_{i=1}^{m} (h_\theta(x^i) - y^i)^2 \\
=& \theta_j - \alpha \frac{1}{2m} \sum_{i=1}^{m} 2 \frac{\delta}{\theta_j} (h_\theta(x^i) - y^i)(\frac{\delta}{\theta_j}(h_\theta(x^i) - y^i)) \\
=& \theta_j - \alpha \frac{1}{m} \sum_{i=1}^{m} (h_\theta(x^i) - y^i)(\sum_{i=0}^{n} \frac{\delta}{\theta_i} \theta_i x_i - \frac{\delta}{\theta_i} y^i)
\end{aligned} \quad (7)$$

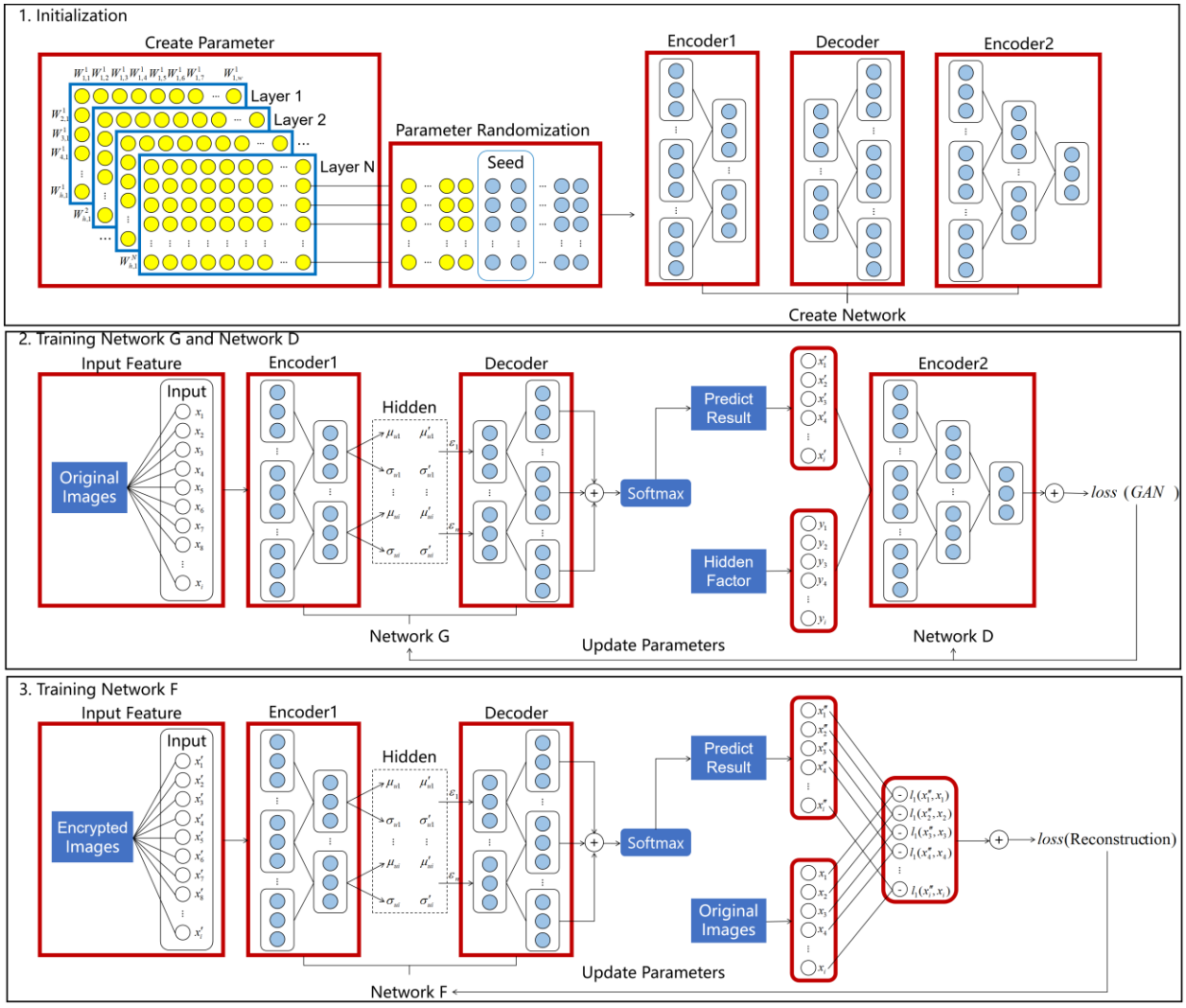
όπου θ_j είναι η τιμή της παραμέτρου θ στην j^{th} περίοδο εκπαίδευσης. Το α είναι ο ρυθμός εκμάθησης και V J(θ) σημαίνει τη διαβάθμιση που επιστρέφει στο στρώμα συνέλιξης θ στην j^{th} περίοδο εκπαίδευσης.

Η διαδικασία δημιουργίας του ιδιωτικού κλειδιού για αποκρυπτογράφηση είναι παρόμοια με τη διαδικασία δημιουργίας του κλειδιού απορρήτου για κρυπτογράφηση, με τη διαφορά ότι η αρχική είσοδος του δικτύου αποκρυπτογράφησης είναι το προβλεπόμενο αποτέλεσμα του δικτύου κρυπτογράφησης. Επιπλέον, η απώλεια δικτύου αποκρυπτογράφησης είναι η απώλεια ανακατασκευής, η οποία δίνεται στην Εξ. (8).

$$\begin{aligned}
L_{reconstruction} =& E_{x \sim p_{data(x)}} \|F(P(X)) - O(X)\|_1 \\
=& E_{x \sim p_{data(x)}} \sum_{i=1}^{n} |F(P(x_i)) - O(x_i)|
\end{aligned} \quad (8)$$

όπου F() είναι το δίκτυο αποκρυπτογράφησης, P(x) είναι το pixel x στην προβλεπόμενη εικόνα και O(x) είναι η αντίστοιχη θέση pixel x στην αρχική εικόνα. Το δίκτυο κρυπτογράφησης G και το δίκτυο αποκρυπτογράφησης F εκπαιδεύονται με εναλλακτικό τρόπο. Όταν η απώλεια γίνει σταθερή, μπορούν

να ληφθούν οι τελικές παράμετροι (κλειδιά απορρήτου) για το δίκτυο κρυπτογράφησης και αποκρυπτογράφησης. Η πλήρης διαδικασία δημιουργίας κλειδιού απορρήτου παρουσιάζεται στην εικόνα 24.



Εικόνα 24: Διαδικασία δημιουργίας κλειδιού απορρήτου[39].

Μετά την απόκτηση του κλειδιού, η ιατρική εικόνα του ασθενούς μπορεί να κρυπτογραφηθεί από το δίκτυο κρυπτογράφησης G και στη συνέχεια να αποκρυπτογραφηθεί από το δίκτυο αποκρυπτογράφησης F. Ο προτεινόμενος αλγόριθμος κρυπτογράφησης/αποκρυπτογράφησης ιατρικής εικόνας δίνεται παρακάτω.

Algorithm 1 Image Encryption/Decryption.

Initialization: Digitize the 255×255 image into a 255×255 matrix X_*^0.And then enter it into our 21-layer(L_c) encryption/decryption model.

1: **while** L< L_c **do**
2: **for all** element (X_1^L, X_2^L,...) in matrix X^L **do**
3: Each pre-trained 3×3 convolution kernel W_*^L in L^{th} layer sequentially traverses the image matrix and multiplies it with the corresponding elements of the matrix($W_*^L \times X_*^L$).
4: Add the obtained nine $W_* X_*$ to get a new predicted value X_*^{L+1} in (L+1)th.
5: Collect all X^{L+1} and combine them into a new matrix to form the next-level feature matrix.
6: **end for**;
7: $L = L + 1$;
8: **end while**

Output: Convert the last layer of matrix X^{L_c} into an image to get the final encrypted/decrypted image.

Δεδομένου ότι το μοντέλο GAN είναι εξαιρετικά μη γραμμικό και τυχαία αρχικοποιημένο, και οι παράμετροι του δικτύου εκμάθησης μπορεί να είναι εντελώς διαφορετικές σε διαφορετικούς χρόνους εκπαίδευσης. Με άλλα λόγια, το δίκτυο GAN είναι ασταθές, κάτι που είναι η αδυναμία του όταν χρησιμοποιείται για εργασίες όρασης υπολογιστή. Ωστόσο, αυτή η αστάθεια έχει πλεονεκτήματα για την κρυπτογραφία. Με τη χρήση αυτής της αστάθειας, η προτεινόμενη μέθοδος κρυπτογράφησης που βασίζεται σε βαθιά μάθηση μπορεί να θεωρηθεί ως μέθοδος One-Time Pad (OTP). Συγκεκριμένα, οι παράμετροι του δικτύου κρυπτογράφησης είναι τελείως διαφορετικές μετά την εκπαίδευση του δικτύου σε διαφορετικούς χρόνους. Συνολικά, λόγω του βάθους και της πολύπλοκης δομής του δικτύου κρυπτογράφησης εκμάθησης, το προτεινόμενο πλαίσιο είναι με υψηλότερη ασφάλεια.

4.3 Δίκτυο εξόρυξης ROI σε περιβάλλοντα κρυπτογραφημένου κειμένου

Αν και διάφορες μέθοδοι έχουν επιτύχει καλή απόδοση στην προστασία του απορρήτου της εικόνας, εξακολουθεί να αποτελεί πρόκληση η άμεση απόκτηση αποτελεσματικών πληροφοριών σε ένα περιβάλλον κρυπτογραφημένου κειμένου, π.χ. εξαγωγή του επιθυμητού ROI από την κρυπτογραφημένη ιατρική εικόνα. Στο DeepEDN, προτείνεται ένα δίκτυο εξόρυξης ROI για να τμηματοποιήσει την περιοχή ενδιαφέροντος από την κρυπτογραφημένη ιατρική εικόνα. Προκειμένου να εξαχθούν χρήσιμα χαρακτηριστικά λεπτομέρειας σε ένα περιβάλλον κρυπτογραφημένου κειμένου, υιοθετείται μια βαθύτερη δομή δικτύου για την εκμάθηση σημασιολογικών χαρακτηριστικών για την ακριβή τμηματοποίηση του συγκεκριμένου στόχου. Η κρυπτογραφημένη εικόνα εισόδου θα υποβληθεί σε επεξεργασία με 5 μπλοκ και κάθε μπλοκ έχει μια συνέλιξη προς τα κάτω δειγματοληψία. Στο πρώτο μπλοκ, καθώς το μέγεθος του συνελικτικού πυρήνα έχει οριστεί σε 3 x 3, κάθε λειτουργία συνέλιξης μπορεί να μάθει τις τοπικές πληροφορίες από την εικόνα εισόδου. Καθώς αυξάνεται το βάθος του δικτύου, μπορούν να ληφθούν πιο αφηρημένες σημασιολογικές πληροφορίες.

Τέλος, συνδυάζοντας τα αποτελέσματα εξόδου από κάθε επίπεδο συνέλιξης, μπορούν να επιτευχθούν τα τελικά αποτελέσματα πρόβλεψης.

Κάθε μπλοκ στο ResNet-50 έχει δύο υπομπλοκ. Το ένα είναι το μπλοκ ταυτότητας (ID) στο οποίο ο διασκελισμός κάθε επιπέδου συνέλιξης είναι 1. Το μπλοκ ταυτότητας χρησιμοποιείται κυρίως για την εξαγωγή αφηρημένων χαρακτηριστικών μέσω συνέλιξης πολλαπλών επιπέδων. Επειδή οι διαστάσεις της εισόδου και της εξόδου είναι ίδιες, αυτοί οι χάρτες χαρακτηριστικών μπορούν να συνδεθούν σειριακά. Το άλλο βασικό μπλοκ είναι το Conv Block όπου οι διαστάσεις της εισόδου και της εξόδου είναι διαφορετικές και χρησιμοποιείται για την αλλαγή της διάστασης του διανύσματος χαρακτηριστικών και για την αλλαγή μεγέθους του μεγέθους χαρακτηριστικών μέσω ενός γραμμωτού συνελικτικού επιπέδου. Το νευρωνικό δίκτυο που βασίζεται στο CNN μετατρέπει συνήθως την εικόνα σε έναν μικρό χάρτη χαρακτηριστικών με πολλά κανάλια. Ωστόσο, αυξάνοντας τα επίπεδα δικτύου, θα υπάρχει ένας τεράστιος αριθμός καναλιών και παραμέτρων εξόδου, με αποτέλεσμα αυξημένη υπολογιστική πολυπλοκότητα και μειωμένη απόδοση δικτύου. Επομένως, είναι απαραίτητο να μειωθεί η διάσταση του αποκλεισμού μετατροπής πριν από την επεξεργασία με το μπλοκ ταυτότητας.

Στο DeepEDN, το προτεινόμενο δίκτυο εξόρυξης ROI χρησιμοποιείται για την υλοποίηση της εργασίας τμηματοποίησης ιατρικής εικόνας στο περιβάλλον κρυπτογραφημένου κειμένου. Η κατάτμηση ιατρικής εικόνας είναι ένα βασικό βήμα στην ανάλυση ιατρικής εικόνας. Σκοπός του είναι να εξάγει χρήσιμα χαρακτηριστικά και να τμηματοποιήσει τα ενδιαφέροντα αντικείμενα των γιατρών. Τα αποτελέσματα κατάτμησης μπορούν να παρέχουν μια αξιόπιστη βάση για κλινική διάγνωση και παθολογική έρευνα. Κατά την εκπαίδευση του δικτύου εξόρυξης ROI, η κρυπτογραφημένη ιατρική εικόνα χρησιμοποιείται αρχικά ως είσοδος του δικτύου. Στη συνέχεια, υιοθετούνται οι ετικέτες τμηματοποίησης σε επίπεδο pixel στην αντίστοιχη ιατρική εικόνα για την επίβλεψη της εκπαιδευτικής διαδικασίας. Τέλος, οι παράμετροι του μοντέλου ενημερώνονται με το μέσο τετραγωνικό σφάλμα (MSE). Η συνάρτηση απώλειας αυτού του μοντέλου τμηματοποίησης περιγράφεται ως εξής:

$$L_S = \frac{1}{N}\sum_{i=0}^{N}(g_i - p_i)^2 \qquad (9)$$

όπου το g_i αντιπροσωπεύει την τιμή του i^{th} pixel στην ετικέτα και το p_i είναι η προβλεπόμενη τιμή του i^{th} pixel στο προβλεπόμενο αποτέλεσμα. Το N αντιπροσωπεύει τον συνολικό αριθμό pixel σε αυτήν την εικόνα. Το τελικό αποτέλεσμα εκπαίδευσης είναι ένας διαχωριστής υψηλής ποιότητας που μπορεί να τμηματοποιήσει τις ιατρικές εικόνες χωρίς αποκρυπτογράφηση.

Η χρήση του δικτύου εξόρυξης ROI είναι μεγάλης σημασίας για την ασφάλεια ιατρικής εικόνας. Μπορεί να εφαρμόσει την εξόρυξη δεδομένων σε ένα μη αξιόπιστο περιβάλλον για την ασφαλή εξαγωγή συγκεκριμένων αντικειμένων, κάτι που είναι επίσης ευεργετικό για την προστασία του απορρήτου του ασθενούς. Αυτό το δίκτυο μπορεί να βελτιώσει περαιτέρω την ασφάλεια της ανάλυσης ιατρικών εικόνων και μπορεί να χρησιμοποιηθεί ευρέως σε πολλές ιατρικές εφαρμογές.

4.4 Μοντέλο αντιπάλου

Στο DeepEDN, οι πιο σημαντικοί παράγοντες της διαδικασίας δημιουργίας κλειδιών περιλαμβάνουν τη δομή του μοντέλου και τους επιλεγμένους κρυφούς παράγοντες. Εάν η δομή του δικτύου ή οι κρυφοί παράγοντες διαρρεύσουν, ο εισβολέας μπορεί να εκπαιδεύσει ένα παρόμοιο δίκτυο κρυπτογράφησης μιμούμενος τη διαδικασία δημιουργίας ιδιωτικού κλειδιού έτσι ώστε να σπάσει την εικόνα κρυπτογραφημένου κειμένου. Αυτό το είδος επίθεσης ονομάζεται επίθεση μίμησης μάθησης. Παρακάτω προτείνονται τρία πιθανά μοντέλα αντιπάλου για μίμηση μαθησιακής επίθεσης: η διαρροή

κρυφών παραγόντων, η διαρροή αρχιτεκτονικής δικτύου και ο συνδυασμός των κρυφών παραγόντων και της διαρροής αρχιτεκτονικής δικτύου.

Η διαρροή κρυφών παραγόντων σημαίνει ότι ο εισβολέας γνωρίζει τους κρυφούς παράγοντες που χρησιμοποιούνται για την κρυπτογράφηση και προσπαθεί να χρησιμοποιήσει τους ίδιους κρυφούς παράγοντες για να εκπαιδεύσει το επιτιθέμενο δίκτυο με πολλές διαφορετικές αρχιτεκτονικές δικτύου για την αποκρυπτογράφηση της εικόνας κρυπτογραφημένου κειμένου. Υπάρχουν δύο δίκτυα κρυπτογράφησης και αποκρυπτογράφησης με διαφορετικές δομές δικτύου. Το δίκτυο κρυπτογράφησης/αποκρυπτογράφησης Α και το δίκτυο κρυπτογράφησης/αποκρυπτογράφησης Β. Αυτά τα δύο δίκτυα κρυπτογράφησης και αποκρυπτογράφησης εκπαιδεύονται με τον ίδιο παράγοντα απόκρυψης. Εάν το δίκτυο αποκρυπτογράφησης Β είναι σε θέση να ανακτήσει την εικόνα που έχει κρυπτογραφηθεί από το δίκτυο κρυπτογράφησης Α, αυτό σημαίνει ότι ο εισβολέας μπορεί να σπάσει το κλειδί ασφαλείας με απομίμηση εκμάθησης επίθεσης.

Η διαρροή αρχιτεκτονικής δικτύου προϋποθέτει ότι διαρρέει μόνο η αρχιτεκτονική του δικτύου κρυπτογράφησης και αποκρυπτογράφησης και οι κρυφοί παράγοντες παραμένουν εμπιστευτικοί. Σε αυτό το μοντέλο αντιπάλου, ο εισβολέας μπορεί να αποκρυπτογραφήσει την κρυπτογραφημένη εικόνα εκπαιδεύοντας την ίδια δομή δικτύου χωρίς να γνωρίζει τους κρυφούς παράγοντες. Ο εισβολέας μπορεί να χρησιμοποιήσει διαφορετικούς κρυφούς παράγοντες για να εκπαιδεύσει την ίδια δομή δικτύου για την κατασκευή διαφορετικών δικτύων αποκρυπτογράφησης. Εάν ο εισβολέας είναι σε θέση να ανακτήσει την κρυπτογραφημένη εικόνα κρυπτογραφημένου κειμένου, η επίθεση είναι επιτυχής.

Το ισχυρότερο μοντέλο αντιπάλου είναι ο συνδυασμός διαρροής της αρχιτεκτονικής του δικτύου και των κρυφών παραγόντων. Σε ένα τέτοιο σενάριο, ο εισβολέας μπορεί να εκπαιδεύσει το δίκτυο με την ίδια δομή δικτύου και κρυφό παράγοντα που υιοθετείται για την εκπαίδευση του δικτύου κρυπτογράφησης/αποκρυπτογράφησης. Για να αποτραπούν τέτοιες επιθέσεις, μετά από κάθε εκπαίδευση του δικτύου, οι παράμετροι του δικτύου κρυπτογράφησης/αποκρυπτογράφησης που αντιπροσωπεύει το πραγματικό ιδιωτικό κλειδί πρέπει να είναι εντελώς διαφορετικές. Πιο συγκεκριμένα ο προτεινόμενος αλγόριθμος κρυπτογράφησης θα πρέπει να είναι παρόμοιος με τον OTP και μπορεί να θεωρηθεί ως ένας χαοτικός αλγόριθμος κρυπτογράφησης.

4.5 Ανάλυση ασφαλείας

4.5.1 Εισαγωγή

Στο DeepEDN, τόσο το δίκτυο κρυπτογράφησης όσο και το δίκτυο αποκρυπτογράφησης κατασκευάζονται με 24 επίπεδα και ο αριθμός των παραμέτρων για κάθε δίκτυο είναι 2.757.936. Οι ρητές προδιαγραφές του δικτύου παρουσιάζονται στην εικόνα 25. Για το δίκτυο εξόρυξης ROI, υιοθετείται μια βαθύτερη αρχιτεκτονική resnet-50. Η δομή του δικτύου εξόρυξης ROI δίνεται στην εικόνα 26. Το σύνολο δεδομένων είναι οι ακτινογραφίες θώρακος. Αυτό το σύνολο δεδομένων παρέχεται από την Εθνική Βιβλιοθήκη Ιατρικής των ΗΠΑ για την προώθηση της έρευνας στη διάγνωση πνευμονικών παθήσεων με τη βοήθεια υπολογιστή. Επικεντρώνεται επίσης στην πνευμονική φυματίωση (ΤΒ). Όλες οι ακτινογραφίες ελήφθησαν από το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών στις Η.Π.Α. και το Νοσοκομείο No. 3 του Λαού Shenzhen στην Κίνα. Τα σύνολα δεδομένων περιέχουν φυσιολογικές, και μη, ακτινογραφίες θώρακος με εκδηλώσεις φυματίωσης και αντίστοιχες μετρήσεις ακτινολόγου. Η

προτεινόμενη μέθοδος εκτελείται στην κάρτα γραφικών Nvidia GTX 2080Ti. Κατά την εκπαίδευση του δικτύου, χρειάζονται περίπου 10 λεπτά για κάθε εποχή (epoch) του μοντέλου.

Convolution Layer Name	Number	Size	Input Channels	Output Channels	Parameters	Total Parameters
Down Convolution1	1	7×7	3	32	4704	4704
Down Convolution2	1	3×3	32	64	18432	23136
Down Convolution3	1	3×3	64	128	73728	95864
Residual Blocks	18	3×3	128	128	2564208	2661072
Up Convolution1	1	3×3	128	64	73728	2734800
Up Convolution2	1	3×3	64	32	18432	2753232
Up Convolution3	1	7×7	32	3	4704	2757936

Εικόνα 25: Δομή κρυπτογραφημένου και αποκρυπτογραφημένου δικτύου[39].

Convolution Layer Name	Number	Size	Input Channels	Output Channels	Parameters	Total Parameters
Block 1	2	7×7	3	64	4704	4704
Block 2	3	3×3	64	256	18432	23136
Block 3	12	3×3	256	512	73728	95864
Block 4	18	3×3	512	1024	2564208	2661072
Block 5	1	3×3	1024	2048	73728	2734800

Εικόνα 26: Δομή δικτύου εξόρυξης ROI[39].

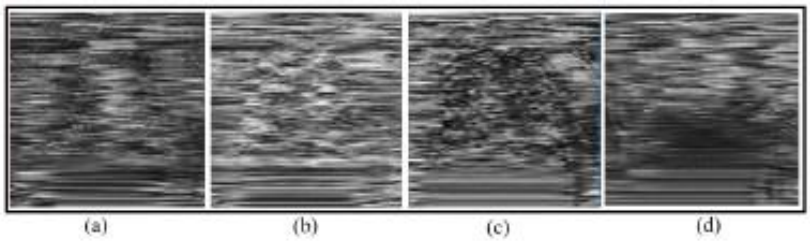
4.5.2 Ανάλυση ασφάλειας κλειδιού

Το ιδανικό σχήμα κρυπτογράφησης έχει τα ακόλουθα χαρακτηριστικά: 1) ο χώρος του κλειδιού θα πρέπει να είναι αρκετά μεγάλος ώστε να μπορεί να αντισταθεί αποτελεσματικά στην εξαντλητική επίθεση υπό την προϋπόθεση της υπάρχουσας υπολογιστικής ισχύος. 2) το κλειδί που δημιουργείται για κάθε φορά θα πρέπει να είναι διαφορετικό, δηλαδή, η δημιουργία κλειδιού πρέπει να είναι ομοιόμορφη τυχαία. και 3) η κρυπτογραφημένη εικόνα πρέπει να είναι πολύ ευαίσθητη στο κλειδί. Η ασφάλεια του κλειδιού θα αναλυθεί από αυτά τα τρία χαρακτηριστικά παρακάτω.

1) Ανάλυση χώρου κλειδιού: Το μέγεθος του χώρου κλειδιού καθορίζει τη δυσκολία που αντιμετωπίζει ένας εισβολέας χρησιμοποιώντας μια εξαντλητική επίθεση. Σε αυτή την εργασία, ο βασικός χώρος του προτεινόμενου αλγόριθμου κρυπτογράφησης είναι ο αριθμός των παραμέτρων για το δίκτυο βαθιάς μάθησης, με συνολικά 2.757.936 παραμέτρους στα πειράματα. Κάθε παράμετρος ή κλειδί είναι ένας αριθμός κινητής υποδιαστολής μεταξύ 0 και 1, ο οποίος είναι 32 bit στον υπολογιστή και μπορεί να εκφραστεί ως δεκαδικός αριθμός με 10 σημαντικά ψηφία. Επομένως, ο χώρος κλειδιού του μοντέλου κρυπτογράφησης μπορεί να εκφραστεί ως το $(2^{32})^{2757936}$. Γίνεται πολύ δύσκολο για τους εισβολείς να σπάσουν το σύστημα και το προτεινόμενο σχήμα μπορεί να αντισταθεί αποτελεσματικά στις επιθέσεις.

2) Ανάλυση τυχαιότητας κλειδιού: Το δίκτυο κρυπτογράφησης εκπαιδεύεται τέσσερις φορές με τις ίδιες ρυθμίσεις. Αντίστοιχα, οι παράμετροι αυτών των τεσσάρων δικτύων υιοθετούνται ως κλειδιά κρυπτογράφησης, δηλ. Κλειδί Α, Κλειδί Β, Κλειδί Γ και Κλειδί Δ, αντίστοιχα. Η ίδια εικόνα κρυπτογραφείται με αυτά τα τέσσερα κλειδιά και οι κρυπτογραφημένες εικόνες φαίνονται στην εικόνα 38. Η εικόνα 27(a), η εικόνα 27(b), η εικόνα 27(c) και η εικόνα 27(d) είναι τα αποτελέσματα που προέκυψαν με την κρυπτογράφηση της ίδιας αρχικής εικόνας από τέσσερα δίκτυα. Είναι σαφές ότι αυτές οι τέσσερις εικόνες είναι διαφορετικές. Η ομοιότητα μεταξύ αυτών των τεσσάρων κρυπτογραφημένων εικόνων (SSIM) υπολογίζεται και το αποτέλεσμα βρίσκεται στην

εικόνα 28. Ο δείκτης SSIM μεταξύ διαφορετικών εικόνων είναι ως επί το πλείστον χαμηλότερος από 0,1, γεγονός που δείχνει ότι η ομοιότητα μεταξύ διαφορετικών εικόνων είναι πολύ χαμηλή.



Εικόνα 27: Αποτελέσματα κρυπτογράφησης εικόνας[39].

Image	A	B	C	D
A	1	0.07	0.11	0.09
B	0.07	1	0.08	0.04
C	0.11	0.08	1	0.05
D	0.09	0.04	0.05	1

Εικόνα 28: SSIM μεταξύ 2 κρυπτογραφημένων εικόνων[39].

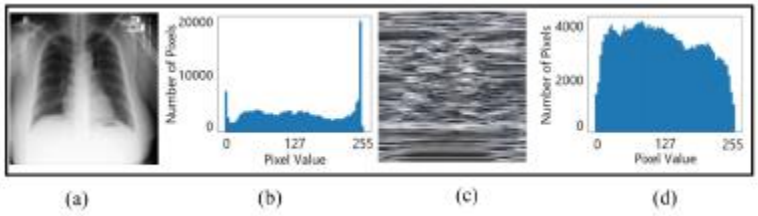
Σύμφωνα με το πείραμα, μπορεί να βρεθεί ότι εφόσον οι παράμετροι του νευρωνικού δικτύου αρχικοποιούνται τυχαία, τα ιδιωτικά κλειδιά για το δίκτυο κρυπτογράφησης ιατρικής εικόνας είναι εντελώς διαφορετικά μετά από κάθε εκπαίδευση. Αυτή η διαφορά έχει ως αποτέλεσμα διαφορετικές κρυπτογραφημένες εικόνες που υποβάλλονται σε επεξεργασία με διαφορετικά δίκτυα κρυπτογράφησης. Η ιδέα πίσω από αυτό είναι ότι η εκπαίδευση του δικτύου βαθιάς μάθησης δεν είναι σταθερή. Διαφορετικές αρχικοποιημένες παράμετροι μπορούν να οδηγήσουν σε δραματική διαφορά στις τελικές παραμέτρους σε διαφορετικές προπονήσεις. Μπορεί να αποδειχθεί ότι η προτεινόμενη μέθοδος είναι παρόμοια με την OTP και μπορεί να θεωρηθεί ως ένας τύπος μεθόδου OTP.

3) Ανάλυση ευαισθησίας κλειδιού: Σε αντίθεση με τους παραδοσιακούς αλγόριθμους κρυπτογράφησης, το σφάλμα στα μοντέλα βαθιάς μάθησης θα διαδοθεί μεταξύ των επιπέδων. Στη διαδικασία συνέλιξης, το I^{th} εικονοστοιχείο στον χάρτη χαρακτηριστικών του N^{th} επιπέδου μεταβιβάζεται σε ένα γειτονικό εικονοστοιχείο του (N+1)th στρώματος μέσω ενός πυρήνα συνέλιξης 3 x 3. Όταν ένα σημείο χαρακτηριστικών είναι λανθασμένο, θα μεταβιβαστεί στα 3 x 3 σημεία χαρακτηριστικών στο επόμενο επίπεδο. Καθώς αυξάνεται το βάθος του συνελικτικού δικτύου, το σφάλμα των σημείων χαρακτηριστικών θα αυξάνεται με δύο pixel για κάθε στρώμα. Στη διαδικασία της ανοδικής δειγματοληψίας, αυτό το σφάλμα αυξάνεται εκθετικά με την υπέρθεση της λειτουργίας αποσυνέλιξης. Το πείραμα υποθέτει ότι ο εισβολέας γνωρίζει τα περισσότερα ιδιωτικά κλειδιά. Και μόνο το 5% περίπου των βασικών παραμέτρων τροποποιείται το οποίο θεωρείται ως το άγνωστο μέρος. Στη συνέχεια, η κρυπτογραφημένη εικόνα εισάγεται στο δίκτυο με νέες παραμέτρους και το δίκτυο δεν μπορεί να αποκρυπτογραφήσει την εικόνα κρυπτογραφημένου κειμένου στην αρχική. Αυτό σημαίνει ότι ακόμη και αν αλλάξει μόνο το 5% των παραμέτρων, το ιδιωτικό κλειδί δεν μπορεί να κρυπτογραφήσει ή να

αποκρυπτογραφήσει σωστά την ιατρική εικόνα. Με άλλα λόγια, γίνεται πολύ δύσκολο για τους επιτιθέμενους να μαντέψουν τουλάχιστον το 95% των σωστών βασικών παραμέτρων σε ένα χώρο κλειδιού με $(10^{10})^{2757936}$, ώστε να σπάσουν τον προτεινόμενο αλγόριθμο.

4.5.3 Ανάλυση ασφάλειας κρυπτογραφημένου κειμένου

1) Ανάλυση ιστογράμματος: Για την αξιολόγηση της απόδοσης του προτεινόμενου δικτύου κρυπτογράφησης, η αρχική εικόνα φαίνεται στην εικόνα 29(a) και η κρυπτογραφημένη εικόνα φαίνεται στην εικόνα 29(c). Μέσα από το πείραμα, μπορεί να διαπιστωθεί ότι η κατανομή pixel της αρχικής εικόνας και της κρυπτογραφημένης εικόνας είναι αρκετά διαφορετική. Στην εικόνα 29, το ιστόγραμμα εικονοστοιχείων της αρχικής εικόνας ακτινογραφίας θώρακα έχει συνολικά 57600*(240 * 240) εικονοστοιχεία (εικόνα 29(b)), στα οποία περισσότερα από 30.000 εικονοστοιχεία έχουν τιμή 0, και περισσότερα από 5000 pixel έχουν τιμή 255. Η κατανομή εικονοστοιχείων της αρχικής εικόνας είναι σχετικά συγκεντρωμένη. Ωστόσο, η κατανομή των κρυπτογραφημένων ιατρικών εικόνων (εικόνα 29(d)) είναι πιο ομοιόμορφη, κάτι που είναι χρήσιμο για τον μετριασμό της στατιστικής ανάλυσης.



Εικόνα 29: Κατανομή pixel της αρχικής εικόνας και της κρυπτογραφημένης εικόνας[39].

2) Ανάλυση εντροπίας: Η εντροπία πληροφοριών της κρυπτογραφημένης εικόνας θεωρείται ως αποτελεσματική ποσοτική μέτρηση για αλγόριθμους έναντι στατιστικών επιθέσεων. Η εντροπία πληροφοριών εικόνας αντιπροσωπεύει το στατιστικό χαρακτηριστικό της κατανομής της κλίμακας του γκρι της εικόνας. Σε μια ιδανική περίπτωση, η κρυπτογραφημένη εικόνα θα πρέπει να είναι παρόμοια με τον τυχαίο θόρυβο, η κατανομή της κλίμακας του γκρι τείνει να είναι ομοιόμορφη και η αναμενόμενη τιμή θα πρέπει να είναι 8. Ο τύπος εντροπίας πληροφοριών ορίζεται ως εξής:

$$Entropy = -\sum_{l=0}^{N} p(l) log_2(p(l)) \qquad (10)$$

όπου N είναι ο αριθμός των επιπέδων του γκρι της τιμής του εικονοστοιχείου και p(l) είναι η πιθανότητα να εμφανιστεί η τιμή του εικονοστοιχείου l. Η μέτρηση της εντροπίας υπολογίζεται στην κρυπτογραφημένη ιατρική εικόνα και τα αποτελέσματα δίνονται στην εικόνα 30. Είναι σαφές ότι η εικόνα που κρυπτογραφείται με την προτεινόμενη μέθοδο είναι κοντά στην ιδανική τιμή του 8 στην εντροπία πληροφοριών. Τα πειράματα δείχνουν ότι οι εικόνες που κρυπτογραφούνται με την προτεινόμενη μέθοδο έχουν την ικανότητα να αντιστέκονται στις στατιστικές επιθέσεις.

Image Id	1	2	3	4	5
Entropy	7.96	7.96	7.95	7.94	7.95
Image Id	**6**	**7**	**8**	**9**	**10**
Entropy	7.97	7.95	7.96	7.96	7.95

Εικόνα 30: Αξιολόγηση του αποτελέσματος εντροπίας του δικτύου[39].

4.5.4 Ανάλυση ασφάλειας κάτω από διαφορετικά μοντέλα αντιπάλου

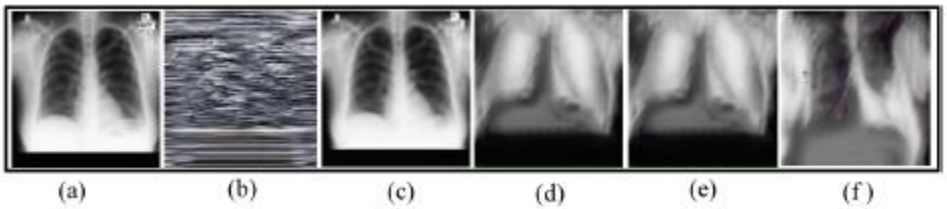
Τα πειράματα διεξάγονται για να επιβεβαιώσουν εάν ένας εισβολέας μπορεί να δημιουργήσει ένα κλειδί σε τρία διαφορετικά μοντέλα αντιπάλου.

1) «Διαρροή κρυφών παραγόντων: Σε αυτό το πείραμα εξετάζονται τέσσερις διαφορετικές δομές δικτύου, δηλαδή το δίκτυο Α, το δίκτυο Β, το δίκτυο Γ και το δίκτυο Δ. Οι συνθήκες εκπαίδευσης διατηρούνται ίδιες. Η δομή δικτύου αυτών των τεσσάρων δικτύων φαίνεται στην εικόνα 31 και ο αριθμός αντιπροσωπεύει τον αριθμό των επιπέδων σε κάθε επίπεδο συνέλιξης.

Convolution Layer	Net. A	Net. B	Net. C	Net. D
Down Convolution1	1	1	1	1
Down Convolution2	1	1	1	1
Down Convolution3	1	1	1	1
Residual Blocks	18	15	12	9
Up Convolution1	1	1	1	1
Up Convolution2	1	1	1	1
Up Convolution3	1	1	1	1

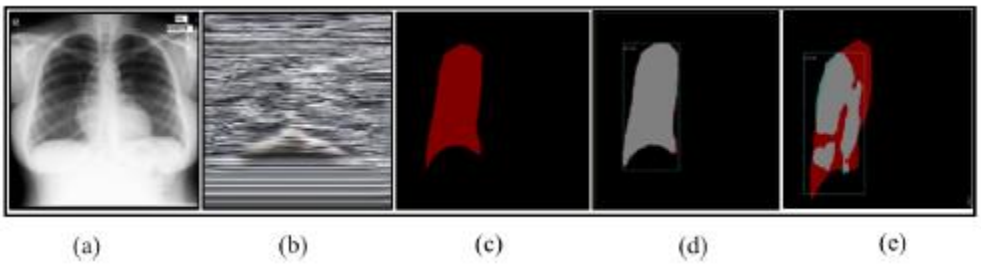
Εικόνα 31: Μοντέλο δικτύου διαφορετικών αρχιτεκτονικών[39].

Η αρχική εικόνα κρυπτογραφείται χρησιμοποιώντας το εκπαιδευμένο δίκτυο Α. Η εικόνα κρυπτογραφημένου κειμένου στη συνέχεια αποκρυπτογραφείται από το δίκτυο αποκρυπτογράφησης που λαμβάνεται από το δίκτυο Α, το δίκτυο Β, το δίκτυο C και το δίκτυο D αντίστοιχα για την επαναφορά της αρχικής εικόνας. Όπως φαίνεται στην εικόνα 32, η αρχική εικόνα (εικ. 32(a)) κρυπτογραφημένη από το δίκτυο Α (η κρυπτογραφημένη εικόνα φαίνεται στην εικόνα 32(b)), μπορεί να αποκρυπτογραφηθεί σωστά μόνο από το δίκτυο αποκρυπτογράφησης Α όπως φαίνεται στην εικόνα 32 (c). Ενώ η εικόνα που αποκρυπτογραφείται από το δίκτυο Β, το δίκτυο C και το δίκτυο D είναι οπτικά μη αναγνωρίσιμη και το αποτέλεσμα φαίνεται στην εικόνα 32(d), 32(e), 32(f), αντίστοιχα. Τα πειράματα δείχνουν ότι ακόμα κι αν ο εισβολέας γνωρίζει τους κρυφούς παράγοντες, το «δίκτυο επίθεσης» που έχει εκπαιδευτεί με διαφορετική δομή δικτύου εξακολουθεί να μην μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση της εικόνας κρυπτογραφημένου κειμένου.



Εικόνα 32: Η απόδοση αποκρυπτογράφησης για διαφορετικά δίκτυα[39].

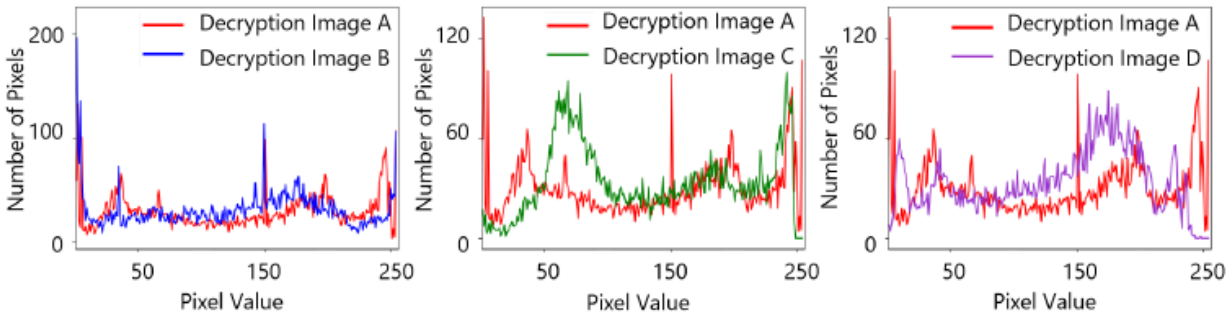
2) Διαρροή αρχιτεκτονικής δικτύου: Σε αυτό το πείραμα, υιοθετούνται διαφορετικοί κρυφοί παράγοντες για την εκπαίδευση του δικτύου κρυπτογράφησης με την ίδια δομή δικτύου. Όλες οι συνθήκες προπόνησης διατηρούνται ίδιες. Όπως φαίνεται στην εικόνα 33(a) και στην εικόνα 33 (b), δύο διαφορετικές εικόνες τομέα ("Κρυφοί Παράγοντες Α" και "Κρυφοί Παράγοντες Β") επιλέγονται ως κρυφοί παράγοντες για την εκπαίδευση του δικτύου με την ίδια αρχιτεκτονική. Στην εικόνα 33(c) είναι η αρχική εικόνα, η εικόνα 33(d) είναι η εικόνα που δημιουργείται από το κρυπτογραφημένο δίκτυο το οποίο εκπαιδεύεται από τους "Κρυφούς Παράγοντες Α" και η εικόνα 33(e) παρουσιάζει το αποτέλεσμα της αποκρυπτογράφησης εικόνας κρυπτογραφημένου κειμένου μέσω το δίκτυο αποκρυπτογράφησης εκπαιδευμένο με «Κρυφούς Παράγοντες Β». Από το πείραμα, μπορεί να βρεθεί ότι η εικόνα που δημιουργείται από το κρυπτογραφημένο δίκτυο που εκπαιδεύεται από τους "Κρυφούς Παράγοντες Α" δεν μπορεί να αποκρυπτογραφηθεί από το δίκτυο που εκπαιδεύεται από τους "Κρυφούς Παράγοντες Β". Επομένως, μπορεί να αποδειχθεί ότι το «δίκτυο επίθεσης» με την ίδια αρχιτεκτονική που εκπαιδεύεται από διαφορετικούς κρυφούς παράγοντες, δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση της εικόνας. Δηλαδή, ακόμα κι αν οι εισβολείς αποκτήσουν την αρχιτεκτονική δικτύου, δεν μπορούν να εκπαιδεύσουν το δίκτυο αποκρυπτογράφησης για την αποκρυπτογράφηση της κρυπτογραφημένης εικόνας χωρίς να γνωρίζουν τους κρυφούς παράγοντες.



Εικόνα 33: Η αμοιβαία απόδοση αποκρυπτογράφησης μεταξύ δικτύων υπό εκπαίδευση διαφορετικών κρυφών παραγόντων[39].

3) Συνδυασμός κρυφών παραγόντων και διαρροής αρχιτεκτονικής δικτύου: Σε αυτό το πείραμα, το δίκτυο εκπαιδεύεται τέσσερις φορές κάτω από τους ίδιους κρυφούς παράγοντες και συνθήκες εκπαίδευσης για να πάρει τα δίκτυα A, B, C και D, αντίστοιχα. Το πείραμα αξιολογεί την απόδοση αποκρυπτογράφησης για αυτά τα τέσσερα δίκτυα στην ίδια εικόνα κρυπτογραφημένου κειμένου για να επαληθεύσει εάν οι παράμετροι που δημιουργούνται για κάθε δίκτυο είναι διαφορετικές. Όπως φαίνεται στην εικόνα 34, η κατανομή της γκρι τιμής της εικόνας που αποκρυπτογραφείται από το κλειδί αποκρυπτογράφησης B, το κλειδί αποκρυπτογράφησης C και το κλειδί αποκρυπτογράφησης D είναι εντελώς διαφορετική από την εικόνα που αποκρυπτογραφείται από το κλειδί αποκρυπτογράφησης A. Μπορεί να διαπιστωθεί σαφώς ότι υπό την ίδια συνθήκη εκπαίδευσης, η κρυπτογραφημένη ιατρική εικόνα που είναι κρυπτογραφημένη από ένα δίκτυο, δεν μπορεί να αποκρυπτογραφηθεί υιοθετώντας τις παραμέτρους σε άλλο δίκτυο. Ακόμα κι αν οι παράμετροι του μοντέλου εκπαιδεύονται με την ίδια αρχιτεκτονική δικτύου και τους ίδιους κρυφούς παράγοντες, δεν μπορούν να χρησιμοποιηθούν για την αποκρυπτογράφηση της εικόνας μεταξύ τους. Τα πειράματα δείχνουν ότι ακόμη και αν διαρρεύσει τόσο η αρχιτεκτονική του δικτύου όσο και οι κρυφοί παράγοντες και η εκπαίδευση του δικτύου υπό τις ίδιες

συνθήκες εκπαίδευσης, οι παράμετροι κάθε δικτύου είναι εντελώς διαφορετικές, δηλαδή τα κλειδιά ασφαλείας είναι διαφορετικά.



Εικόνα 34: Η απόδοση αποκρυπτογράφησης για αυτά τα τέσσερα δίκτυα στην ίδια εικόνα κρυπτογραφημένου κειμένου[39].

Μπορεί να αποδειχθεί ότι το DeepEDN είναι ασφαλές ακόμα κι αν αποκαλυφθεί η αρχιτεκτονική του δικτύου και οι κρυφοί παράγοντες.

4.5.5 Ανάλυση ασφάλειας κάτω από διαφορετικά μοντέλα επίθεσης

1) Επίθεση μόνο κρυπτογραφημένου κειμένου: Σε αυτόν τον τύπο επίθεσης, ο εισβολέας έχει πρόσβαση σε μια συμβολοσειρά κρυπτογραφημένου κειμένου, αλλά δε μπορεί να έχει πρόσβαση στο αντίστοιχο απλό κείμενο.

Στο DeepEDN, ο χώρος κλειδιού του μοντέλου κρυπτογράφησης μπορεί να εκφραστεί ως $(2^{32})^{2757936}$ και είναι πολύ δύσκολο για τον εισβολέα να διασπαστεί. Ταυτόχρονα, το κλειδί απορρήτου που δημιουργείται με πολλαπλές επαναλήψεις και διαχύσεις είναι πολύπλοκο. Επομένως, είναι δύσκολο να σπάσει το κρυπτογραφημένο κείμενο μόνο μέσω επιθέσεων κρυπτογραφημένου κειμένου.

2) Γνωστή επίθεση απλού κειμένου: Η γνωστή επίθεση απλού κειμένου σημαίνει ότι ο εισβολέας γνωρίζει μια συμβολοσειρά απλού κειμένου και το αντίστοιχο κρυπτογραφημένο κείμενο. Ο εισβολέας θα προσπαθήσει να αποκρυπτογραφήσει το υπόλοιπο κρυπτογραφημένο κείμενο χρησιμοποιώντας αυτές τις γνωστές πληροφορίες.

Στις παραδοσιακές μεθόδους διαδοχικών μοτίβων επίσκεψης εικονοστοιχείων, συγκεκριμένοι παράγοντες κρυπτογράφησης, οι οποίοι γενικά ανακτώνται ως ισοδύναμα κλειδιά, μπορούν να χρησιμοποιηθούν για την ανάκτηση των ληφθέντων κρυπτογραφημένων κειμένων. Λαμβάνοντας ως παράδειγμα την κρυπτογράφηση XOR, οι μάσκες που υπολογίζονται απευθείας από το απλό κείμενο και το κρυπτογραφημένο κείμενο επαρκούν για την αποκωδικοποίηση του κρυπτογραφημένου κειμένου. Τυπικά, οι μάσκες αντιστοιχούν διαδοχικά στα απλά εικονοστοιχεία και οι μάσκες που ανακτήθηκαν με επίθεση απλού κειμένου μπορούν να υιοθετηθούν απευθείας για να σπάσουν άλλα κρυπτογραφημένα κείμενα. Ωστόσο, ο προτεινόμενος αλγόριθμος υιοθέτησε τον μη διαδοχικό μηχανισμό κρυπτογράφησης. Χωρίς τη γνώση του μοτίβου επίσκεψης εικονοστοιχείων, το κλειδί απορρήτου δε μπορεί να αποκτηθεί από τον εισβολέα, καθιστώντας έτσι την επίθεση απλού κειμένου ανέφικτη. Ο

προτεινόμενος αλγόριθμος υιοθετεί τις διαδικασίες επανάληψης και διάχυσης για τη δημιουργία του κλειδιού απορρήτου. Αυτού του είδους διαδικασίες μπορούν να βελτιώσουν σημαντικά την απόδοση ασφάλειας και να παρέχουν πρόσθετη άμυνα της κρυπτογράφησης έναντι γνωστών επιθέσεων απλού κειμένου.

3) Επιλεγμένη επίθεση απλού κειμένου: Σε αυτόν τον τύπο επίθεσης, ο εισβολέας μπορεί να έχει πρόσβαση στη συσκευή κρυπτογράφησης, να επιλέξει μια συμβολοσειρά απλού κειμένου και να κατασκευάσει την αντίστοιχη συμβολοσειρά κρυπτογραφημένου κειμένου.

Γενικά, ένας εισβολέας μπορεί να παρατηρήσει την αλλαγή της εικόνας κρυπτογραφημένου κειμένου κάνοντας μικρές αλλαγές στην εικόνα απλού κειμένου, όπως αλλάζοντας την τιμή μόνο ενός εικονοστοιχείου του κρυπτογραφημένου κειμένου, έτσι ώστε να αποκτήσει τη σύνδεση μεταξύ της εικόνας απλού κειμένου και της εικόνας κρυπτογραφημένου κειμένου. Αυτός ο τύπος επίθεσης ονομάζεται διαφορική επίθεση που είναι ένα είδος επιλεγμένης μεθόδου επίθεσης απλού κειμένου. Εάν μια μικρή αλλαγή στην εικόνα απλού κειμένου μπορεί να προκαλέσει τεράστια αλλαγή στην εικόνα κρυπτογραφημένου κειμένου, αυτή η μέθοδος διαφορικής επίθεσης συνήθως αποτυγχάνει να εφαρμοστεί. Υποδεικνύει ότι ο αλγόριθμος κρυπτογράφησης μπορεί να αντισταθεί σε αυτήν την επιλεγμένη μέθοδο επίθεσης απλού κειμένου. Εδώ, ο αριθμός του ρυθμού αλλαγής εικονοστοιχείων (NPCR) υιοθετείται για τη μέτρηση του βαθμού αλλαγής της εικόνας. Το NPCR αναφέρεται στον ρυθμό αλλαγής των εικονοστοιχείων που υποδεικνύει την αναλογία διαφορετικών τιμών εικονοστοιχείων στην ίδια θέση μεταξύ δύο εικόνων απλού κειμένου/κρυπτογραφημένου κειμένου. Ο ορισμός του NPCR είναι ο ακόλουθος:

$$NPCR = \frac{\sum_{i=0}^{W}\sum_{j=0}^{H} D(i,j)}{W \times H} \qquad (11)$$

όπου τα W και H αντιπροσωπεύουν το πλάτος και το ύψος της εικόνας, αντίστοιχα. Τα T1 και T2 αντιπροσωπεύουν μια εικόνα κρυπτογραφημένου κειμένου που λαμβάνεται με την κρυπτογράφηση δύο διαφορετικών εικόνων απλού κειμένου, αντίστοιχα. Αν T1(i , j) = T2(i , j), D(i , j) = 1. Αν T1(i , j) ≠ T2(i , j), D(i , j) = 0. Στο πείραμα, υπάρχει περίπου μόνο 1% διαφορετικά pixel μεταξύ αυτών των δύο εικόνων απλού κειμένου. Τόσο η αρχική εικόνα απλού κειμένου όσο και η εικόνα απλού κειμένου με 1% αλλαγμένη τιμή pixel, εισάγονται στο προτεινόμενο μοντέλο κρυπτογράφησης. Στη συνέχεια, το NPCR χρησιμοποιείται για τη σύγκριση των διαφορών μεταξύ αυτών των δύο κρυπτογραφημένων εικόνων. Η υπολογισμένη μέση τιμή NPCR είναι 94.21%, που σημαίνει ότι οι πληροφορίες της εικόνας απλού κειμένου διαχέονται καλά στην εικόνα κρυπτογραφημένου κειμένου. Δεδομένου ότι το DeepEDN έχει καλή απόδοση διάχυσης και είναι εξαιρετικά ευαίσθητο στο απλό κείμενο, επιτυγχάνει καλή απόδοση για να αντισταθεί στην επιλεγμένη επίθεση απλού κειμένου όπως η διαφορική επίθεση.

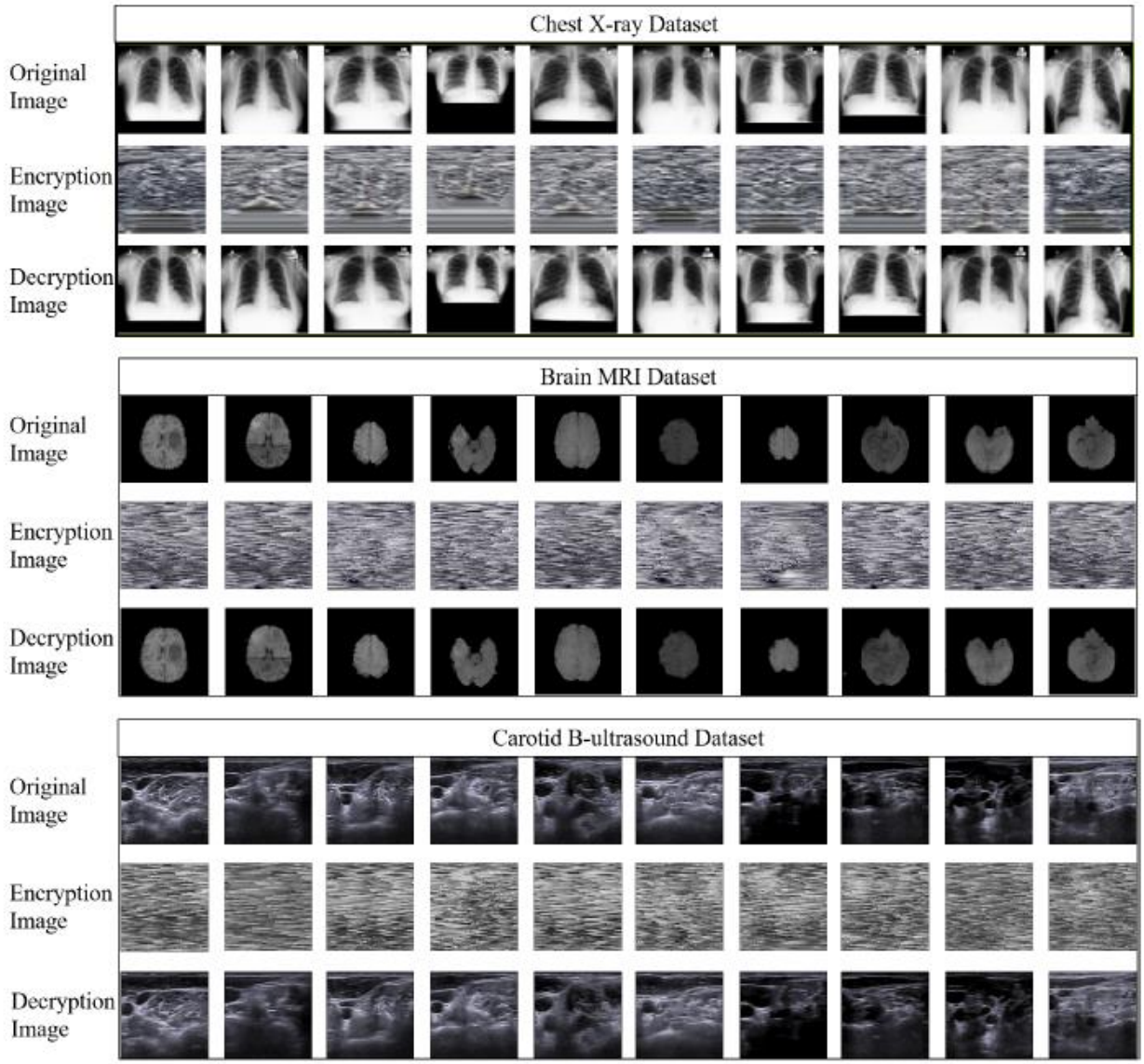
4) Επιλεγμένη επίθεση κρυπτογραφημένου κειμένου: Σε αυτόν τον τύπο επίθεσης, ο εισβολέας μπορεί να έχει πρόσβαση στη συσκευή αποκρυπτογράφησης, να επιλέξει μια συμβολοσειρά κρυπτογραφημένου κειμένου και να κατασκευάσει την αντίστοιχη συμβολοσειρά απλού κειμένου. Δεδομένου ότι η δομή του μοντέλου αποκρυπτογράφησης είναι ακριβώς η ίδια με το μοντέλο κρυπτογράφησης, το πείραμα για την επιλεγμένη επίθεση κρυπτογραφημένου κειμένου είναι παρόμοιο με αυτό στην επιλεγμένη επίθεση απλού κειμένου. Σε αυτό το πείραμα, η είσοδος του δικτύου αποκρυπτογράφησης είναι η εικόνα κρυπτογραφημένου κειμένου και το NPCR χρησιμοποιείται για τον υπολογισμό της διαφοράς μεταξύ δύο αποκρυπτογραφημένων εικόνων. Σύμφωνα με το πείραμα,

διαπιστώθηκε ότι όταν η εικόνα κρυπτογραφημένου κειμένου εισόδου αλλάζει ελαφρώς (μόλις 1% εικονοστοιχεία άλλαξαν), η μέση τιμή NPCR μεταξύ δύο αποκρυπτογραφημένων εικόνων είναι 94.87%. Σημαίνει ότι εάν η εικόνα κρυπτογραφημένου κειμένου εισόδου αλλάξει ελαφρώς, η αποκρυπτογραφημένη εικόνα θα αλλάξει δραματικά. Αυτό δείχνει ότι ο προτεινόμενος αλγόριθμος έχει καλή απόδοση διάχυσης και είναι επίσης πολύ ευαίσθητος στο κρυπτογραφημένο κείμενο. Έτσι είναι αποτελεσματικό να αντιστέκεται στην επιλεγμένη επίθεση κρυπτογραφημένου κειμένου.

4.6 Αποτελέσματα πειράματος

4.6.1 Απόδοση Κρυπτογράφησης και Αποκρυπτογράφησης

Εκτός από το σύνολο δεδομένων ακτίνων Χ θώρακα, πραγματοποιήθηκαν περαιτέρω πειράματα σε εικόνες MRI εγκεφάλου και εικόνες υπερήχων, προκειμένου να αξιολογηθεί η αποτελεσματικότητα της προτεινόμενης μεθόδου μας σε περισσότερες ιατρικές συσκευές απεικόνισης. Οι εικόνες μαγνητικής τομογραφίας εγκεφάλου προέρχονται από το σύνολο δεδομένων BRATS 2015. Αυτό το σύνολο δεδομένων περιλαμβάνει εικόνες εγκεφάλου 274 ασθενών και υπάρχουν τέσσερις διαφορετικοί τρόποι T1, T1c, T2 και Flair για κάθε ασθενή. Και το σύνολο δεδομένων υπερήχων συλλέγεται για την τμηματοποίηση, η οποία αποτελείται από 1055 εικόνες υπερήχων. Όπως φαίνεται στην εικόνα 35, τα αποτελέσματα της προτεινόμενης μεθόδου για κρυπτογράφηση και αποκρυπτογράφηση ιατρικής εικόνας παρουσιάζονται με οπτικό τρόπο. Μπορεί να διαπιστωθεί ότι η προτεινόμενη μέθοδος επιτυγχάνει επίσης καλή απόδοση κρυπτογράφησης σε αυτά τα σύνολα δεδομένων.



Εικόνα 35: Η απόδοση κρυπτογράφησης και αποκρυπτογράφησης της προτεινόμενης μεθόδου[39].

Μπορεί να φανεί ότι η εικόνα κρυπτογραφημένου κειμένου που δημιουργείται από το δίκτυο κρυπτογράφησης G, είναι εντελώς διαφορετική από την αρχική ιατρική εικόνα και οι πληροφορίες παθολογίας δε μπορούν να παρατηρηθούν. Επιπλέον, η εικόνα στην τρίτη σειρά αποκρυπτογραφείται από την κρυπτογραφημένη μέσω του δικτύου αποκρυπτογράφησης F. Επιπλέον, μπορεί να ανακτήσει τις λεπτομερείς πληροφορίες της αρχικής εικόνας και να επαναφέρει στην αρχική. Προκειμένου να αξιολογηθεί η αποτελεσματικότητα του δικτύου αποκρυπτογράφησης, ο λόγος κορυφής σήματος προς θόρυβο (PSNR) και ο δείκτης δομικής ομοιότητας (SSIM) χρησιμοποιούνται ως μετρήσεις αξιολόγησης.

Το ποσοτικό μέτρο του σφάλματος αποκρυπτογράφησης είναι το PSNR, το οποίο βασίζεται στο ριζικό μέσο τετραγωνικό σφάλμα (RMSE) μεταξύ των αποκρυπτογραφημένων δεδομένων και της αληθείας βάσης. Μπορεί να αναπαρασταθεί ως:

$$PSNR = 20log_{10}\frac{255}{RMSE} \qquad (12)$$

Για την περαιτέρω αξιολόγηση της απόδοσης της κρυπτογράφησης και της αποκρυπτογράφησης, η SSIM χρησιμοποιείται ως άλλη μέτρηση.

$$SSIM(x,y) = [l(x,y)]^{\alpha}[c(x,y)]^{\beta}[s(x,y)]^{\gamma} \qquad (13)$$

όπου l(x , y) είναι η σύγκριση φωτεινότητας, c(x , y) είναι η σύγκριση αντίθεσης και s(x , y) είναι η σύγκριση δομής. Όσο πιο κοντά βρίσκεται η SSIM στο 1, τόσο μεγαλύτερη ομοιότητα έχουν οι δύο εικόνες. Και αν αυτή η τιμή πλησιάσει το 0, οι δύο εικόνες είναι εντελώς διαφορετικές. Σε μια ιδανική περίπτωση, η SSIM μεταξύ της κρυπτογραφημένης εικόνας και της αρχικής εικόνας είναι ίση με 0 και η SSIM μεταξύ της αποκρυπτογραφημένης εικόνας και της αρχικής εικόνας είναι ίση με 1. Όπως φαίνεται στη δεύτερη και τρίτη σειρά της εικόνας 36, η SSIM μεταξύ της κρυπτογραφημένης εικόνας και της αρχικής εικόνας είναι κοντά στο 0 και η SSIM μεταξύ της αποκρυπτογραφημένης εικόνας και της αρχικής εικόνας είναι κοντά στο 1.

Image Id	1	2	3	4	5	6	7	8	9	10
SSIM(Encrypted)	0.01	0.02	0.01	0.01	0.02	0.02	0.01	0.02	0.01	0.01
SSIM(Decrypted)	0.93	0.88	0.90	0.94	0.93	0.91	0.91	0.93	0.91	0.89
SSIM(2X)	0.90	0.92	0.90	0.92	0.89	0.91	0.88	0.90	0.91	0.90
PSNR	37.43	35.34	36.01	38.03	35.76	35.87	36.13	37.17	35.88	35.74
PSNR(2X)	35.48	35.74	35.03	35.28	34.87	36.73	34.75	34.61	36.17	34.80

Εικόνα 36: Αξιολόγηση SSIM και PSNR[39].

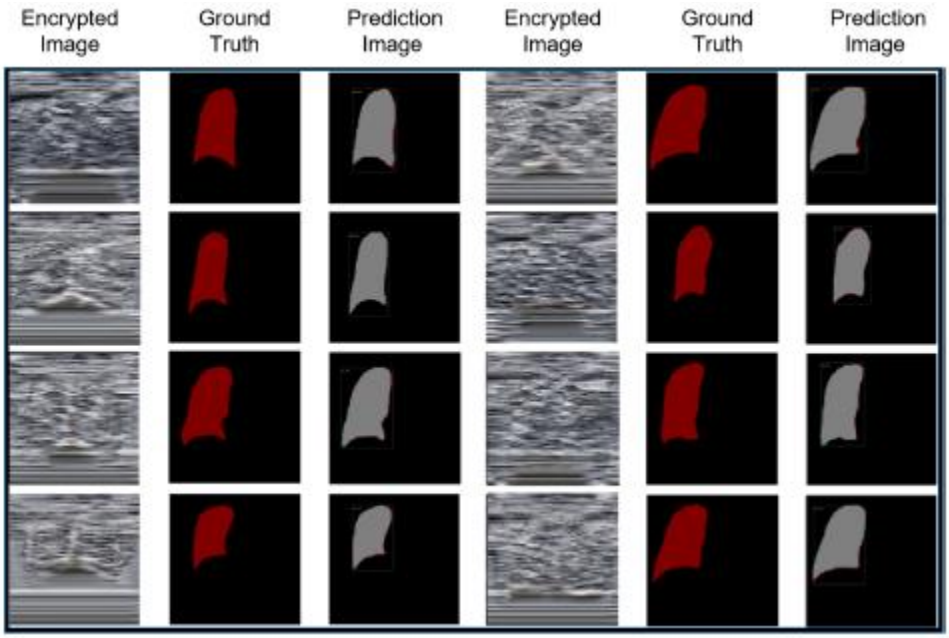
Για τις περισσότερες εργασίες επεξεργασίας ιατρικών εικόνων, η εικόνα μπορεί να συμπιεστεί στο μισό μέγεθος της αρχικής για μείωση της κατανάλωσης αποθήκευσης και δεν επηρεάζει τη διάγνωση του γιατρού. Προκειμένου να διασφαλιστεί ότι η αποκρυπτογραφημένη εικόνα δεν επηρεάζει τη διάγνωση του γιατρού, η απόδοση της ανακατασκευασμένης εικόνας που αποκρυπτογραφείται από το δίκτυο αποκρυπτογράφησης συγκρίνεται επίσης με τη μισή συμπιεσμένη εικόνα. Σύμφωνα με το πείραμα, αποδεικνύεται ότι η απόδοση της ανακατασκευασμένης εικόνας είναι ισοδύναμη με αυτή μέσω της απευθείας συμπίεσης της αρχικής εικόνας στο μισό και στη συνέχεια επαναφοράς της. Στην εικόνα 36, από τη γραμμή 3 έως τη γραμμή 6, το 2X σημαίνει ότι η αρχική εικόνα συμπιέζεται στο μισό και στη συνέχεια αποκαθίσταται. Σε αυτό το επίπεδο, ο άνθρωπος μπορεί να αναγνωρίσει με ακρίβεια τα περιγράμματα των οργάνων του ασθενούς και τις πληροφορίες των οστών από ανακατασκευασμένες εικόνες.

4.6.2 Απόδοση Δικτύου Εξόρυξης ROI

Η άμεση εξαγωγή των χρήσιμων πληροφοριών υπό συνθήκες κρυπτογραφημένου κειμένου είναι μεγάλης σημασίας για την ασφάλεια ιατρικής εικόνας και επίσης για την εξόρυξη δεδομένων με προστασία της ιδιωτικής ζωής. Το προτεινόμενο δίκτυο εξόρυξης ROI μπορεί να τμηματοποιήσει τον ιστό οργάνου που ενδιαφέρει τον ασθενή από την εικόνα κρυπτογραφημένου κειμένου χωρίς πρώτα να αποκρυπτογραφήσει την εικόνα. Το προτεινόμενο δίκτυο έχει τη δυνατότητα να πραγματοποιήσει την εξόρυξη δεδομένων από το περιβάλλον απορρήτου εξάγοντας απευθείας το ROI από την κρυπτογραφημένη εικόνα. Προκειμένου να αξιολογηθεί το προτεινόμενο δίκτυο εξόρυξης απόδοσης επένδυσης (ROI), η γνωστή βαθμολογία μετρικής αξιολόγησης Dice υιοθετείται εδώ και ορίζεται ως:

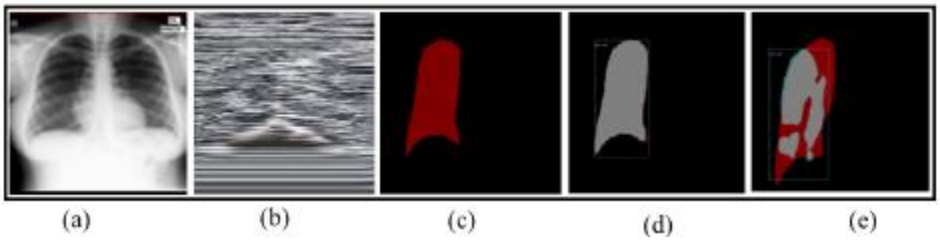
$$Dice(GT, AT) = \frac{GT \cap AT}{(|GT| + |AT|)/2} \qquad (14)$$

Το GT αντιπροσωπεύει την ακριβή αλήθεια και το AT αντιπροσωπεύει τις προβλέψεις του μοντέλου. Η εικόνα 37 δείχνει την απόδοση του προτεινόμενου δικτύου εξόρυξης ROI στον αριστερό πνεύμονα του ασθενούς. Μπορεί να φανεί ξεκάθαρα ότι η πρόβλεψη (γκρι) που λαμβάνεται από το μοντέλο είναι σχεδόν ίδια με την ακριβή αλήθεια (κόκκινα). Επιπλέον, οι αρχικές ιατρικές εικόνες υιοθετούνται επίσης ως δεδομένα πειράματος για την εκπαίδευση του ίδιου δικτύου εξόρυξης ROI, το οποίο χρησιμοποιείται κυρίως ως σύγκριση. Υπό τις ίδιες συνθήκες εκπαίδευσης, το DICE του δικτύου τμηματοποίησης για απλό κείμενο είναι 0,967, ενώ το DICE του δικτύου τμηματοποίησης για την εικόνα κρυπτογραφημένου κειμένου είναι 0,962. Μπορεί να αποδειχθεί ότι το δίκτυο εξόρυξης ROI μπορεί να επιτύχει καλή απόδοση τμηματοποίησης τόσο σε εικόνες απλού κειμένου όσο και σε εικόνες κρυπτογραφημένου κειμένου.



Εικόνα 37: Η απόδοση του δικτύου εξόρυξης ROI[39].

Όπως αναφέρθηκε προηγουμένως, τα κλειδιά απορρήτου του δικτύου είναι τελείως διαφορετικά κατά την εκπαίδευση του δικτύου σε διαφορετικές χρονικές στιγμές, ακόμη και αν όλες οι συνθήκες είναι ίδιες. Επομένως, ο εισβολέας δε μπορεί να αποκτήσει το ίδιο δίκτυο εξόρυξης απόδοσης επένδυσης (ROI) ακόμα κι αν χρησιμοποιεί την ίδια εικόνα κρυπτογραφημένου κειμένου για εκπαίδευση. Το πείραμα μπορεί να βρεθεί στην εικόνα 38. Σε αυτό το πείραμα, η εικόνα 38 (a) είναι η αρχική εικόνα και η εικόνα 38 (b) είναι η εικόνα κρυπτογραφημένου κειμένου της εικόνας 38 (a). Η εικόνα 38 (c) είναι η ακριβή αλήθεια για την κατάτμηση του δεξιού πνεύμονα. Η εικόνα 38 (d) είναι το σωστό αποτέλεσμα εξόρυξης τμηματοποιημένο από το δίκτυο εξόρυξης ROI. Η εικόνα 38 (e) είναι το αποτέλεσμα εξαγωγής σφάλματος τμηματοποιημένο από τον εισβολέα.



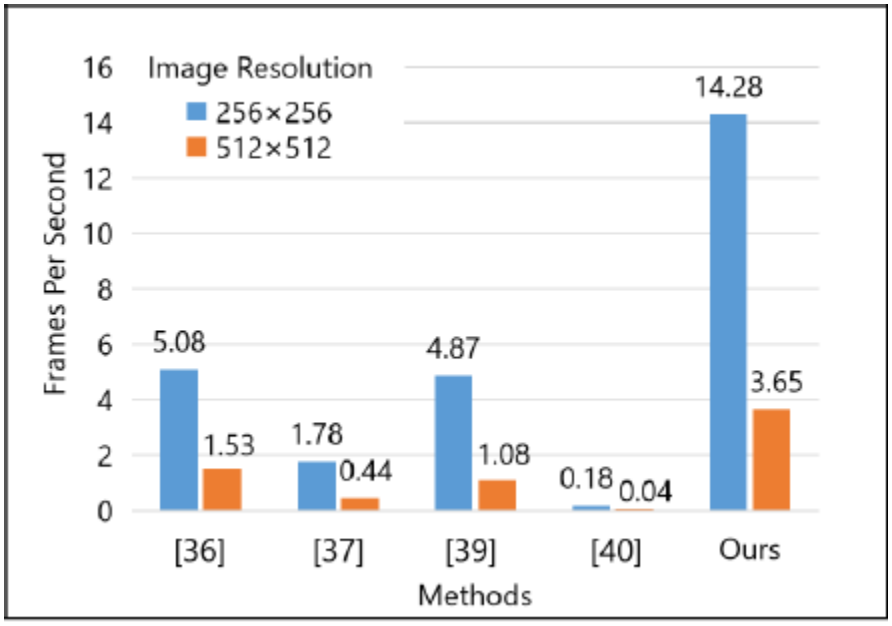
Εικόνα 38: Πείραμα επίθεσης για το προτεινόμενο δίκτυο εξόρυξης ROI[39].

4.6.3 Αποδοτικότητα

Για την αξιολόγηση της αποτελεσματικότητας του προτεινόμενου δικτύου, αξιολογείται η ταχύτητα εκτέλεσης της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης σε ιατρικές εικόνες διαφορετικής ανάλυσης. Για ανάλυση 256x256, το προτεινόμενο δίκτυο μπορεί να κρυπτογραφήσει ή να αποκρυπτογραφήσει 14,28 ιατρικές εικόνες ανά δευτερόλεπτο, ενώ η ταχύτητα είναι 3,65 εικόνες/δευτερόλεπτο για κρυπτογράφηση ή αποκρυπτογράφηση εικόνας ανάλυσης 512x512. Αυτή η ταχύτητα κρυπτογράφησης/αποκρυπτογράφησης μπορεί βασικά να καλύψει την απαίτηση αποτελεσματικότητας στην κλινική πράξη. Επιπλέον, ορισμένοι χαοτικοί αλγόριθμοι κρυπτογράφησης έχουν υιοθετηθεί ως μέθοδος σύγκρισης για την αξιολόγηση της αποτελεσματικότητας. Για παράδειγμα, ο Zhou και άλλοι εισάγουν ένα απλό χαοτικό σύστημα, το οποίο χρησιμοποιεί έναν συνδυασμό δύο υπαρχόντων μονοδιάστατων (1D) χαοτικών χαρτών (seed maps). Ο Liao και άλλοι εισάγουν έναν νέο αλγόριθμο κρυπτογράφησης εικόνας που βασίζεται σε αυτοπροσαρμοζόμενη μετάδοση κυμάτων. Ο Wu και άλλοι εισάγουν ένα χαοτικό σύστημα διακόπτη τροχού για κρυπτογράφηση εικόνας. Μια άλλη προτεινόμενη μέθοδος υιοθετεί αρχικά τον δισδιάστατο λογιστικό χάρτη με περίπλοκες δομές λεκάνης και ελκυστήρες για κρυπτογράφηση εικόνας. Αυτή η μέθοδος μπορεί να κρυπτογραφήσει μια κατανοητή εικόνα σε μια τυχαία εικόνα τόσο από την άποψη του στατιστικού όσο και του ανθρώπινου οπτικού συστήματος.

Η εικόνα 39 δείχνει τη σύγκριση μεταξύ των προαναφερθέντων πέντε αλγορίθμων χαοτικής κρυπτογράφησης και της προτεινόμενης μεθόδου. Το FPS αντιπροσωπεύει τον αριθμό των εικόνων που μπορούν να κρυπτογραφηθούν/αποκρυπτογραφηθούν σε ένα δευτερόλεπτο. Διαπιστώθηκε ότι οι μέθοδοί μας επιτυγχάνουν την ταχύτερη ταχύτητα κρυπτογράφησης τόσο σε εικόνες ανάλυσης 512 x 512 όσο και σε εικόνες ανάλυσης 256 x 256. Αν και ο αριθμός των κλειδιών στη μέθοδό μας είναι μεγαλύτερος

από τον αριθμό των κλειδιών που χρησιμοποιούνται σε χαοτικές μεθόδους κρυπτογράφησης, ο χρόνος επεξεργασίας της μεθόδου μας εξακολουθεί να είναι με υψηλότερη απόδοση.



Εικόνα 39: Η σύγκριση αποτελεσματικότητας μεταξύ της μεθόδου μας και άλλων υπαρχουσών μεθόδων[39].

Σε σύγκριση με τον κρυπτογραφημένο τμήμα(block), το μήκος του κρυπτογραφημένου κειμένου που έχει κρυπτογραφηθεί με την προτεινόμενη μέθοδο μας είναι ίσο με το απλό κείμενο. Αλλά σε ορισμένα κρυπτογραφημένα τμήματα, το μήκος του κρυπτογραφημένου κειμένου είναι μεγαλύτερο από το μήκος του απλού κειμένου, γεγονός που προκαλεί επιβάρυνση αποθήκευσης. Επιπλέον, αξιολογήσαμε την αποτελεσματικότητα των κρυπτογραφημένων τμημάτων σε ανάλυση 512 x 512, όπου το DES κρυπτογραφεί μια εικόνα σε 0,79 δευτερόλεπτα και το AES κρυπτογραφεί μια εικόνα σε 0,54 δευτερόλεπτα. Όπως φαίνεται από την εικόνα 39, η μέθοδός μας διαρκεί μόνο 0,27 δευτερόλεπτα για κάθε εικόνα ανάλυσης 512 x 512. Δείχνει ότι η προτεινόμενη μέθοδος είναι με υψηλή απόδοση[39].

5. Εναρμόνιση προσωπικών δεδομένων με το γενικό κανονισμό προσωπικών δεδομένων (GDPR)

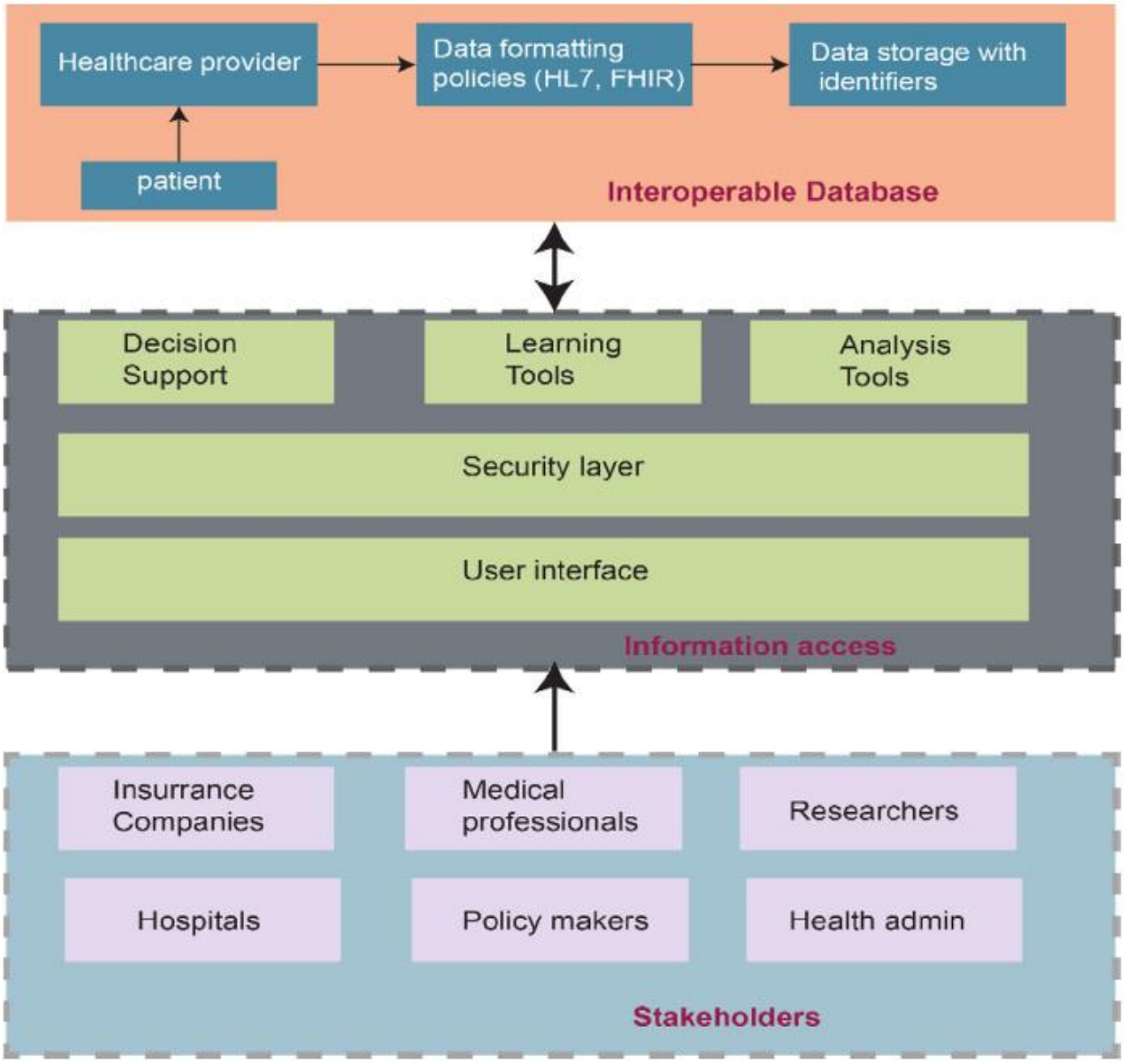
5.1 Εισαγωγή

Το Ευρωπαϊκό Κοινοβούλιο ψήφισε τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) τον Μάιο του 2016. Ο GDPR τέθηκε σε ισχύ και αντικατέστησε την οδηγία για την Προστασία Δεδομένων 95/46/ΕΚ (εφεξής DIR95) τον Μάιο του 2018. Έχει σκοπό να βελτιώσει το απόρρητο των δεδομένων και να διευκολύνει το έργο των οργανισμών και των εταιρειών μέσω των διευκρινισμένων κανόνων του, των πιο συγκεκριμένων απαιτήσεων και ακόμη και των άμεσων οδηγιών για την εφαρμογή των διατάξεων. Από την άλλη πλευρά, οι νέες υποχρεώσεις του GDPR επιφέρουν σημαντικές αλλαγές στην εφαρμογή της προστασίας της ιδιωτικής ζωής των εταιρειών. Όλες οι εταιρείες που χειρίζονται προσωπικά δεδομένα κατοίκων της ΕΕ ή παρακολουθούν τη συμπεριφορά των υποκειμένων των δεδομένων εντός της ΕΕ, ανεξάρτητα από το πού βρίσκονται, θα διέπονται από τον GDPR. Αυτό υποδηλώνει ότι εταιρείες εκτός ΕΕ και διεθνείς θα πρέπει να συμμορφωθούν τόσο με την εθνική τους νομοθεσία όσο και με τον GDPR. Από την υιοθέτησή του το 1995, το DIR95 είναι το κεντρικό νομοθετικό μέσο προστασίας προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση (ΕΕ). Ο GDPR βρίσκεται υπό ανάπτυξη από το 2009 και η Ευρωπαϊκή Επιτροπή δημοσίευσε επίσημα πρόταση για τη μεταρρύθμιση της προστασίας δεδομένων στις αρχές του 2012 (ντε Χερτ και Παπακωνσταντίνου, 2016). Το 2018, ο GDPR τέθηκε τελικά σε ισχύ μετά από αυτή τη νομοθετική διαδικασία πολλαπλών φάσεων. Ο GDPR στοχεύει να βελτιώσει το επίπεδο προστασίας και εναρμόνισης των προσωπικών δεδομένων σε ολόκληρη την ΕΕ καθώς το DIR95 δεν πληροί πλέον τις απαιτήσεις απορρήτου του σημερινού ψηφιακού περιβάλλοντος.

5.2 Προσωπικά αρχεία υγείας, παγκόσμια πολιτική και ανασκόπηση κανονισμού GDPR

Οι κλινικές πληροφορίες παράγονται από τις τρέχουσες κλινικές δοκιμές ασθενών. Αυτές οι υπηρεσίες συνήθως εκτελούνται σε παθολογικά εργαστήρια, νοσοκομεία ή κλινικές μέσω διαφορετικών εξετάσεων και ακτινολογικών εκθέσεων. Αυτά τα όργανα παράγουν μεγάλες ποσότητες κλινικών δεδομένων παγκοσμίως και ο όγκος τους αυξάνεται εκθετικά. Τα κλινικά δεδομένα προβλέπεται να αυξηθούν απότομα [40]. Κλινικά δεδομένα που παράγονται σε τακτικές κλινικές δοκιμές αποθηκεύονται σε έντυπη μορφή στις περισσότερες αναπτυσσόμενες χώρες. Οι επαγγελματίες υγείας ακολουθούν αυτή τη στρατηγική, καθώς είναι εύκολη και δε χρειάζεται προηγμένες γνώσεις ΤΠΕ. Ωστόσο, η διατήρηση των πληροφοριών ασθενών που βασίζονται σε έντυπη μορφή δεν είναι χρήσιμη για τους ασθενείς και δε μπορεί να προσφέρει αξιόπιστη και έγκαιρη υγειονομική περίθαλψη.

Οι οργανισμοί υγείας χρησιμοποιούν διαδικασίες για την ψηφιοποίηση των ιατρικών αρχείων για την επίλυση των προβλημάτων που περιγράφονται παραπάνω. Επί του παρόντος, τα κλινικά δεδομένα ασθενών διατηρούνται ως EHR. Το EHR είναι ηλεκτρονικά αρχεία υγείας ασθενών που περιέχουν πλήρεις πληροφορίες ασθενών και αρχεία θεραπείας σε ένα σχέδιο (που περιγράφεται στην εικόνα 40) το οποίο μπορεί εύκολα να μοιραστεί ή να ανακτηθεί από διάφορους παρόχους υγειονομικής περίθαλψης μέσω άλλων συνδεδεμένων τοποθεσιών όπως απαιτείται.



Εικόνα 40: Μια εννοιολογική επισκόπηση των συστημάτων HER [59].

Η χρήση EHR έχει πολλά πλεονεκτήματα σε σχέση με το συμβατικό μηχανισμό που βασίζεται σε χαρτί. Για παράδειγμα:

1. Το EHR μπορεί να αποθηκεύσει δομημένο, κρυπτογραφημένο και λεπτομερές ιστορικό υγείας του ασθενούς.

2. Το EHR παρέχει μια βάση για το σύστημα υποστήριξης ιατρικών αποφάσεων (DSS) για την τακτική παρακολούθηση της κατάστασης της υγείας του ασθενούς και τη βελτίωση της ποιότητας της υγειονομικής περίθαλψης. Το DSS διευκολύνει τη λήψη αποφάσεων αυτοματοποιώντας την ανάλυση δεδομένων.

3. Το EHR λειτουργεί ως κεντρικός αποθηκευτικός χώρος για την παρακολούθηση και τη χρέωση ασθενών, διατηρώντας την ποιότητα και διευκολύνοντας τη λήψη αποφάσεων που είναι ευαίσθητες στον ασθενή.

4. Τα αρχεία που είναι αποθηκευμένα σε EHR μπορούν να χρησιμοποιηθούν εύκολα από διαφορετικά συνεργαζόμενα μέρη σε διαφορετικές τοποθεσίες. Ως εκ τούτου, είναι δυνατή η παροχή δεδομένων σε ενδιαφερόμενους γιατρούς σε πολλές τοποθεσίες για την παροχή αποτελεσματικών και ποιοτικών εγκαταστάσεων υγείας.

5. Το EHR μειώνει τον κίνδυνο σφαλμάτων επεξεργασίας ιατρικών δεδομένων αποθηκεύοντας πλήρη ιατρικά αρχεία, μειώνοντας έτσι το κόστος υγειονομικής περίθαλψης.

Με τα πλεονεκτήματα της χρήσης του EHR στην υγειονομική περίθαλψη, εντοπίζονται επίσης διάφορα συγκεκριμένα ζητήματα. Το πιο σημαντικό ζήτημα είναι η ασφάλεια των αρχείων και το απόρρητο του ασθενούς. Εάν η πρόσβαση στα δεδομένα EHR γίνεται με κάποιο τρόπο με μη εξουσιοδοτημένο τρόπο, μπορεί να γίνει επικίνδυνη κακή χρήση τους, όπως αλλαγές φαρμάκων ή θεραπείας μη ασφαλείς για τους ασθενείς και μπορεί να οδηγήσει σε σοβαρά προβλήματα ή να προκαλέσει θάνατο ασθενούς [41]. Ως εκ τούτου, είναι απαραίτητο να προστατεύονται οι πληροφορίες των ασθενών από τα ανεπιθύμητα χέρια λάθος ανθρώπων στην κεντρική βάση δεδομένων. Οι πληροφορίες ασθενών μπορεί επίσης να κλαπούν όταν μεταδίδονται μέσω του δικτύου σε πολλά άλλα δίκτυα ή αποθηκεύονται σε κατανεμημένους διακομιστές cloud [42,43,44].

Το EHR μπορεί επίσης να χρησιμοποιηθεί για διάφορους δευτερεύοντες σκοπούς, όπως κλινικές μελέτες, ασφάλιση υγείας, κλινικός έλεγχος και κρατική υποστήριξη λήψης αποφάσεων. Επιπλέον, μπορεί να χρησιμοποιηθεί για εκστρατείες πρόληψης, ελέγχους εθνικών προτύπων, εθνικές προβλέψεις, μελλοντικό σχεδιασμό υπηρεσιών, κατανομή πόρων κ.λ.π. Οι ασθενείς δεν επιτρέπεται να αποκαλύπτουν τις πληροφορίες για την υγεία τους προς όφελος παρά να μοιράζονται τα προσωπικά τους δεδομένα υγείας για θεραπεία και όχι άλλες δευτερεύουσες χρήσεις. Η χρήση προσωπικών δεδομένων ασθενών για διάφορες δευτερεύουσες δραστηριότητες χωρίς τη συγκατάθεσή τους θα διαταράξει σημαντικά το απόρρητο του ασθενούς. Για την προστασία της ιδιωτικής ζωής του ασθενούς τα διάφορα πρότυπα απορρήτου που ακολουθούνται σε διαφορετικές περιοχές είναι το GDPR στην Ευρώπη [43] και το HIPAA στις Ηνωμένες Πολιτείες. Παρακάτω εξετάζονται τα πρότυπα απορρήτου HIPAA και GDPR και εντοπίζονται προκλήσεις για την παροχή απορρήτου δεδομένων για τις αυξανόμενες πληροφορίες EHR.

Τα δεδομένα EHR πρέπει να μοιράζονται μεταξύ διαφόρων διασυνδεδεμένων τοποθεσιών, όπως ιατρεία, νοσοκομεία, φαρμακεία, διαγνωστικά εργαστήρια κ.λπ., για αποτελεσματική χρήση που φαίνεται στην εικόνα 40. Η κοινή χρήση δεδομένων σε πολλές τοποθεσίες διασφαλίζει ευέλικτη και αποτελεσματική θεραπεία ασθενών με τον εντοπισμό των βασικές ανάγκες όπως φροντίδα, υποστήριξη, ασφάλεια, επικαιρότητα και ανάγκες παρακολούθησης. Υποστηρίζει επαγγελματίες (φυσικούς, νοσηλευτές, κ.λπ.) στη λήψη των σωστών αποφάσεων με βάση τα συμπτώματα [45,46,47]. Η προσβασιμότητα των δεδομένων βελτιώνεται περαιτέρω εάν τα δεδομένα EHR συνδέονται με διαφορετικές κλινικές βάσεις δεδομένων και συστήματα υποστήριξης αποφάσεων (DSS). Τα CDSS είναι μια πλατφόρμα αυτόματης ανάλυσης ιατρικών δεδομένων που συνιστά περισσότερες παρεμβάσεις φροντίδας και δημιουργεί προειδοποιήσεις μέσω ανάλυσης δεδομένων που προβλέπουν μελλοντικές καταστάσεις. Οι γιατροί μπορούν να λάβουν σοφές αποφάσεις εύκολα και εικονικά.

Η κοινή χρήση δεδομένων EHR σε πολλές τοποθεσίες είναι περίπλοκη χωρίς ανταλλαγή πληροφοριών για την υγεία και τα πρότυπα απορρήτου. Οι πάροχοι υγειονομικής περίθαλψης αντιμετώπισαν το ίδιο πρόβλημα κατά την κοινή χρήση δεδομένων EHR και διαφόρων DSS, καθώς δεν υπήρχε πρότυπο για το απόρρητο και την κοινή χρήση πληροφοριών υγείας. Αποτελεί βασικό παράγοντα πίσω από το χαμηλό ποσοστό υιοθέτησης του EHR σε οργανισμούς υγειονομικής περίθαλψης, αν και η εισαγωγή του EHR στην υγειονομική περίθαλψη είναι πολύ επωφελής.

5.3 Επικρατείς κανονισμοί προστασίας δεδομένων και οι προκλήσεις τους

Οι αρχές έχουν επιβάλει κανονισμούς προστασίας δεδομένων σε ορισμένα μέρη του κόσμου για να εξασφαλίσουν προσωπικά αρχεία υγείας από διάφορες απειλές και επιθέσεις κατά της ασφάλειας. Οι πιο διαδεδομένοι κανονισμοί προστασίας δεδομένων είναι ο GDPR [49] και ο HIPAA.

Παρακάτω, εξετάζονται αυτοί οι κανονισμοί, συμπεριλαμβανομένου του τρόπου διατήρησης του απορρήτου των ασθενών και επιβολής της ασφάλειας των δεδομένων. Ο GDPR τέθηκε σε ισχύ σε όλες τις χώρες της Ε.Ε. στις 26 Μαΐου 2018, καταργώντας τους προηγούμενους κανονισμούς της για την προστασία δεδομένων το 1995 [50]. Ο GDPR είναι ένας κανονισμός που έγινε νόμος της Ε.Ε. και έπρεπε να τηρηθεί από όλα τα μέλη της Ε.Ε. . Ο νόμος περιλαμβάνει όλες τις προσωπικές πληροφορίες, συμπεριλαμβανομένων των δεδομένων υγείας, που αποθηκεύονται, ανταλλάσσονται και χρησιμοποιούνται. Ο χειρισμός των δεδομένων υγείας από τους πολίτες της Ε.Ε. είναι πιθανό να κοστίσουν και να ωφελήσουν τους επαγγελματίες υγείας και τους αναλυτές υγείας.

5.3.1 Γενικές διατάξεις του GDPR

Ο GDPR ορίζει τα «προσωπικά δεδομένα» ως «το σύνολο δεδομένων» που περιλαμβάνει όλες τις πληροφορίες για την ταυτοποίηση ενός ατόμου. Θεωρητικά, ο GDPR ισχύει για όλους τους «ελεγκτές» και «υπεύθυνους επεξεργασίας» που ασχολούνται με τα προσωπικά δεδομένα ανεξάρτητα από την τοποθεσία τους [51]. Τα δικαστικά καθήκοντα των υπευθύνων επεξεργασίας και των ελεγκτών είναι παρόμοια, αλλά ο υπεύθυνος επεξεργασίας έχει την κύρια πρόσβαση στα ευαίσθητα υποκείμενα των δεδομένων [50].

Ενώ η επεξεργασία εξαρτάται από τη συγκατάθεση, ο χρήστης θα πρέπει να μπορεί να αποκρύψει τη συγκατάθεσή του ανά πάσα στιγμή και η διαδικασία θα πρέπει να είναι τόσο απλή όσο η παροχή συγκατάθεσης. Οι υπεύθυνοι επεξεργασίας είναι υπεύθυνοι για την απόδειξη της συγκατάθεσής τους. Επίσης, η γονική συναίνεση απαιτείται για ανήλικα άτομα.

Ο GDPR παρέχει στα άτομα πολλά σημαντικά προνόμια, όπως:

- Δικαίωμα γνώσης της συλλογής δεδομένων.
- Δικαίωμα πρόσβασης σε πληροφορίες.
- Σωστή φορητότητα δεδομένων.

- Δικαίωμα αντίρρησης για αποθήκευση.
- Δικαίωμα επίλυσης λανθασμένων δεδομένων.
- Εξαιρετικά αμφιλεγόμενα (ιδιαίτερα στο πλαίσιο του Δικαιώματος στην ελευθερία του λόγου) δικαιώματα να αφαιρούνται όταν τα δεδομένα δεν διατηρούνται πλέον. ΕΕ. Οι Αρχές Προστασίας Δεδομένων μπορούν να επιβάλλουν πρόστιμα στους παραβάτες έως και 4% των ακαθάριστων εσόδων και τα άτομα μπορούν να έχουν ιδιωτικά νομικά δικαιώματα έναντι των υπευθύνων επεξεργασίας και των ελεγκτών.

Εφαρμογή GDPR στην υγειονομική περίθαλψη

Ο GDPR έχει πολλά κριτήρια για δεδομένα υγείας και επιστημονική μελέτη. Συνολικά, η συλλογή, η χρήση και η μετάδοση δεδομένων για υγειονομικούς και επιστημονικούς σκοπούς ρυθμίζονται περισσότερο, ενισχύοντας το συνονθύλευμα κανόνων του DPD. Οι συγκεκριμένοι κανόνες είναι περίπλοκοι και συνήθως πιο επαχθείς από τους προηγούμενους νόμους. Ισχύουν ειδικοί κανόνες για την υγεία και τα προσωπικά γενετικά δεδομένα, που θεωρούνται «ευαίσθητα». Πρέπει να τηρούνται πολλές συγκεκριμένες οδηγίες και προϋποθέσεις πριν από την επεξεργασία οποιασδήποτε τέτοιας πληροφορίας [52]. Ο όρος περιλάμβανε ότι έχει χορηγηθεί «ρητή» συγκατάθεση στο υποκείμενο των δεδομένων εάν:

- Ασφάλιση ενός συνόλου δεδομένων για ασθενείς που δε μπορούν να δώσουν τη συγκατάθεσή τους, όπως η επείγουσα ιατρική κατάσταση ενός αναίσθητου ασθενούς.
- Όταν είναι απαραίτητο να προσφέρουμε υγειονομική περίθαλψη πχ γιατρός να χρειάζεται δεδομένα από άλλο γιατρό ή πάροχο υγειονομικής περίθαλψης.
- Για την αντιμετώπιση των αναγκών υγείας, όπως η προστασία από διασυνοριακές απειλές για την υγεία ή η διατήρηση της ασφάλειας της υγείας.

5.3.2 Νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας (HIPAA)

Γενικές διατάξεις του HIPAA

Ο HIPAA ρυθμίζει τη χρήση και αποκάλυψη των προστατευόμενων πληροφοριών υγείας (PHI) των ΗΠΑ. Ο HIPAA περιγράφει το PHI ως παροχή πληροφοριών σχετικά με την ψυχική ή σωματική υγεία ενός ατόμου. Ο HIPAA αναφέρεται μόνο σε ένα υποσύνολο οργανισμών—σχέδια υγειονομικής περίθαλψης, συστήματα πληρωμών υγειονομικής περίθαλψης (δηλαδή, επιχειρηματικοί συνεργάτες). Ο HIPAA περιλαμβάνει προστατευμένους οργανισμούς και ενώσεις για την παροχή ασφάλειας και απορρήτου στο PHI. Γενικά, οι προστατευμένοι οργανισμοί και οι επιχειρηματικοί συνεργάτες δε μπορούν να αποκαλύψουν ή να χρησιμοποιήσουν PHI χωρίς προηγούμενη έγκριση από τον ασθενή, εκτός εάν υπάρχει εξαίρεση [53]. Ο HIPAA προβλέπει εύλογα ευρείες εξαιρέσεις από αυτόν τον γενικό κανόνα [54].

Εφαρμογή HIPAA στην υγειονομική περίθαλψη

Ο HIPAA ρυθμίζει επίσης εάν θα χρησιμοποιηθεί το PHI για ερευνητικούς σκοπούς. Οι ερευνητές μπορούν να αποκτήσουν, να δημιουργήσουν, να χρησιμοποιήσουν ή να αποκαλύψουν PHI κατά τη διάρκεια της έρευνας. Ωστόσο, οι συνήθως καλυπτόμενοι οργανισμοί έχουν υποκείμενους ερευνητές δεδομένων [55]. Οι καλυπτόμενοι οργανισμοί πρέπει είτε να έχουν την άδεια του ασθενούς να αποκαλύπτουν τέτοιες πληροφορίες για ερευνητική εργασία είτε να έχουν καταγεγραμμένη έγκριση από το Institutional Review Board (IRB) ή το Privacy Board για την αποκάλυψη τέτοιων πληροφοριών χωρίς την άδεια του ασθενή [56] προκειμένου να αποκαλύπτουν τέτοιες πληροφορίες στους ερευνητές.

Δεδομένου ότι η έγκριση από το IRB για εξουσιοδότηση ασθενούς μπορεί να είναι μια περίπλοκη διαδικασία, οι περισσότεροι ερευνητές επιλέγουν την εξουσιοδότηση ασθενών εάν συμφωνούν με τη μελέτη. Οι προστατευόμενοι οργανισμοί μπορούν επίσης να παρέχουν πληροφορίες [57].

5.4 Απαιτήσεις για HIPAA και η λύση συμμόρφωσης GDPR

Η συλλογή και χρήση δεδομένων υγείας μόνο στις ΗΠΑ για ερευνητικούς, ιατρικούς ή άλλους συναφείς σκοπούς παραμένει υπό τον έλεγχο του HIPAA (και σε ορισμένες περιπτώσεις την ισχύουσα πολιτειακή νομοθεσία) και δεν επηρεάζεται από τον GDPR. Ωστόσο, ο GDPR πρέπει να τηρείται σε κάθε «επεξεργασία», όπως συλλογή, εφαρμογή ή διατήρηση προσωπικών πληροφοριών αναγνωρίσιμων για ένα άτομο στην ΕΕ. Ομοίως, οι οντότητες που λαμβάνουν δεδομένα υγείας από άτομα με έδρα την ΕΕ θα πρέπει να πληρούν αυστηρές απαιτήσεις GDPR για οποιονδήποτε λόγο. Οι οργανισμοί που μεταφέρουν δεδομένα που σχετίζονται με την υγεία των ΗΠΑ στην Ευρωπαϊκή Ένωση πρέπει να συμμορφώνονται και με τους δύο κανόνες.

Παρά τους εννοιολογικούς παραλληλισμούς και ορισμένες ομοιότητες — όπως η εξαίρεση των ανώνυμων δεδομένων από το ρεπορτάζ — τα πρότυπα HIPAA και Common Law δεν είναι ισοδύναμα, ούτε με το GDPR. Κατά συνέπεια, κανένας δε θεωρείται ότι συνεργάζεται για τη διασφάλιση της πλήρους συμμόρφωσης με το σύστημα υγειονομικής περίθαλψης. Υπάρχουν μερικές βασικές λειτουργικές διαφορές:

1. Η Επιτροπή Θεσμικής Αναθεώρησης (IRB) δεν εγγυάται ότι έχουν συμμορφωθεί οι διατάξεις συναίνεσης του GDPR. Οι εγκρίσεις IRB πραγματοποιούνται χωριστά. Ωστόσο, οι απαιτήσεις του GDPR σπάνια θα παραιτηθούν εάν η επεξεργασία δεδομένων υγείας βάσει συναίνεσης σε ένα ίδρυμα στην Ε.Ε. ξεκινά με την ανάγκη για τον GDPR και εγγυάται ότι τα αρχεία συναίνεσης κατόπιν ενημέρωσης των ΗΠΑ πληρούν το πρότυπο.
2. Τα δικαιώματα των υποκειμένων των δεδομένων του GDPR της ΕΕ υπερβαίνουν κατά πολύ τα πρότυπα μιας ενημερωμένης συμφωνίας συναίνεσης των ΗΠΑ — για παράδειγμα, δικαιώματα πρόσβασης, διορθώσεων και διαγραφής GDPR. Οργανισμοί που συγκεντρώνουν ή επεξεργάζονται με άλλο τρόπο τα δεδομένα της Ε.Ε. θα πρέπει πρώτα να εξοικειωθούν με αυτά τα δικαιώματα. Και πάλι, η έγκριση και η συμμόρφωση του IRB των ΗΠΑ ενδέχεται να είναι ανεπαρκείς.

3. Ο νόμος GDPR απλοποιήθηκε σχεδόν σε κάθε περίπτωση για τις αγορές one-stop. Επιβάλλει επίσης όρους που δε μπορούν να αγνοηθούν, συμπεριλαμβανομένης της ονομασίας ενός εκπροσώπου στην επιλεγμένη Ε.Ε. αρχή προστασίας δεδομένων της χώρας.
4. Η μεταφορά δεδομένων από τα μέλη της Ε.Ε. στα μέλη που εδρεύουν στις ΗΠΑ είναι συνήθως το πιο περίπλοκο μέρος. Οι κατευθυντήριες γραμμές είναι ακριβείς και συνήθως ασυμβίβαστες, αλλά είναι δυνατό, κυρίως με συναίνεση, επομένως αυτό είναι ένα διαφορετικό πρόβλημα που πρέπει να αντιμετωπιστεί σε κάθε διαδικασία σχεδιασμού έργου διεθνών δεδομένων υγείας.

5.5 Προτεινόμενη λύση συμμόρφωσης HIPAA και GDPR για την υγειονομική περίθαλψη

Ο HIPAA και ο GDPR απαιτούν επίσης αποτελεσματικά τεχνικά μέτρα, δηλαδή ψευδωνυμοποίηση και κρυπτογράφηση, για την ασφάλεια των δεδομένων υγείας. Δεν είναι εύκολο να εφαρμοστούν σωστά και θα απαιτηθούν εκτενείς πόροι ανάπτυξης. Η εικόνα 41 δείχνει τις απαιτήσεις συμμόρφωσης HIPAA και GDPR για την υγειονομική περίθαλψη.

1. Οι τεχνολογικές απαιτήσεις παραμένουν οργανωτική ευθύνη. Απαιτούνται περαιτέρω μέτρα, όπως επαρκής κρυπτογράφηση και αρχεία ελέγχου. Δεν υπάρχει επίπεδο ασφάλειας που πρέπει να προστεθούν στα AWS, Azure κ.λπ. Αυτές οι απαιτήσεις, ωστόσο, είναι δύσκολο να εφαρμοστούν και τελικά απαιτούν μια ομάδα επαγγελματικής ανάπτυξης.
2. Ο πάροχος cloud του οργανισμού διαχειρίζεται συνήθως τείχη προστασίας, συστήματα εξισορρόπησης φορτίου κ.λπ. Επίσης, αυτά θα πρέπει να τοποθετηθούν σωστά.
3. Οι διοικητικές απαιτήσεις μπορούν να κατανεμηθούν στους δικηγόρους. Ωστόσο, δε μπορούν ακόμα να συμπληρώσουν έγγραφα όπως DPIA ή BAA.

5.5.1 Κρυπτογράφηση

Η κρυπτογράφηση δεδομένων προστατεύει τα δεδομένα χρησιμοποιώντας κρυπτογραφία. Υπάρχουν διάφορες μέθοδοι κρυπτογράφησης. Πολλοί πάροχοι cloud παρέχουν επίσης κρυπτογράφηση. Ωστόσο, δεν υπάρχουν αρκετά για τον GDPR ή τον HIPAA. Τα άτομα μπορούν να εμφανίζουν ή να επεξεργάζονται δεδομένα υγείας χρησιμοποιώντας κρυπτογράφηση σε επίπεδο εφαρμογής. Η κρυπτογράφηση από άκρο σε άκρο θα μπορούσε να είναι χρήσιμη για την ασφάλεια των συνομιλιών ιατρού-ασθενούς.

Τα δεδομένα μπορούν να κρυπτογραφηθούν με πολλούς τρόπους, αλλά τρεις προσεγγίσεις είναι κατάλληλες για δεδομένα υγείας. Κανένας από τους παρόχους cloud δεν προσφέρει αυτές τις μεθόδους από προεπιλογή.

1. Κρυπτογράφηση σε επίπεδο βάσης δεδομένων: ολόκληρη η βάση δεδομένων έχει κρυπτογραφηθεί ως ομάδα. Η λύση του δεν είναι πολύ ασφαλής και μπορεί να ανοίξει αμέσως.
2. Κρυπτογράφηση σε επίπεδο εφαρμογής: Κάθε αρχείο ασθενούς κρυπτογραφείται ξεχωριστά. Είναι επίσης μια καλή επιλογή σε σχέση με την κρυπτογράφηση σε επίπεδο βάσης δεδομένων, καθώς κάθε κλειδί ξεκλειδώνει μόνο μία εγγραφή.

3. Κρυπτογράφηση από άκρο σε άκρο: Κρυπτογράφηση E2E. Οι εγγραφές κρυπτογραφούνται στο τέλος της συσκευής χρησιμοποιώντας ιδιωτικά κλειδιά. Είναι μια ασφαλής προσέγγιση εάν δεν χρειάζεστε καν πρόσβαση στις πληροφορίες υποστήριξης.

5.5.2 Ψευδωνυμοποίηση

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, η ψευδωνυμοποίηση είναι η διαδικασία αντικατάστασης όλων των προσωπικών δεδομένων (ή των πληροφοριών προσωπικής ταυτότητας) με τυχαία ψευδώνυμα. Η αντιστοίχιση μεταξύ ψευδωνύμων και δεδομένων πρέπει να αποθηκεύεται με ασφάλεια και χωριστά. Το βασικό πλεονέκτημα της ψευδωνυμοποίησης θα είναι ότι μπορείτε να αποθηκεύσετε τα ευαίσθητα δεδομένα σας (π.χ. δεδομένα υγείας) σε μια εύκολα προσβάσιμη τοποθεσία, ώστε να μπορείτε εύκολα να δημιουργήσετε νέες εφαρμογές χρησιμοποιώντας αυτά τα δεδομένα. Είναι σημαντικό να σημειωθεί ότι ο GDPR θεωρεί τέτοια δεδομένα ως προσωπικά δεδομένα καθώς τα έμμεσα αναγνωριστικά μπορούν να επαναπροσδιορίσουν έναν χρήστη.

Η ψευδωνυμοποίηση μπορεί να χρησιμοποιηθεί όταν αποθηκεύεται με ασφάλεια αλλά εξακολουθεί να είναι διαθέσιμη (π.χ. αναζήτηση). Είναι γνωστή ως ασφαλής τεχνική GDPR και HIPAA.

Η εξήγηση του τρόπου με τον οποίο η ψευδώνυμη εργασία στην υγειονομική περίθαλψη συζητείται παρακάτω.

1. Αρχικός φάκελος υγείας ασθενούς: πλήρη στοιχεία στην αρχική μορφή.
2. Διακεκριμένοι φάκελοι υγείας από προσωπικά δεδομένα: προσωπικές πληροφορίες για κάθε ασθενή εξάγονται από τα αρχεία υγείας του και αποθηκεύονται αλλού.
3. Τυχαία δημιουργία ψευδωνύμων: δημιουργείται ένας μοναδικός κωδικός αναγνώρισης για τη σύνδεση ατόμων.
4. Κρατήστε ένα ψευδώνυμο για κάθε αρχείο υγείας: τα προσωπικά στοιχεία και τα αρχεία υγείας αποθηκεύονται με τον ίδιο κωδικό αναγνώρισης.

5.5.3 Ανωνυμοποίηση

Η ανωνυμοποίηση απαιτεί την πλήρη διαγραφή των προσωπικών δεδομένων και στη συνέχεια τη διαχείριση των υπόλοιπων δεδομένων για τη διαγραφή έμμεσων αναγνωριστικών. Ο στόχος είναι να διασφαλιστεί ότι τα υπόλοιπα δεδομένα δε μπορούν να αναγνωριστούν εκ νέου από ένα άτομο. Η τυπική στρατηγική ανωνυμοποίησης είναι μια γενίκευση, ανατροπή διακοπής, συνάθροιση. Η σωστή ανωνυμοποίηση είναι εξαιρετικά δύσκολη, όπως ανακάλυψε το Netflix στις αρχές του 2008. Το πρόβλημα είναι ότι οι προδιαγραφές διαφέρουν ανάλογα με το πόσο ιδιαίτερα είναι τα δεδομένα. Για παράδειγμα, εάν έχετε μια ομάδα 20 ασθενών, αλλά μόνο ένας είναι άνω των 50, η στρογγυλοποίηση των ηλικιών στον πλησιέστερο ακέραιο αριθμό είναι αναποτελεσματική. Έχει πραγματοποιηθεί σημαντική έρευνα για πρωτοβουλίες για τη διασφάλιση ανώνυμων δεδομένων, π.χ. κ-ανωνυμία.

Εικόνα 41: Απαίτηση συμμόρφωσης HIPAA και GDPR στην υγειονομική περίθαλψη[59].

Δεν υπάρχουν νόμοι περί απορρήτου που να καλύπτουν ανώνυμα δεδομένα και τα αναλυτικά δεδομένα μπορούν να χρησιμοποιηθούν ή να κοινοποιηθούν με άλλους. Αλλά τα προνόμια ανωνυμοποίησης είναι δύσκολα. Τα δικαιώματα ανωνυμοποίησης είναι δύσκολα.

Η εξήγηση του τρόπου λειτουργίας της ανωνυμοποίησης στην υγειονομική περίθαλψη συζητείται παρακάτω.

1. Πολυάριθμα αρχικά αρχεία υγείας: τα αρχικά πλήρη δεδομένα στην αρχική μορφή
2. Πραγματικά κατεστραμμένα προσωπικά αναγνωριστικά: απλά προσωπικά δεδομένα διαγράφονται και δε μπορούν να ανακτηθούν αργότερα.
3. Τα δεδομένα υγείας τροποποιούνται για να αποφευχθεί ο επαναπροσδιορισμός: αυτό μπορεί να επιτευχθεί με πολλούς διαφορετικούς τρόπους, μέσω κάλυψης, τυχαίας δειγματοληψίας, γενίκευσης και προσθήκης θορύβου.
4. Δεδομένα έτοιμα για ανάλυση: τα δεδομένα μπορούν να μελετηθούν ή να μεταδοθούν χωρίς τον κίνδυνο ταυτοποίησης ασθενών.

6. Συμπεράσματα

Στην παρούσα διπλωματική εργασία αναλύσαμε τη διαδικασία, τις μεθόδους της κυβερνοασφάλειας και κυρίως τη χρησιμότητά της στον τομέα της υγειονομικής περίθαλψης μέσα από διάφορες τεχνικές που περιλάμβαναν την ανωνυμοποίηση, την ψευδωνυμοποίηση και την κρυπτογράφηση με τη βοήθεια της βαθιάς μάθησης.

Δεδομένου ότι τα εμπιστευτικά δεδομένα και οι οιονεί αναγνωριστικές τιμές ενδέχεται να διασπείρονται σε όλα τα έγγραφα, η ανωνυμοποίηση δεδομένων κειμένου χρειάζεται περισσότερη έρευνα. Έχει γίνει κάποια εργασία που χρησιμοποιεί την έννοια της μηχανικής μάθησης για την αναγνώριση του ονόματος της νόσου, αλλά εξακολουθεί να απαιτεί μοντέλα πλήρους απόδειξης που εντοπίζουν αποτελεσματικά το οιονεί αναγνωριστικό και το ευαίσθητο χαρακτηριστικό.

Τεχνικές όπως η γενίκευση, η καταστολή, η ανατομοποίηση, η δημιουργία κάδου είναι οι προσεγγίσεις με τις οποίες αυξήθηκε το απόρρητο του χρήστη στα δημοσιευμένα δεδομένα. Γίνεται έρευνα σχετικά με τη χρήση κρυπτογραφικής τεχνικής για την εξόρυξη δεδομένων διατήρησης της ιδιωτικής ζωής. Στο μέλλον, μπορεί να διερευνηθεί αποτελεσματική εφαρμογή κρυπτογραφικών τεχνικών για τη διατήρηση του απορρήτου στα δημοσιευμένα δεδομένα[2].

Η εφαρμογή μεθόδων ψευδωνυμοποίησης αντιμετωπίζει παρουσιαζόμενα ελαττώματα διατηρώντας τη βασική χρησιμότητα δεδομένων που διαφορετικά θα χάνονταν. Στο βαθμό που γνωρίζουμε, η LPL (Layered Privacy Language) είναι η πρώτη γλώσσα απορρήτου που μοντελοποιεί και επιβάλλει μεθόδους ψευδωνυμοποίησης. Η υλοποίηση είναι επί του παρόντος περιορισμένη και βρίσκεται σε εξέλιξη. Ωστόσο, ενδέχεται να προστεθούν διάφορες μέθοδοι ψευδωνυμοποίησης (οι οποίες ακολουθούν την περιγραφόμενη δομή διαμόρφωσης). Για παράδειγμα, οι ασύμμετρες κρυπτογραφικές συναρτήσεις και οι προσεγγίσεις κατακερματισμού χωρίς κλειδί με χρήση αντιστοιχίσεων για επαναπροσδιορισμό είναι κατάλληλες προσθήκες. Η LPL σίγουρα επιτρέπει αυθαίρετους συνδυασμούς ψευδωνυμοποίησης και ανωνυμοποίησης. Ωστόσο, είναι σημαντικό να επιλέξουμε κατάλληλες μεθόδους (ψευδωνυμοποίηση, ανωνυμοποίηση, μοντέλα απορρήτου) με βάση τον επιδιωκόμενο σκοπό, διαφορετικά το απόρρητο μπορεί να διαταραχθεί. Η επιλογή της κατάλληλης αποταυτοποίησης θα πρέπει να εκτελείται από ειδικό, π.χ. εκπαιδευμένο υπεύθυνο προστασίας δεδομένων.

Το απόρρητο είναι ένα αναδυόμενο θέμα που πρέπει να εξεταστεί σε διάφορους τομείς. Στην υγειονομική περίθαλψη είναι ιδιαίτερα απαραίτητο να λαμβάνεται υπόψη το απόρρητο των δεδομένων επειδή τα επεξεργασμένα δεδομένα εμπίπτουν στις ειδικές κατηγορίες δεδομένων. Η LPL σκοπεύει να μοντελοποιήσει πολιτικές απορρήτου για να ενημερώνει τα υποκείμενα των δεδομένων και να επιβάλλει το απόρρητο βάσει σχεδιασμού. Στην LPL, ορίστηκαν και χρησιμοποιήθηκαν αποκλειστικά μοντέλα ανωνυμοποίησης και απορρήτου για αποταυτοποίηση. Ωστόσο, αποδείχθηκε ότι η ψευδωνυμοποίηση είναι απαραίτητη για τα σενάρια υγειονομικής περίθαλψης. Η επέκταση της ψευδωνυμοποίησης της LPL προσφέρει τη δυνατότητα ορισμού μεθόδων ψευδωνυμοποίησης που πρέπει να εφαρμοστούν στο σύνολο δεδομένων. Για παράδειγμα, οι αμφιμονοσήμαντες αντιστοιχίες θα επέτρεπαν μια εξουσιοδοτημένη αποταυτοποίηση, η οποία δεν είναι δυνατή μόνο για τεχνικές ανωνυμοποίησης. Επιπλέον, το tokenization επιτρέπει τη σαφή διάκριση των αρχικών τιμών. Η διαδικασία αποταυτοποίησης βάσει πολιτικής συνδυάζει τα μοντέλα ψευδωνυμοποίησης, ανωνυμοποίησης και απορρήτου ως ολιστική προσέγγιση. Η LPL και το γενικό της πλαίσιο αναπτύσσονται και ερευνώνται συνεχώς. Η αξιολόγηση της διαδικασίας αποταυτοποίησης βάσει πολιτικής που βασίζεται σε πραγματικά

δεδομένα υγειονομικής περίθαλψης είναι ταξινομημένη. Επίσης, η αξιολόγηση της LPL στοχεύει σε άλλους τομείς όπως το IoT, το Cloud και το Mobility. Το ίδιο το πλαίσιο θα πρέπει να επεκταθεί για την εκπλήρωση των δικαιωμάτων του υποκειμένου δεδομένων για την υποστήριξη των υπεύθυνων προστασίας δεδομένων. Αναπτύσσονται κατάλληλες διεπαφές χρήστη για διαφορετικούς τομείς και ομάδες χρηστών (π.χ. ηλικιωμένοι ή παιδιά) για να επιτρέπουν τη συναίνεση που είναι συμβατή με τον GDPR[14].

Η μέθοδος κρυπτογράφησης και αποκρυπτογράφησης ιατρικής εικόνας (δηλαδή DeepEDN) με τη χρήση τεχνικών βαθιάς μάθησης είναι μία από τις πρώτες προσπάθειες υιοθέτησης της έννοιας της «βαθιάς μάθησης» για την κρυπτογράφηση ιατρικής εικόνας. Το δίκτυο Cycle-GAN υιοθετείται ως το δίκτυο εκμάθησης για την κρυπτογράφηση και την αποκρυπτογράφηση της ιατρικής εικόνας. Ένας τομέας στόχος χρησιμοποιείται για να καθοδηγήσει το μοντέλο εκμάθησης στη διαδικασία κρυπτογράφησης. Το δίκτυο ανακατασκευής μπορεί να αποκρυπτογραφήσει την κρυπτογραφημένη εικόνα στην αρχική εικόνα (απλό κείμενο). Επιπλέον, προτείνεται ένα δίκτυο εξόρυξης ROI για την άμεση εξαγωγή του ROI από την κρυπτογραφημένη ιατρική εικόνα, με το οποίο το DeepEDN μπορεί να τμηματοποιήσει το ενδιαφερόμενο όργανο ή ιστό στο περιβάλλον κρυπτογραφημένου κειμένου χωρίς να αποκρυπτογραφήσει την ιατρική εικόνα. Διεξήχθησαν πειράματα στα σύνολα δεδομένων ακτίνων Χ θώρακα και τα αποτελέσματα δείχνουν ότι ο προτεινόμενος αλγόριθμος μπορεί να προστατεύσει την ιατρική εικόνα με υψηλό επίπεδο ασφάλειας και μπορεί να κρυπτογραφήσει/αποκρυπτογραφήσει την εικόνα με πιο αποτελεσματικό τρόπο, σε σύγκριση με την τελευταία λέξη της τεχνολογίας, τις μεθόδους κρυπτογράφησης ιατρικών εικόνων[39].

Τέλος, για την παροχή αναγκών απορρήτου και ασφάλειας, οι κανονισμοί GDPR και HIPAA καθοδηγούν την αρχή, αλλά η εφαρμογή τους σε συστήματα EHR είναι δύσκολη. Παραπάνω έχει εξεταστεί η συμμόρφωση των συστημάτων EHR που βασίζονται σε Blockchain ως προς τη συμμόρφωση με τις απαιτήσεις GDPR και HIPAA. Τα συστήματα EHR που βασίζονται σε blockchain υποστηρίζουν κρυπτογραφημένη, ψευδώνυμη αποθήκευση αρχείων απαραίτητη για τη συμμόρφωση με τον GDPR και το HIPAA. Ως εκ τούτου, έχει αναθεωρηθεί και διαπιστώθηκε ότι αυτά τα συστήματα μπορούν να συμμορφώνονται με τις οδηγίες GDPR και HIPAA εάν ακολουθούν τις περιγραφόμενες φυσικές, τεχνικές και διοικητικές απαιτήσεις[59].

Βιβλιογραφία

[1] Lynne Coventry, Dawn Branley et al, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward”, in: Elsevier Inc, Northumbria University, Newcastle upon Tyne, UK, 2018.

[2] Vartika Puri, Shelly Sachdeva, Parmeet Kaur et al, “Privacy preserving publication of relational and transaction data: Survey on the anonymization of patient data”, in: Elsevier Inc, Department of Computer Science, Jaypee Institute of Information Technology, Noida, India and Department of Computer Science, National Institute of Technology, Delhi, India, 2019.

[3] Xiaojin Zhang, Shuang Ma , Songlin Chenc et al, “Healthcare process modularization using design structure matrix”, in: Elsevier Inc, Office of Clinical Epidemiology, Analytics and Knowledge (OCEAN), Tan Tock Seng Hospital, Singapore, School of Management and Economics, Beijing Institute of Technology, Beijing, China, School of Mechanical & Aerospace Engineering, Nanyang Technological University, Singapore 639798, Singapore, 2019.

[4]. Mrinai M.Dhanvijay, Shailaja C.Patil et al, “Internet of Things: A survey of enabling technologies in healthcare and its applications”, in Elsevier Inc, Department of Technology, Savitribai Phule Pune University, Pune, India, Department of Electronics and Telecommunication Engineering, Jayawant Shikshan Prasarak Mandal's Rajarshi Shahu College of Engineering, Pune, India, 2019.

[5]. R.Z. Arndt, In healthcare, breach dangers come from inside the house, Mod. Healthc. http://www.modernhealthcare.com/article/20180410/NEWS/180419999, 2018.

[6]. E. Bower, How does the general data protection regulation (GDPR) affect GPs? GP Online, https://www.gponline.com/does-general-data-protectionregulation-gdpr-affect-gps/article/1460998 , 2018.

[7]. F. Hassan, J. Domingo-Ferrer, J. Soria-Comas et al, “Anonymization of unstructured data via named-entity recognition”, in: Proceedings of the International Conference on Modeling Decisions for Artificial Intelligence, MDAI, 2018.

[8]. D. Toshniwal et al, “Privacy preserving data mining techniques privacy preserving data mining techniques for hiding sensitive data: A step towards open data”, in: Data Science Landscape, in: Studies in Big Data, vol. 38, Springer, Singapore, 2018.

[9]. Fabian Prasser, Helmut Spengler et al, “Privacy-enhancing ETL-processes for biomedical data”, in Elsevier Inc, Institute of Medical Informatics, Statistics and Epidemiology, University Hospital rechts der Isar, Technical University of Munich, Ismaninger Str. 22, 81675 Munich, Germany, 2019.

[10]. Yan, Y., Herman, E.A. et al, “A weighted K-member clustering algorithm for K-anonymization”, School of Computer and Communication, in: Springer, Lanzhou University of Technology, Lanzhou, 730050, China, Department of Computing, Faculty of Science and Engineering, Macquarie University, Sydney, NSW, 2109, Australia, 2021.

[11]. A. Gerl, N. Bennani, H. Kosch, and L. Brunie, LPL, towards a GDPR-compliant privacy language: formal definition and usage, In: *Transactions on Large-Scale Data-and Knowledge-Centered Systems XXXVII*, Springer, 2018

[12]. A. Gerl, Extending layered privacy language to support privacy icons for a personal privacy policy user interface, In: *Proceedings of the 32nd International BCS Human Computer Interaction Conference*., Belfast, Ireland, 2018

[13]. A. Gerl and D. Pohl, Critical analysis of LPL according to articles 12-14 of the GDPR, In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ACM, Hamburg, Germany, 2018

[14]. Armin Gerl, Felix Bölz, "Layered Privacy Language Pseudonymization Extension for Health Care", in: Pubmed, Chair of Distributed Information Systems, University of Passau, Passau, Bavaria, Germany, 2021.

[15]. Damian Eke, Ida E.J. Aasebø et al, "Pseudonymisation of neuroimages and data protection: Increasing access to data while retaining scientific utility", in: Elsevier Inc, Centre for Computing and Social Responsibility, De Montfort University, Leicester, UK, University of Oslo, Norway et al, 2021.

[16]. Abigail Rai, Samarjeet Borah, " Study of Various Methods for Tokenization", in: Springer, Department of Computer Application, SMIT, Sikkim Manipal Institute of Technology, Sikkim, India, 2020.

[17]. A. Gatouillat, Y. Badr et al, "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," IEEE Internet of Things Journal, 2018.

[18]. N Zhang, P Yang, J Ren, et. Al., "Synergy of big data and 5g wireless networks: opportunities, approaches, and challenges," IEEE Wireless Communications, 2018.

[19]. B. Liu, H. Huang, "Picture archiving and communication systems and electronic medical records for the healthcare enterprise," Biomedical Information Technology, Academic Press, 2020.

[20]. D. Chen, N. Zhang, et al., "Channel precoding based message authentication in wireless networks: Challenges and solutions", IEEE Network, 2018.

[21]. D. Chen, N. Zhang et al, "Physical Layer based Message Authentication with Secure Channel Codes", IEEE Transactions on Dependable and Secure Computing, 2020.

[22]. Natgunanathan, A. Mehmood, et al, "Location Privacy Protection in Smart Health Care System," IEEE Internet of Things Journal, 2019.

[23]. M. Preishuber, T. Hutter, et al, "Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption," IEEE Transactions on Information Forensics and Security, 2018.

[24]. L. Ale, N. Zhang, et. al., "Online Proactive Caching in Mobile Edge Computing Using Bidirectional Deep Recurrent Neural Network", IEEE Internet of Things Journal, 2019.

[25]. H. Chen, Z. Qin, Y. Ding, et.al., “Brain tumor segmentation with deep convolutional symmetric neural network,” Neurocomputing, in: Elsevier Inc, University of Elctronic Science and Technology of China, Chengdu, China, 2019.

[26]. Y. Ding, C. Luo, et.al., “High-order correlation detecting in features for diagnosis of Alzheimer’s disease and mild cognitive impairment,” Biomedical Signal Processing and Control, in: Elsevier Inc, The School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan Province, China, 2019.

[27]. B. Xiao, G. Ou, et.al., “Multi-Focus Image Fusion by Hessian Matrix Based Decomposition,” IEEE Transactions on Multimedia, 2020.

[28]. B. Xiao, K. Wang, et.al., “2D-LBP: An Enhanced Local Binary Feature for Texture Image Classification,” IEEE Transactions on Circuits and Systems for Video Technology, 2019.

[29]. H. Tang, B. Xiao, et al. “Pixel Convolutional Neural Network for Multi-Focus Image Fusion,” Information Sciences, in: Elsevier Inc, Chongqing Key Laboratory of Computational Intelligence, Chongqing University of Posts and Telecommunications, Chongqing 400065, China, 2018.

[30]. B. Xiao et al., “Follow the Sound of Childrens Heart: A Deep- Learning-Based Computer-Aided Pediatric CHDs Diagnosis System,” IEEE Internet of Things Journal, 2020.

[31]. A. Cherian and A. Sullivan, “Sem-GAN: Semantically-Consistent Image-to-Image Translation,” in Proc. IEEE WACV2019, USA, 2019.

[32]. K. Zhang, W. Zuo et al, “FFDNet: Toward a Fast and Flexible Solution for CNN-Based Image Denoising,” IEEE Transactions on Image Processing, 2018.

[33]. Y. Li and L. Shen, “cC-GAN: A Robust Transfer-learning Framework for HEp-2 Specimen Image Segmentation,” IEEE Access, 2018.

[34]. A. Cherian and A. Sullivan, “Sem-GAN: Semantically-Consistent Image-to-Image Translation,” in Proc. IEEE WACV2019, USA, 2019.

[35]. N. Wang, W. Zha, et al, “Back projection: An effective postprocessing method for GAN based face sketch synthesis,” Pattern Recognition Letters, 2018.

[36]. F. Jiang, Y. Fu, et. al., “Deep Learning based Multi-channel intelligent attack detection for Data Security,” IEEE Transactions on Sustainable Computing, 2020.

[37]. D. Chen, N. Zhang, et. al., “An LDPC code based physical layer message authentication scheme with prefect security”, IEEE Journal on Selected Areas in Communications, 2018.

[38]. A. Ferdowsi and W. Saad, “Deep Learning for signal authentication and security in massive Internet of Things Systems,” IEEE Transactions on Communications, 2019.

[39]. Yi Ding, Guozheng Wu, et al, “DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things”, in: IEEE Internet of Things Journal, 2021

[40]. P. K. D. Pramanik, S. Pal, and M. Mukhopadhyay, ‘‘Healthcare Big Data,” in: igiglobal.
com, 2018, pp. 72–100.

[41]. J. Wang, Z. Zhang, K. Xu, Y. Yin, and P. Guo, ‘‘A research on security and privacy issues for patient related data in medical organization system,” Int. J. Secur. Its Appl., 7(4), pp. 287–298, 2013, Accessed: Jan.22,2021.[Online].Available:https://pdfs.semanticscholar.org/205b/a04d17ace6f175c744a8163adae4ba7633ed.pdf.

[42]. M. Shuaib, S. Alam, S. Mohd, and S. Ahmad, ‘‘Blockchain-Based Initiatives in Social Security Sector,” in: EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD), 2020, p. 8.

[43]. M. Shuaib, S.M. Daud, S. Alam, W.Z. Khan, ‘‘Blockchain-based framework for secure and reliable land registry system, TELKOMNIKA Telecommunication Comput Electron. Control. 18 (5) (2020) 2560, https://doi.org/10.12928/telkomnika.v18i510.12928/telkomnika.v18i5.15787.

[44]. M. Shuaib, S. Alam, S.M. Daud, Improving the Authenticity of Real Estate Land Transaction Data Using Blockchain-Based Security Scheme, Springer, Singapore, 2021, pp. 3–10.

[45]. S. Alam, S. T. Siddiqui, A. Ahmad, R. Ahmad, and M. Shuaib, ‘‘Internet of Things (IoT) Enabling Technologies, Requirements, and Security Challenges,” in: Lecture Notes in Networks and Systems, vol. 94, 2020, pp. 119–126.

[46]. S. T. Siddiqui, M. Shuaib, and B. Mohammad.Ubaidullah, ‘‘Web Based Requirements Management Tools for Software Development: A Study,” Proc. 12th INDIACom; INDIACom-2018; IEEE, no. February 2019, pp. 10–15, 2018.

[47]. M. Shuaib, A. Samad, S. Alam, and S. T. Siddiqui, ‘‘Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration in Organizations,” in: Advances in Intelligent Systems and Computing, vol. 904, 2019, pp. 387–399.

[48]. T. Benson and G. Grieve, ‘‘The Health Information Revolution,” 2021, pp. 3–19.

[49]. C.F. Mondschein, C. Monda, The eu’s general data protection regulation (GDPR) in a research context, in: Fundamentals of Clinical Data Science, Springer International Publishing, Cham, 2018, pp. 55–71.

[50]. E. Politou, A. Michota, E. Alepis, M. Pocs, C. Patsakis, Backups and the right to be forgotten in the GDPR: an uneasy relationship, Comput. Law Secur. Rev. 34 (6) (2018) 1247–1257, https://doi.org/10.1016/j.clsr.2018.08.006.

[51]. M.J. Taylor, M. Prictor, Insight or intrusion? Correlating routinely collected employee data with health risk, Soc. Sci. 8 (10) (2019) 291, https://doi.org/10.3390/socsci8100291.

[52]. C. Tikkinen-Piri, A. Rohunen, J. Markkula, EU General Data Protection Regulation: changes and implications for personal data collecting companies, Comput. Law Secur. Rev. 34 (1) (2018) 134–153, https://doi.org/10.1016/j.clsr.2017.05.015.

[53]. N. Yaraghi and Ram d gopal, ‘‘The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study,” Milbank Q., 96(1), pp. 144–166, Mar. 2018, doi: 10.1111/1468-0009.12314.

[54]. W. Moore and S. Frye, ‘‘Review of HIPAA, Part 1: History, protected health information, and privacy and security rules,” J. Nucl. Med. Technol., 47(4), pp. 269–272, Dec. 2019, doi:10.2967/JNMT.119.227819.

[55]. C.T. Lye, H.P. Forman, J.G. Daniel, H.M. Krumholz, The 21st Century Cures Act and electronic health records one year later: will patients see the benefits?, J. Am. Med. Informatics Assoc. 25 (9) (2018) 1218–1220, https://doi.org/10.1093/jamia/ocy065.

[56]. D. Mohammed, ‘‘U.S. Healthcare Industry: Cybersecurity Regulatory and Compliance Issues,” J. Res. Business, Econ. Manag., vol. 9, no. 5, pp. 1771–1776, 2017, Accessed: Jan. 22, 2021. [Online]. Available: https://core.ac.uk/download/pdf/267833341.pdf.

[57]. S.M. Ahmed, A. Rajput, Threats to patients’ privacy in smart healthcare environment, in: Innovation in Health Informatics, Elsevier, 2020, pp. 375–393.

[58]. Chino.io, ‘‘GDPR and HIPAA Compliance for health applications,” Oct. 01, 2020. https://www.chino.io/compliance/gdpr-hipaa-health-application-compliance (accessed Jan. 18, 2021).

[59]. Mohammed Shuaib Shadab Alam et al, “Compliance with HIPAA and GDPR in blockchain-based electronic health record”, Razak Faculty of Technology and Informatics, University Teknologi Malaysia, Malaysia, Department of Computer Science, College of C.S. & IT, Jazan University, Jazan, Saudi Arabia, 2021