ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΘΕΜΑ:

«ΔΙΑΤΗΡΗΣΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΗΝ ΕΞΟΡΥΞΗ ΚΑΝΟΝΩΝ ΣΥΣΧΕΤΙΣΗΣ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ονοματεπώνυμο: Δίντσης Θωμάς
ΑΜ: 1700033

Επιβλέπων Καθηγητής: Βερύκιος Βασίλειος

ΙΟΥΛΙΟΣ 2005
ΒΟΛΟΣ

Στην οικογένειά μου.

Περίληψη

Η διανομή των δεδομένων είναι συχνά ευεργετική στις εφαρμογές εξόρυξης γνώσης από δεδομένα. Έχει αποδειχθεί ότι είναι χρήσιμο να υποστηριχθούν και οι δύο διαδικασίες λήψης αποφάσεων και να προωθηθούν οι κοινωνικοί στόχοι. Εντούτοις, από την διανομή των δεδομένων έχουν προκύψει διάφορα ηθικά ζητήματα. Αναφορικά, μεταξύ αυτών των ζητημάτων είναι εκείνα της ιδιωτικότητας, της ασφάλειας δεδομένων και των δικαιωμάτων πνευματικής ιδιοκτησίας.

Σε αυτήν την εργασία, εστιάζουμε πρώτιστα στα ζητήματα ιδιωτικότητας στην εξόρυξη γνώσης από δεδομένα, ειδικότερα όταν διαμοιράζονται τα δεδομένα πριν από την εξόρυξη. Ιδιαίτερα, εξετάζουμε μερικά σενάρια στα οποία οι εφαρμογές της εξόρυξης κανόνων συσχέτισης απαιτούν κάποια μέτρα προστασίας της ιδιωτικότητας. Η εξέταση της διατήρησης της ιδιωτικότητας σε τέτοια σενάρια είναι σύνθετη. Κάποιος πρέπει όχι μόνο να καλύψει τις απαιτήσεις ιδιωτικότητας αλλά και να εγγυηθεί τα έγκυρα αποτελέσματα εξόρυξης δεδομένων. Αυτή η κατάσταση δείχνει την επείγουσα ανάγκη για αναθεώρηση μηχανισμών που θα επιβάλλουν μέτρα προστασίας της ιδιωτικότητας χωρίς απώλεια του οφέλους της εξόρυξης. Αυτοί οι μηχανισμοί είναι σε θέση να οδηγήσουν σε νέες μεθόδους ελέγχου της ιδιωτικότητας όπου θα μετατρέπουν μια βάση δεδομένων σε μια νέα με τέτοιο τρόπο ώστε να διατηρηθούν τα βασικά χαρακτηριστικά γνωρίσματα της αρχικής βάσης δεδομένων κατά την εξόρυξη γνώσης.

Ειδικότερα, εξετάζεται το πρόβλημα της μετατροπής μιας βάσης δεδομένων που πρόκειται να διαμοιραστεί σε μια νέα που κρύβει τις ιδιωτικές πληροφορίες ενώ παράλληλα διατηρεί τα γενικά πρότυπα και τις τάσεις από την αρχική βάση δεδομένων. Για να εξετάσουμε αυτό το προκλητικό πρόβλημα, προτείνεται ένα σύνολο αλγορίθμων καθαρισμού για διατήρηση της ιδιωτικότητας κατά την εξόρυξη γνώσης από δεδομένα που εξασφαλίζει ότι η διαδικασία εξόρυξης δεν θα παραβιάσει την ιδιωτικότητα μέχρι έναν ορισμένο βαθμό ασφάλειας. Το σύνολο αυτό ανήκει σε μια οικογένεια μεθόδων μετασχηματισμού των δεδομένων για διατήρηση της ιδιωτικότητας.

Η έρευνα καταλήγει στο συμπέρασμα ότι η διατήρηση της ιδιωτικότητας κατά την εξόρυξη γνώσης από δεδομένα είναι ως ένα ορισμένο βαθμό εφικτή. Καταδεικνύουμε εμπειρικά και θεωρητικά την πρακτικότητα και την δυνατότητα της διατήρησης ιδιωτικότητας στην εξόρυξη δεδομένων. Τα πειράματα μας

αποκαλύπτουν ότι οι αλγόριθμοι είναι αποτελεσματικοί, καλύπτουν τις απαιτήσεις ιδιωτικότητας, και εγγυόνται έγκυρα αποτελέσματα εξόρυξης δεδομένων προστατεύοντας τις ευαίσθητες πληροφορίες (π.χ. ευαίσθητη γνώση και ιδιωτικότητα των ατόμων).

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Βασίλειο Βερύκιο για την εμπιστοσύνη που έδειξε στο πρόσωπό μου. Οι χρήσιμες συμβουλές και η σημαντική καθοδήγηση που μου έδωσε, με βοήθησαν να βρω τον σωστό δρόμο της αποπεράτωσης αυτής της διπλωματικής.

Ευχαριστώ πολύ τον εξεταστή καθηγητή κ. Γεώργιο Μουστακίδη για την ανάγνωση και την αξιολόγηση της εργασίας μου.

Ένα μεγάλο ευχαριστώ στην οικογένεια και τους συγγενείς μου για την ψυχολογική στήριξη και την υπομονή τους.

Ευχαριστώ πολύ τους φίλους και συμφοιτητές μου για το κουράγιο και την υπομονή τους όλο αυτό το διάστημα.

Βόλος, 4 Ιούλιου 2005.

Περιεχόμενα

Εικόνες

Πίνακες

Ονοματολογία αλγορίθμων

Η ονοματολογία των αλγορίθμων σε αυτήν την διπλωματική έγινε με την βοήθεια των παρακάτω συμβόλων των οποίων η σημασία δίνεται στον παρακάτω πίνακα.

S	Support
C	Confidence
R	Reduce
P	Pattern
V	Victim Item
Gr	Group
Tc	Confidence Threshold
Ts	Support Threshold
Tp	Threshold per Pattern
Q	Question Mark "?"
G	Graph
Min	Minimum
Sh	Share Rules
Srb	Round Robin Selection
Sr	Random Selection

Πίνακας 1: Σύμβολα Ονοματολογίας Αλγορίθμων Καθαρισμού

Για κάθε αλγόριθμο, υπάρχει το όνομα με το οποίο αναφέρεται στην βιβλιογραφία, το νέο όνομα μετα την αντιστοίχηση με τα παραπάνω σύμβολο, μια σύντομη περιγραφή του και η αναφορά στην βιβλιογραφία.

Όνομα Αλγορίθμου	**Νέο Όνομα**	**Περιγραφή**	**Αναφορά**
GIH	RSTsQ	Κρύβει τους ευαίσθητους κανόνες με τη μείωση της ελάχιστης υποστήριξης των στοιχειοσυνόλων που τους παράγουν έως ότου η ελάχιστη υποστήριξη πέσει κάτω από ένα ελάχιστο κατώφλι υποστήριξης. Για να το πετύχει αυτό αλλάζει γνωστές τιμές με αγνώστους «?».	[5]
CR	RCTcTsQ	Κρύβει τους ευαίσθητους κανόνες με τη μείωση της ελάχιστης εμπιστοσύνης των στοιχειοσυνόλων που τους παράγουν έως ότου η ελάχιστη υποστήριξη πέσει κάτω από ένα	[5]

		ελάχιστο κατώφλι υποστήριξης, Για να το πετύχει αυτό αλλάζει γνωστές τιμές με αγνώστους «?».	
BA	RCTcQ	Κρύβει τους ευαίσθητους κανόνες με τη μείωση της ελάχιστης εμπιστοσύνης των στοιχειοσυνόλων που τους παράγουν έως ότου η ελάχιστη εμπιστοσύνη πέσει κάτω από ένα ελάχιστο κατώφλι εμπιστοσύνης. Για να το πετύχει αυτό αλλάζει γνωστές τιμές με αγνώστους «?».	[52]
Algo1a	RCTc	Κρύβει τους ευαίσθητους κανόνες με τη μείωση της ελάχιστης εμπιστοσύνης των στοιχειοσυνόλων που τους παράγουν έως ότου η ελάχιστη εμπιστοσύνη πέσει κάτω από ένα ελάχιστο κατώφλι εμπιστοσύνης. Για να το πετύχει αυτό αυξάνει την υποστήριξη του πρότερου τμήματος του κανόνα.	[4]
Algo1b	RCTc2	Κρύβει τους ευαίσθητους κανόνες με τη μείωση της ελάχιστης εμπιστοσύνης των στοιχειοσυνόλων που τους παράγουν έως ότου η ελάχιστη εμπιστοσύνη πέσει κάτω από ένα ελάχιστο κατώφλι εμπιστοσύνης. Για να το πετύχει αυτό μειώνει την υποστήριξη του ακόλουθου τμήματος του κανόνα.	[4]
Algo2a	RSTcTs	Κρύβει τους ευαίσθητους κανόνες με τη μείωση της ελάχιστης υποστήριξης των στοιχειοσυνόλων που τους παράγουν έως ότου η ελάχιστη υποστήριξη πέσει κάτω από ένα ελάχιστο κατώφλι υποστήριξης ή η ελάχιστη εμπιστοσύνη πέσει κάτω από ένα ελάχιστο κατώφλι εμπιστοσύνης. Για να το πετύχει αυτό μειώνει την υποστήριξη είτε του πρότερου είτε του ακόλουθου τμήματος του.κανόνα.	[4]

Naive	AllPV	Επιλέγει να αφαιρέσει όλα τα αντικείμενα σε μια δοσοληψία ως θύματα με σκοπό την απόκρυψη των ευαίσθητων προτύπων/κανόνων.	[40]
MinFIA	MinFPV	Επιλέγει ως αντικείμενο-θύμα, για ένα δεδομένο περιοριστικό πρότυπο, το αντικείμενο με τη μικρότερη υποστήριξη στο πρότυπο. Αυτό συνεπάγεται την επιλογή των δοσοληψιών με τον μικρότερο αριθμό συγκρούσεων.	[40]
RRA	SrbPV	Αντί να επιλέγει ένα μοναδικό αντικείμενο-θύμα ανά δεδομένο ευαίσθητο πρότυπο/κανόνα, επιλέγει διαφορετικά αντικείμενα-θύματα σε κάθε γύρο, αρχίζοντας από το πρώτο αντικείμενο, έπειτα το δεύτερο και ου το καθεξής σε κάθε ευαίσθητη δοσοληψία.	[41]
RA	SrPV	Επιλέγει τυχαία ένα αντικείμενο από μια δοσοληψία ως αντικείμενο-θύμα.	[41]
IGA	GrPV	Ομαδοποιεί τους ευαίσθητους κανόνες συσχέτισης σε ομάδες κανόνων που μοιράζονται τα ίδια στοιχειοσύνολα. Αν δύο ή περισσότεροι κανόνες τέμνονται, καθαρίζοντας το κοινό αντικείμενο αυτών των ευαίσθητων κανόνων μπορούν να αποκρυφθούν αυτοί οι κανόνες σε ένα βήμα.	[40]
SWA	WPVTp	Σαρώνει ένα σύνολο από K δοσοληψίες, το παράθυρο, τη φορά και καθαρίζει τους ευαίσθητους κανόνες που βρίσκονται στις ευαίσθητες δοσοληψίες με βάση ένα κατώφλι κοινοποίησης που το ορίζει ο χρήστης. Η διαφορά είναι ότι μπορεί να οριστεί διαφορετικό κατώφλι για κάθε ευαίσθητο κανόνα.	[42]
DSA	GPSh	Ενεργεί στους κανόνες που προκύπτουν από	[43]

		την βάση δεδομένων παρά στην ίδια την βάση. Τα στοιχειοσύνολα που δίνουν τους κανόνες αναπαρίστανται με την βοήθεια του γράφου στοιχειοσυνόλων. Κρύβει τους κανόνες πριν τον διαμοιρασμό τους και έτσι η υποστήριξη και η εμπιστοσύνη των μη-ευαίσθητων κανόνων παραμένει αμετάβλητη.	

Πίνακας 2: Ονοματολογία Αλγορίθμων Καθαρισμού

Γλωσσάρι

Αλγόριθμοι Διαμοιρασμού Δεδομένων: είναι μια κλάση των αλγορίθμων καθαρισμού στους οποίους οι πράξεις της διαδικασίας καθαρισμού ενεργούν στα στοιχεία για να αφαιρέσουν ή να κρύψουν την ομάδα των ευαίσθητων κανόνων συσχέτισης.

Αλγόριθμοι Διαμοιρασμού Προτύπων: είναι μια κλάση των αλγορίθμων καθαρισμού στους οποίους οι πράξεις της διαδικασίας καθαρισμού ενεργούν στους κανόνες που εξήχθησαν από μια βάση δεδομένων αντί στα ίδια τα δεδομένα. Ο καθαρισμός αφαιρεί όχι μόνο όλα τα ευαίσθητα πρότυπα αλλά και εμποδίζει άλλα πρότυπα που θα μπορούσαν να χρησιμοποιηθούν για να συμπεράνουν τα ευαίσθητα.

Αντικείμενο-Θύμα: ορίζεται ως το υποψήφιο αντικείμενο που πρέπει να αποβληθεί από τις ευαίσθητες δοσοληψίες κατά τον καθαρισμό δεδομένων. Αφαιρώντας αυτό το αντικείμενο από τις ευαίσθητες δοσοληψίες, ένας ή περισσότεροι ευαίσθητοι κανόνες θα κρυφτούν σε μια βάση δεδομένων δοσοληψιών.

Βάση Δεδομένων Δοσοληψιών: είναι μια σχέση που αποτελείται από τις δοσοληψίες στις οποίες κάθε δοσοληψία t χαρακτηρίζεται από έναν μοναδικό αριθμό αναγνωριστή (TID) και έναν κατάλογο αντικειμένων που αποτελούν τη δοσοληψία. Οι βάσεις δεδομένων δοσοληψιών χρησιμοποιούνται ευρέως στην εξόρυξη κανόνων συσχέτισης.

Διατήρηση Ιδιωτικότητας κατ την Εξόρυξη Γνώσης από Δεδομένα: καλύπτει το διπλό στόχο της απαίτησης για ιδιωτικότητα και της ανάγκης έγκυρων αποτελεσμάτων εξόρυξης γνώσης από δεδομένα.

Εμπιστοσύνη: στους κανόνες συσχέτισης, η εμπιστοσύνη ενός κανόνα $X \Rightarrow Y$ ορίζεται ως η αναλογία των δοσοληψιών που περιέχουν το X και που περιέχουν επίσης το Y στις δοσοληψίες που περιέχουν το X.

Ευαίσθητες Δοσοληψίες: Το σύνολο των δοσοληψιών που συμμετέχουν στην παραγωγή των ευαίσθητων κανόνων.

Ευαίσθητη Γνώση: περιγράφεται ως γνώση που μπορεί να παρέχει το ανταγωνιστικό πλεονέκτημα στον επιχειρησιακό κόσμο.

Ευαίσθητοι Κανόνες: είναι ειδική ομάδα κανόνων συσχέτισης που αντιπροσωπεύουν την ευαίσθητη γνώση που εξάγεται από τις βάσεις δεδομένων.

Καθαρισμός Δεδομένων: είναι η διαδικασία απόκρυψης των ευαίσθητων κανόνων στις βάσεις δεδομένων δοσοληψιών. Ο καθαρισμός επιτυγχάνεται με την τροποποίηση μερικών δοσοληψιών. Σε μερικές περιπτώσεις, διάφορα αντικείμενα διαγράφονται από μια ομάδα δοσοληψιών (ευαίσθητες δοσοληψίες) με σκοπό το κρύψιμο των ευαίσθητων κανόνων που προέρχονται από εκείνες τις δοσοληψίες. Με αυτό τον τρόπο, η υποστήριξη τέτοιων ευαίσθητων κανόνων μειώνεται κάτω από ένα ελάχιστο κατώφλι υποστήριξης που ορίζεται από τον κάτοχο των δεδομένων. Ένας άλλος τρόπος να κρυφτούν οι ευαίσθητοι κανόνες είναι να προστεθούν νέα αντικείμενα σε μερικές δοσοληψίες για να αλλάξει (μείωση) η εμπιστοσύνη των ευαίσθητων κανόνων.

Κανάλια Συμπεράσματος: εμφανίζονται όταν κάποιος εξάγει ένα καθαρισμένο σύνολο κανόνων και, βασισμένος στους μη-ευαίσθητους κανόνες, συνάγει έναν ή περισσότερους ευαίσθητους κανόνες που υποτίθεται ότι δεν πρέπει να ανακαλυφθούν.

Κανόνες Συσχέτισης: περιγράφουν σημαντικές συσχετίσεις μεταξύ αντικειμένων που βρίσκονται ομαδοποιημένα σε έναν σημαντικό αριθμό παραδειγμάτων.

Κατώφλι Κοινοποίησης: είναι ένα κατώφλι που εκφράζει κατά πόσο θα κοινοποιηθεί η ευαίσθητη γνώση που περιέχεται στους ευαίσθητους κανόνες που θέλουμε να κρυφτούν. Όταν το κατώφλι είναι 0%, κανένας κανόνας δεν θα κοινοποιηθεί, ενώ όταν το κατώφλι είναι 100% κοινοποιούνται όλοι οι κανόνες.

Μεμονωμένη Ιδιωτικότητα: ενδιαφέρεται για την προστασία της ευαίσθητης γνώσης που αντιστοιχεί σε προσωπικές πληροφορίες ενός ατόμου.

Συλλογική Ιδιωτικότητα: ενδιαφέρεται για την προστασία αντιπροσωπεύει τις δραστηριότητες μιας ομάδας. Η ευαίσθητη γνώση πρέπει να προστατευθεί για λόγους στρατηγικούς ή ανταγωνιστικούς.

Υποστήριξη: στους κανόνες συσχέτισης, η υποστήριξη ενός στοιχειοσυνόλου ορίζεται ως η αναλογία των δοσοληψιών που περιέχουν το στοιχειοσύνολο σε όλες τις δοσοληψίες.

Αντιστοίχηση Ελληνικής Ορολογίας σε Αγγλική

Ανακάλυψη Γνώσης από Βάσεις Δεδομένων: Knowledge Discovery in Databases, KDD

Παρασκηνιακή δραστηριότητα: Behind the scenes activity

Εξυπηρετητές αρχείων: File servers

Προβλεπτικό μοντέλο: Predictive Modeling

Διατήρηση Ιδιωτικότητας κατά την Εξόρυξη Γνώσης, ΔΙΕΓ: Privacy Preserving Data Mining, PPDM

Συναθροίσεις: Aggregates

Συσχετίσεις: Relationships

Ρητά (σαφή) δεδομένα: Explicit data

Υπονοούμενα δεδομένα: Implicit data

Μέτρα ποσότητας ενδιαφέροντος: Interestingness measures

Κοινοποίηση: Disclosure

Διαμοιρασμός δεδομένων: Data sharing

Διαμοιρασμός πρότυπων: Pattern sharing

Οδηγημένος-από-δεδομένα: Data-driven

Οδηγημένος-από-ερωτήσεις: Query-driven

Χαρακτηρισμός: Characterization

Περιληπτική παρουσίαση της πληροφορίας: Summarization

Κατηγοριοποίηση: Classification

Πλειάδα: Tuple

Δείγματα εκπαίδευσης: Training samples

Κανόνες συσχέτισης: Association Rules

Ανάλυση καλαθιών αγοράς: Market basket analysis

Αναγνωριστής: Identifier

Εμφανίσεων: Occurrences

Καταστολή αναγνωριστή: Identifier suppression

Παρενέργεια: Side effect

Μαγνήτες δεδομένων: Data magnets

Διαμέριση δεδομένων: Data partitioning

Μετατροπή δεδομένων: Data modification

Περιορισμός δεδομένων: Data restriction

Ιδιοκτησία δεδομένων: Data ownership

Ασφαλές Πολυκομματικό Πρόβλημα Υπολογισμού: Secure Multi-party Computation Problem

Συνδυαστής: Combiner

Τεχνικές προσθήκης θορύβου: Noise addition techniques

Τεχνικές χωρικού μετασχηματισμού: Space transformation techniques

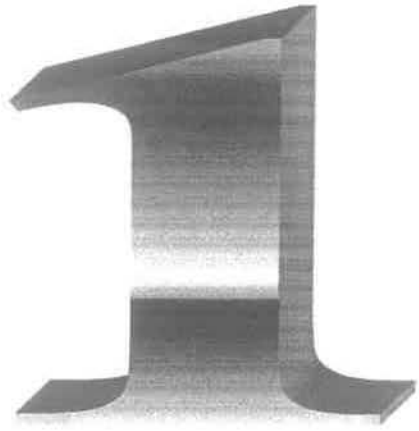
Τεχνικές ανταλλαγής δεδομένων: Data swapping

Τεχνικές διαταραχής δεδομένων: Data perturbation

Τεχνικές τυχαιοποίησης δεδομένων: Data randomization

Γράφος στοιχειοσυνόλων: Itemset graph

Συγκρουόμενες δοσοληψίες: Conflicting transactions



Κεφάλαιο 1

Μια Εισαγωγή στην Διατήρηση Ιδιωτικότητας κατά την Εξόρυξη Γνώσης από Δεδομένα

1.1. Εισαγωγή

Οι πρόσφατες εξελίξεις στην τεχνολογία πληροφοριών έχουν καταστήσει δυνατή τη συλλογή και την ανάλυση εκατομμυρίων δοσοληψιών που περιέχουν προσωπικά δεδομένα. Αυτά τα δεδομένα περιλαμβάνουν, μεταξύ των άλλων, συνήθειες αγορών, ποινικά μητρώα, ιατρικά ιστορικά και πιστωτικά αρχεία [7]. Αυτή η πρόοδος στην αποθήκευση και την ανάλυση των δεδομένων έχει οδηγήσει τα άτομα και τις οργανώσεις να αντιμετωπίσουν την πρόκληση της μετατροπής τέτοιων δεδομένων σε χρήσιμες πληροφορίες και γνώση.

Η εξόρυξη γνώσης από δεδομένα είναι μια ελπιδοφόρος προσέγγιση που προσπαθεί να καλύψει αυτήν την προκλητική απαίτηση. Ο τομέας της εξόρυξης δεδομένων, αποκαλούμενος επίσης Ανακάλυψη Γνώσης από Βάσεις Δεδομένων, λαμβάνει ιδιαίτερη προσοχή από τη δεκαετία του '90. Αυτός ο νέος ερευνητικός τομέας έχει προκύψει ως μέσο *εξαγωγής* των κρυμμένων προτύπων ή των προηγουμένως άγνωστων υπονοούμενων πληροφοριών από τις μεγάλες αποθηκεύσεις των δεδομένων [21]. Η γοητεία που ασκεί η υπόσχεση της ανάλυσης τεραστίων ποσοτήτων δεδομένων έχει οδηγήσει σε έναν αυξανόμενο αριθμό επιτυχών εφαρμογών της εξόρυξης δεδομένων τα τελευταία χρόνια. Αναμφισβήτητα, αυτές οι

εφαρμογές είναι πολύ χρήσιμες σε πολλές περιοχές όπως το μάρκετινγκ, η επιχειρηματικότητα, η ιατρική ανάλυση και άλλες εφαρμογές στις οποίες η ανακάλυψη προτύπων είναι κυρίαρχη για τη στρατηγική λήψης αποφάσεων.

Παρά το όφελος της στις διάφορες περιοχές, η χρήση των τεχνικών εξόρυξης μπορεί επίσης να οδηγήσει σε νέες απειλές στη ιδιωτικότητα και στην ασφάλεια πληροφοριών. Το πρόβλημα δεν είναι η ίδια η εξόρυξη, αλλά ο τρόπος με τον οποίο αυτή γίνεται [31]. Όπως αναφέρουν οι Vaidya & Clifton [50], τα αποτελέσματα της εξόρυξης γνώσης, σπάνια παραβιάζουν τη ιδιωτικότητα, δεδομένου ότι αποκαλύπτουν γενικά την υψηλού επιπέδου γνώση παρά τα ίδια τα δεδομένα. Παρόλα αυτά, η ανησυχία μεταξύ των συνηγόρων της ιδιωτικότητας αρχίζει και εμφανίζεται έντονα, δεδομένου ότι φέρνοντας τα δεδομένα πιο κοντά στην υποστήριξη προγραμμάτων εξόρυξης γνώσης, η κακή χρήση τους καθίσταται ευκολότερη. Κατά συνέπεια, δεδομένης της απουσίας επαρκών μέτρων προστασίας, η χρήση της εξόρυξης δεδομένων μπορεί να διακινδυνεύσει την ιδιωτικότητα και την αυτονομία των ατόμων. Σοβαρότερη είναι η προσβολή ιδιωτικότητας που προκαλείται από τη δευτεροβάθμια χρήση των δεδομένων, όταν τα άτομα αγνοούν την παρασκηνιακή χρήση των τεχνικών εξόρυξης γνώσης [29]. Για παράδειγμα, η Culnan [16] έκανε μια ιδιαίτερη μελέτη της δευτεροβάθμιας χρήσης πληροφοριών, την οποία όρισε ως «*η χρήση των προσωπικών πληροφοριών για άλλους λόγους επακόλουθους της αρχικής δοσοληψίας μεταξύ ενός ατόμου και μιας οργάνωσης όταν συλλέχθησαν οι πληροφορίες*». Βασικό δεδομένο αυτής της μελέτης ήταν ότι η ανησυχία σχετικά με τη δευτεροβάθμια χρήση συσχετίστηκε με το επίπεδο ελέγχου που το άτομο έχει πέρα από τη δευτεροβάθμια χρήση.

Παρότι πολλά κράτη έχουν αναπτύξει νόμους και κανονισμούς ενάντια στην ιδιωτική χρήση προσωπικών πληροφοριών, οι υφιστάμενοι νόμοι και οι θεμελιώδεις έννοιές τους έχουν ξεπεραστεί λόγω των εξελίξεων στην τεχνολογία [34, 38, 20, 15]. Κατά συνέπεια, αυτά τα προσωπικά δεδομένα υπάρχουν σε χιλιάδες εξυπηρετητές αρχείων, κατά ένα μεγάλο μέρος πέρα από τον έλεγχο των υφιστάμενων νόμων ιδιωτικότητας, οδηγώντας σε πιθανή προσβολή της ιδιωτικότητας σε τέτοια κλίμακα όσο ποτέ άλλοτε.

Σύνθετα ζητήματα, όπως εκείνα που περιλαμβάνονται στην «*Διατήρηση Ιδιωτικότητας κατά την Εξόρυξη Γνώσης από δεδομένα, ΔΙΕΓ*», δεν μπορούν απλά να αντιμετωπιστούν με τον περιορισμό της συλλογής δεδομένων ή ακόμα και με τον περιορισμό της δευτεροβάθμιας χρήσης της τεχνολογίας πληροφοριών [2, 7, 39].

Επιπλέον, δεν υπάρχει καμία ακριβής λύση που επιλύει τη διατήρηση ιδιωτικότητας στην εξόρυξη δεδομένων. Μια κατά προσέγγιση λύση θα μπορούσε να είναι επαρκής μόνο ανάλογα με την εφαρμογή, δεδομένου ότι το κατάλληλο επίπεδο ιδιωτικότητας μπορεί να ερμηνευθεί σε διαφορετικά πλαίσια [12, 11]. Σε μερικές εφαρμογές (π.χ. κανόνες συσχέτισης, κατηγοριοποίηση, ή συσταδοποίηση), πρέπει να βρεθεί μια σωστή ισορροπία μεταξύ της ανάγκης για ιδιωτικότητα και της ανακάλυψης γνώσης.

Η διατήρηση της ιδιωτικότητας όταν διαμοιράζονται τα δεδομένα για εξόρυξη γνώσης είναι ένα προκλητικό πρόβλημα. Οι παραδοσιακές μέθοδοι της ασφάλειας βάσεων δεδομένων, όπως ο έλεγχος πρόσβασης και η πιστοποίηση ταυτότητας [8 , 24, 47], που έχουν υιοθετηθεί για να διαχειριστούν επιτυχώς την πρόσβαση στα δεδομένα παρουσιάζουν κάποιους περιορισμούς στα πλαίσια της εξόρυξης δεδομένων. Ενώ ο έλεγχος πρόσβασης και η πιστοποίηση ταυτότητας μπορούν να παρέχουν προστασία ενάντια στην άμεση κοινοποίηση, δεν εξετάζεται η κοινοποίηση που βασίζεται σε συμπεράσματα που μπορούν να προέρχονται από δημοσιευμένα δεδομένα. Η παρεμπόδιση αυτού του τύπου ανίχνευσης συμπερασμάτων είναι πέρα από την προσιτότητα των υπαρχουσών μεθόδων [2, 39]. Επομένως, κάποια δεδομένα της εργασίας αυτής ξεφεύγουν από τα παραδοσιακά πρότυπα για την ασφάλεια βάσεων δεδομένων.

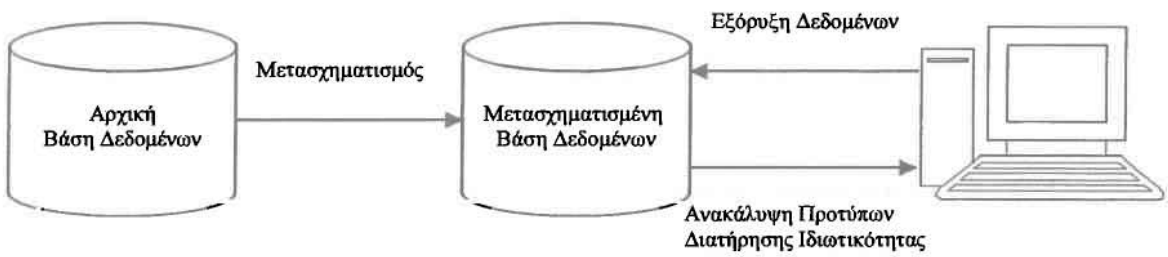
Αναμφίβολα, τα ζητήματα ιδιωτικότητας θέτουν νέες προκλήσεις για νέους χρήστες της τεχνολογίας εξόρυξης γνώσης από δεδομένα [38, 33, 37]. Αυτές οι τεχνικές προκλήσεις δείχνουν μια επείγουσα ανάγκη για αναθεώρηση των μηχανισμών αντιμετώπισης των ζητημάτων της ιδιωτικότητας και της ακρίβειας κατά το διαμοιρασμό των δεδομένων ή την ανταλλαγή τους πριν από την εξόρυξη. Τέτοιοι μηχανισμοί μπορούν να οδηγήσουν σε νέες μεθόδους ελέγχου ιδιωτικότητας ώστε να μετατραπεί μια βάση δεδομένων σε μια νέα που *κρύβει* τις ιδιωτικές πληροφορίες διατηρώντας παρόλα αυτά τα γενικά πρότυπα και τις τάσεις από την αρχική βάση δεδομένων.

1.2. Διατήρηση Ιδιωτικότητας: Μια Πρώτη Προσέγγιση

Στην εργασία αυτή, εξετάζεται το πρόβλημα της μετατροπής μιας βάσης δεδομένων σε μια νέα που θα αποκρύπτει ευαίσθητες πληροφορίες ενώ παράλληλα θα διατηρεί τα γενικά πρότυπα και τις τάσεις από την αρχική βάση δεδομένων. Οι

ευαίσθητες πληροφορίες δεν περιορίζονται σε προσωπικά δεδομένα αλλά μπορεί να αντανακλούν προσωπικές συμπεριφορές πελατών, οικονομικές, ιατρικές και ασφαλιστικές πληροφορίες καθώς επίσης και ευαίσθητα πρότυπα.

Ο μετασχηματισμός που εφαρμόζεται στη βάση δεδομένων εμφανίζεται πριν από τον διαμοιρασμό των δεδομένων για τη εξόρυξη, όπως μπορούμε να δούμε στην Εικόνα 1.



Εικόνα 1: Ένα παράδειγμα μετατροπής βάσης δεδομένων πριν την εξόρυξη

Εστιάζουμε πρωτίστως στη ΔΙΕΓ, ιδιαίτερα στα πλαίσια των κανόνων που περιγράφουν ενδιαφέρουσες συσχετίσεις μεταξύ των αντικειμένων που συγκεντρώνονται σε έναν σημαντικό αριθμό παραδειγμάτων (κανόνες συσχέτισης).

Το πρόβλημα της μετατροπής μιας βάσης δεδομένων, πριν από το διαμοιρασμό των δεδομένων για εξόρυξη, θα προσεγγιστεί από την σκοπιά της διατήρησης ιδιωτικότητας σε εξόρυξη κανόνων συσχέτισης.

1.2.1. Διατήρηση Ιδιωτικότητας σε Εξόρυξη Κανόνων Συσχέτισης

Στα πλαίσια της διατήρησης ιδιωτικότητας στην εξόρυξη κανόνων συσχέτισης, δεν εξετάζεται το πρόβλημα της ιδιωτικότητας των ατόμων. Αντί αυτού, εξετάζεται το πρόβλημα της ευαίσθητης γνώσης που εξάγεται από τις βάσεις δεδομένων. Η ευαίσθητη γνώση αντιπροσωπεύεται από μια ειδική ομάδα κανόνων συσχέτισης αποκαλούμενων *ευαίσθητων κανόνων συσχέτισης*. Αυτοί οι κανόνες είναι κυρίαρχοι για τη στρατηγική αποφάσεων και πρέπει να παραμένουν ιδιωτικοί (δηλαδή οι κανόνες είναι ιδιωτικοί στην επιχείρηση ή την οργάνωση που είναι κυρία των δεδομένων).

Το πρόβλημα της προστασίας της ευαίσθητης γνώσης στις βάσεις δεδομένων δοσοληψιών, προϋποθέτει τα ακόλουθα:

- Οι κάτοχοι δεδομένων πρέπει να ξέρουν εκ των προτέρων κάποια γνώση (κανόνες) που θέλουν να προστατεύσουν. Τέτοιοι κανόνες είναι θεμελιώδεις στις λήψεις αποφάσεων και, έτσι, δεν πρέπει να ανακαλύπτονται.
- Οι ανεξάρτητες τιμές δεδομένων (π.χ. ένα συγκεκριμένο αντικείμενο) δεν περιορίζονται. Γι'αυτόν τον λόγο, μερικές συναθροίσεις και συσχετίσεις πρέπει να προστατεύονται.

Το πρόβλημα της διατήρησης της ιδιωτικότητας στην εξόρυξη κανόνων συσχέτισης μπορεί να οριστεί ως εξής:

> Εάν D είναι η αρχική βάση δεδομένων των δοσοληψιών και R είναι ένα σύνολο σχετικών κανόνων συσχέτισης που θα μπορούσαν να εξαχθούν από την D, ο στόχος είναι να μετασχηματιστεί η D σε μια βάση δεδομένων D' έτσι ώστε οι περισσότεροι κανόνες συσχέτισης στο R να μπορούν ακόμα να εξαχθούν από την D' ενώ άλλοι, που αντιπροσωπεύουν την ευαίσθητη γνώση, να κρύβονται. Σε αυτήν την περίπτωση, η D' είναι η βάση δεδομένων που διαμοιράζεται.

1.2.2. Προστασία Γνώσης έναντι Διατήρησης Ιδιωτικότητας

Η προστασία ευαίσθητων πληροφοριών στα πλαίσια της έρευνάς μας καλύπτει δύο σημαντικούς στόχους: *προστασία γνώσης* και *διατήρηση ιδιωτικότητας*. Ο πρώτος συσχετίζεται με την εξόρυξη κανόνων συσχέτισης, ενώ ο δεύτερος αφορά στη διατήρηση ιδιωτικότητας στη συσταδοποίηση. Στην εργασία αυτή θα κινηθούμε στα πλαίσια του πρώτου στόχου.

Μια ενδιαφέρουσα πτυχή μεταξύ προστασίας και διατήρησης ιδιωτικότητας είναι ότι έχουν ένα κοινό χαρακτηριστικό. Παραδείγματος χάριν, στην προστασία γνώσης, ένας οργανισμός είναι ο ιδιοκτήτης των δεδομένων και έτσι πρέπει να προστατεύσει την ευαίσθητη γνώση που μπορεί να ανακαλυφθεί από τέτοια δεδομένα, ενώ στη διατήρηση ιδιωτικότητας *τα άτομα* είναι ο ιδιοκτήτης των προσωπικών πληροφοριών τους. Αφ' ετέρου, η προστασία γνώσης και η διατήρηση ιδιωτικότητας έχουν επίσης ένα μοναδικό χαρακτηριστικό. Η διατήρηση

ιδιωτικότητας συσχετίζεται με την προστασία των ρητών (σαφών) δεδομένων (π.χ. μισθός), ενώ η προστασία γνώσης ενδιαφέρεται για την προστασία των υπονοούμενων δεδομένων, δηλαδή πρότυπα που ανακαλύπτονται από τα δεδομένα.

Ένας περιορισμός με την προσέγγιση της προστασίας γνώσης είναι ότι η ευαίσθητη γνώση πρέπει να κοινοποιηθεί *εκ των προτέρων* από τους κατόχους των δεδομένων. Σε αυτήν την περίπτωση, οι κάτοχοι των δεδομένων πρέπει να εξορύξουν τις βάσεις δεδομένων τους και να χρησιμοποιήσουν μέτρα ποσότητας ενδιαφέροντος (π.χ. υποστήριξη και εμπιστοσύνη) με σκοπό τον εντοπισμό πολύτιμων προτύπων, δηλαδή ευαίσθητης γνώσης. Στη συνέχεια, οι κάτοχοι δεδομένων μπορούν να κρύψουν την ευαίσθητη γνώση με τη χρησιμοποίηση αλγορίθμων που περιγράφονται στο κεφάλαιο 5. Η βάση δεδομένων διατίθεται έπειτα για εξόρυξη.

Ένας άλλος περιορισμός της προσέγγισης της προστασίας γνώσης είναι ότι δεν εστιάζουμε στην προστασία από τους συσχετισμούς μεταξύ των μεταβλητών, όπως για παράδειγμα ο μισθός και η ηλικία ενός προσώπου. Αντ'αυτού, προστατεύουμε συγκεκριμένους δυαδικούς κανόνες (π.χ. $X \Rightarrow Y$), όπου X και Y αντιπροσωπεύουν για παράδειγμα αντικείμενα που αγοράζονται σε ένα κατάστημα ή γνωρίσματα με συγκεκριμένες τιμές. Ωστόσο, αυτοί οι κανόνες είναι ιδιωτικοί στην επιχείρηση ή τον οργανισμό που είναι κύριος των δεδομένων και πρέπει να προστατευθούν διότι μπορούν να παρέχουν ένα ανταγωνιστικό πλεονέκτημα στον επιχειρησιακό κόσμο.

1.3. Κεντρική Ιδέα Διπλωματικής

Σε αυτήν την εργασία, ερευνούμε τη δυνατότητα πραγματοποίησης της ΔΙΕΓ από το μετασχηματισμό δεδομένων. Η κεντρική ιδέα της διπλωματικής είναι η εξής:

Η διατήρηση ιδιωτικότητας στην εξόρυξη γνώσης από δεδομένα (ΔΙΕΓ), με το μετασχηματισμό δεδομένων, είναι δυνατή, ως ένα ορισμένο βαθμό.

Αυτή η έρευνα παρουσιάζει εμπειρικά και θεωρητικά την πρακτικότητα και την δυνατότητα πραγματοποίησης της ΔΙΕΓ. Ειδικότερα, αποδεικνύεται ότι μια ισορροπία μεταξύ της συντήρησης ιδιωτικότητας και της ανακάλυψης γνώσης μπορεί να ολοκληρωθεί κατά την εξέταση της προστασίας γνώσης στην εξόρυξη κανόνων συσχέτισης.

Τρία σημαντικά ζητήματα αντιμετωπίζονται για να υποστηρίξουν την κεντρική ιδέα της διπλωματικής αυτής:

- Είναι δυνατόν να προστατευθεί η ευαίσθητη γνώση που ανακαλύπτεται από τις βάσεις δεδομένων χωρίς απώλεια του οφέλους της εξόρυξης της μετασχηματισμένης βάσης δεδομένων.
- Είναι δυνατόν να *προσδιοριστεί ποσοτικά* η κοινοποίηση της ευαίσθητης γνώσης που ανακαλύπτεται από μια μετασχηματισμένη βάση δεδομένων.
- Είναι δυνατό να μετρηθεί η απώλεια πληροφοριών σε μια μετασχηματισμένη βάση δεδομένων διαθέσιμη για εξόρυξη κανόνων συσχέτισης.

1.4. Συνεισφορές της Διπλωματικής

Οι σημαντικότερες συνεισφορές αυτής της εργασίας μπορούν να συνοψιστούν ως εξής:

1. **Θεμελίωση ΔΙΕΓ**: Θέτουμε τα θεμέλια και τα ζητήματα τυποποίησης για ΔΙΕΓ. Πιο συγκεκριμένα, περιγράφουμε τα προβλήματα που αντιμετωπίζουμε σχετικά με το ποιες πληροφορίες είναι ιδιωτικές στην εξόρυξη δεδομένων, και συζητάμε πώς η ιδιωτικότητα μπορεί να παραβιαστεί στην εξόρυξη δεδομένων. Περιγράφουμε τη βάση της ΔΙΕΓ συμπεριλαμβανομένων των ιστορικών ριζών, του ορισμού της διατήρησης ιδιωτικότητας στην εξόρυξη δεδομένων, και των μοντέλων των εξόρυξης δεδομένων σε ΔΙΕΓ.
2. **Μια ταξινόμηση των τεχνικών ΔΙΕΓ**: Ερευνήσαμε τις υπάρχουσες τεχνικές ΔΙΕΓ στη βιβλιογραφία, και προτείνουμε μια ταξινόμηση, η οποία περιγράφεται στο κεφάλαιο 4.
3. **Μια βιβλιοθήκη αλγορίθμων**: Για να επιβάλουμε την προστασία γνώσης στη εξόρυξη κανόνων συσχέτισης, προτείνουμε μια βιβλιοθήκη αλγορίθμων. Τέτοιοι αλγόριθμοι σχεδιάζονται λαμβάνοντας υπόψη heuristics για τις τεχνικές ΔΙΕΓ που παρουσιάζονται στο κεφάλαιο 5.

1.5. Δομή της Εργασίας

Το υπόλοιπο της εργασίας είναι οργανωμένο ως εξής:

- Στο κεφάλαιο 2, Για τους κανόνες συσχέτισης, επικεντρωνόμαστε στο πλαίσιο υποστήριξη-εμπιστοσύνη και σε μερικά μέτρα ποσότητας ενδιαφέροντος.

Επιπλέον, παρέχουμε τον ορισμό των ευαίσθητων κανόνων συσχέτισης και των ευαίσθητων δοσοληψιών. Κατόπιν, περιγράφουμε τη διαδικασία προστασίας της ευαίσθητης γνώσης στις βάσεις δεδομένων δοσοληψιών.

- Στο κεφάλαιο 3, προχωρούμε προς την θεμελίωση της ΔΙΕΓ. Πιο συγκεκριμένα, συζητάμε τα προβλήματα του προσδιορισμού της ιδιωτικότητας και πώς η ιδιωτικότητα μπορεί να παραβιαστεί κατά την εξόρυξη γνώσης από δεδομένα. Κατόπιν, περιγράφουμε τις ιστορικές ρίζες και τις βάσεις της ΔΙΕΓ συμπεριλαμβανομένων: α) των ορόσημων ΔΙΕΓ που χαρακτηρίζουν την πρόοδο και την επιτυχία αυτής της νέας έρευνας περιοχή β) του ορισμού της ΔΙΕΓ γ) διαφόρων ενδιαφερόντων σεναρίων σε ΔΙΕΓ και δ) μοντέλων εξόρυξης δεδομένων σε ΔΙΕΓ.
- Στο κεφάλαιο 4, κάνουμε μια ανασκόπηση στην κατάσταση προόδου της έρευνας στη ΔΙΕΓ. Περιγράφουμε τη βασική ιδέα πίσω από τις υπάρχουσες τεχνικές ΔΙΕΓ στη βιβλιογραφία. Κατόπιν, κάνουμε αναφορά στην ταξινόμηση των υπαρχουσών τεχνικών σε τέσσερις σημαντικές κατηγορίες: διαχωρισμός δεδομένων, τροποποίηση δεδομένων, περιορισμός δεδομένων, και ιδιοκτησία δεδομένων.
- Στο κεφάλαιο 5, εισάγουμε τη μέθοδο καθαρισμού δεδομένων που κρύβει τους ευαίσθητους κανόνες συσχέτισης με τη μείωση είτε της υποστήριξης είτε της εμπιστοσύνης αυτών των κανόνων. Η προστασία των ευαίσθητων κανόνων επιτυγχάνεται με την τροποποίηση μερικών δοσοληψιών. Σε μερικές περιπτώσεις, διάφορα αντικείμενα διαγράφονται από μια ομάδα δοσοληψιών με σκοπό την απόκρυψη των ευαίσθητων κανόνων που προέρχονται από εκείνες τις δοσοληψίες. Για να ολοκληρωθεί αυτή η προσέγγιση, παρατίθεται ένα σύνολο αλγορίθμων για τους ευαίσθητους κανόνες. Οι αλγόριθμοι αυτοί κατηγοριοποιούνται σε δύο ομάδες: Διαμοιρασμού-δεδομένων και Διαμοιρασμού-πρότυπων. Στην πρώτη προσέγγιση, ο καθαρισμός ενεργεί στα δεδομένα για να αφαιρέσει ή να κρύψει την ομάδα ευαίσθητων κανόνων συσχέτισης που περιέχουν την ευαίσθητη γνώση. Στην δεύτερη, ο αλγόριθμος καθαρισμού δρα στους κανόνες που εξήχθησαν από μια βάση δεδομένων, αντί στα ίδια τα δεδομένα. Γίνεται επίσης μια ταξινόμηση που καλύπτει αυτές τις δύο κατηγορίες αλγορίθμων καθαρισμού.

- Σε επόμενο κεφάλαιο γίνεται μια επεξήγηση του προγραμμάτων υλοποίησης των αλγορίθμων και βγάζουμε κάποια συμπεράσματα για τα αποτελέσματα εκτέλεσης.

Κεφάλαιο 2

Βασικές Έννοιες της Εξόρυξης Γνώσης

2.1. Βασικές Έννοιες

Στο κεφάλαιο αυτό, κάνουμε μια ανασκόπηση σε βασικές έννοιες που είναι απαραίτητες για την περαιτέρω ανάλυση που πρόκειται να ακολουθήσει με ιδιαίτερη έμφαση στους κανόνες συσχέτισης. Η παράγραφος 2.3 περιέχει τα βασικά της εξόρυξης κανόνων συσχέτισης. Ειδικότερα, ορίζεται το πλαίσιο υποστήριξη-εμπιστοσύνη και αναφέρονται μερικά μέτρα ποσότητας ενδιαφέροντος. Επιπλέον, παρέχουμε τον ορισμό των *ευαίσθητων κανόνων συσχέτισης,* των *περιοριστικών προτύπων* και των *ευαίσθητων δοσοληψιών.* Στη συνέχεια, περιγράφουμε τη διαδικασία της διατήρησης της ευαίσθητης γνώσης στις βάσεις δεδομένων δοσοληψιών.

2.1.1. Μια Ματιά στις Στοιχειώδεις Εργασίες Εξόρυξης Γνώσης

Σε αυτό το τμήμα, περιγράφουμε εν συντομία τη βασική ιδέα πίσω από τις αρχικές στοιχειώδεις εργασίες εξόρυξης γνώσης [9, 10, 18, 22, 27]. Όπως επισημαίνεται από τους Chen et al [9], οι στοιχειώδεις εργασίες εξόρυξης δεδομένων μπορούν να κατηγοριοποιηθούν σύμφωνα με τα ακόλουθα κριτήρια: (α) τα είδη βάσεων δεδομένων, (β) τη γνώση που εξάγεται (π.χ. κανόνες συσχέτισης) και (γ) τις

τεχνικές που χρησιμοποιούνται (π.χ. οδηγημένος-από-δεδομένα ή οδηγημένος-από-ερωτήσεις). Σε αυτήν την εργασία, εστιάζουμε στη δεύτερη κατηγορία (τη γνώση που εξάγεται), οπότε και παρουσιάζουμε τις βασικές εργασίες εξόρυξης αυτής της κατηγορίας:

Περιληπτική παρουσίαση της πληροφορίας: Επίσης αποκαλούμενη και ως χαρακτηρισμός, η περιληπτική παρουσίαση της πληροφορίας αναφέρεται στα γενικά χαρακτηριστικά ή τα χαρακτηριστικά γνωρίσματα μιας κλάσης δεδομένων. Μερικές φορές, ο στόχος είναι να εξαχθούν απλά τα πρότυπα που περιγράφουν ένα υποσύνολο των δεδομένων. Τα δεδομένα που αντιστοιχούν στην κλάση ή το υποσύνολο που καθορίζει ο χρήστης συλλέγονται με ερωτήσεις σε βάσεις δεδομένων. Παραδείγματος χάριν, για να αναλυθούν τα γνωρίσματα ορισμένων προϊόντων των οποίων οι πωλήσεις αυξήθηκαν κατά 15% στον περασμένο χρόνο, τα δεδομένα σχετικά με τέτοια προϊόντα μπορούν να συλλεχθούν με την εκτέλεση μιας ερώτησης SQL.

Προβλεπτικό μοντέλο: Ο στόχος αυτής της στοιχειώδους εργασίας εξόρυξης είναι να προβλεφθούν μερικά γνωρίσματα σε μια βάση δεδομένων βασισμένη σε άλλα γνωρίσματα. Το στοχευόμενο γνώρισμα λέγεται κλάση. Αυτό το μοντέλο είναι γνωστό και ως κατηγοριοποίηση και μπορεί να χρησιμοποιηθεί για να προβλέψει τις τιμές της κλάσης για τα νέα δεδομένα. Παραδείγματος χάριν, λαμβάνοντας υπόψη ένα σύνολο δεδομένων, μόνο ένα μέρος από αυτό χρησιμοποιείται για να παραγάγει ένα προβλεπτικό μοντέλο. Αυτό το μέρος αναφέρεται ως δεδομένα εκπαίδευσης (training dataset). Μεμονωμένες πλειάδες που αποτελούν το σύνολο δεδομένων εκπαίδευσης αναφέρονται ως δείγματα εκπαίδευσης και επιλέγονται τυχαία από το σύνολο των δειγμάτων. Δεδομένου ότι η ετικέτα κλάσης κάθε δείγματος εκπαίδευσης παρέχεται, αυτό το βήμα είναι γνωστό ως *εποπτευόμενη εκμάθηση*. Το υπόλοιπο μέρος, που καλείται σύνολο δεδομένων εξέτασης, διατηρείται για την αξιολόγηση της προβλεπτικής ικανότητας και απόδοσης του μοντέλου σε νέα, απαρατήρητα δεδομένα (δηλαδή για να υπολογίσει την ισχύ των προτύπων στα νέα δεδομένα).

Συσταδοποίηση: Επίσης γνωστή ως κατάτμηση, η συσταδοποίηση σχετίζεται με την ομαδοποίηση των αντικειμένων σε κλάσεις παρόμοιων αντικειμένων. Λαμβάνοντας υπόψη ένα σύνολο δεδομένων, η εργασία είναι να χωριστούν τα δεδομένα στις νέες κλάσεις (συστάδες). Ο στόχος είναι να επιτευχθεί υψηλή ομοιότητα μεταξύ των

αντικειμένων μέσα στις μεμονωμένες συστάδες (interclass ομοιότητα) και η χαμηλή ομοιότητα μεταξύ των αντικειμένων που ανήκουν σε διαφορετικές συστάδες (intraclass ομοιότητα). Σε αντίθεση με το προβλεπτικό μοντέλο που αναλύει τα δεδομένα ανά ετικέτα κλάσης, η συσταδοποίηση αναλύει τα αντικείμενα δεδομένων χωρίς διαβούλευση μιας γνωστής ετικέτας κλάσης. Για αυτόν τον λόγο, η συσταδοποίηση είναι επίσης γνωστή ως *μη-εποπτευόμενη εκμάθηση*. Η συσταδοποίηση παίζει έναν σημαντικό ρόλο στις εφαρμογές εξόρυξης γνώσης όπως στην εξερεύνηση επιστημονικών δεδομένων, το μάρκετινγκ, τα ιατρικά διαγνωστικά, και την υπολογιστική βιολογία.

Κανόνες συσχέτισης: Η ανάλυση συσχέτισης είναι η ανακάλυψη των κανόνων συσχέτισης περιγράφοντας τις ενδιαφέρουσες σχέσεις μεταξύ των αντικειμένων που συγκεντρώνονται σε έναν σημαντικό αριθμό παραδειγμάτων. Η ανάλυση καλαθιών αγοράς είναι ένα ισχυρό κίνητρο για την ανάπτυξη της εξόρυξης κανόνων συσχέτισης. Η διαδικασία εύρεσης κανόνων συσχέτισης εκτελείται σε δύο βήματα. Κατ' αρχάς, όλα τα συχνά itemsets βρίσκονται, όπου ένα itemset λέγεται ότι είναι συχνό εάν εμφανίζεται τουλάχιστον σε ένα δεδομένο ποσοστό s (αποκαλούμενο υποστήριξη) όλων των δοσοληψιών. Κατόπιν, οι κανόνες συσχέτισης βρίσκονται στη μορφή $X \Rightarrow Y$, όπου X και Y είναι συχνά . Οι ισχυροί κανόνες συσχέτισης προέρχονται από τα συχνά itemsets και περιορίζονται από μια ελάχιστη εμπιστοσύνη, δηλ. το ποσοστό των δοσοληψιών που περιέχουν το X που περιέχουν επίσης το Y. Ο ορισμός του πλαισίου υποστήριξη-εμπιστοσύνη ακολουθεί σε επόμενη παράγραφο.

2.2. Τα Βασικά της Εξόρυξης Κανόνων Συσχέτισης

2.2.1. Το πλαίσιο Υποστήριξη-Εμπιστοσύνη (Support-Confidence)

Ένα από τα σημαντικότερα ζητήματα που μελετούνται στην εξόρυξη γνώσης είναι η διαδικασία ανακάλυψης κανόνων συσχέτισης από μεγάλες βάσεις δεδομένων. Οι περισσότεροι από τους υπάρχοντες αλγορίθμους για τους κανόνες συσχέτισης στηρίζονται στο πλαίσιο υποστήριξη-εμπιστοσύνη.

Τυπικά, οι κανόνες συσχέτισης ορίζονται ως εξής:

Έστω $I = \{i_1, i_2, \ldots, i_n\}$ είναι ένα σύνολο αντικειμένων. Έστω D μία βάση δεδομένων δοσοληψιών, όπου κάθε δοσοληψία t είναι ένα στοιχειοσύνολο έτσι ώστε $t \subseteq I$. Ένας

μοναδικός αναγνωριστής, αποκαλούμενος TID, συνδέεται με κάθε δοσοληψία. Μια δοσοληψία t υποστηρίζει το X, ένα σύνολο αντικειμένων στο I, εάν $X \subset t$. Ένας κανόνας συσχέτισης είναι μια επαγωγή της μορφής $X \Rightarrow Y$, όπου $X \subset I, Y \subset I$ *και* $X \cap Y = \varnothing$. Κατά συνέπεια, λέμε ότι ένας κανόνας $X \Rightarrow Y$ κρατά στη βάση δεδομένων D με εμπιστοσύνη c εάν $\frac{|X \cup Y|}{|X|} > c$, όπου |A| είναι ο αριθμός εμφανίσεων του συνόλου αντικειμένων A στο σύνολο δοσοληψιών της D. Ομοίως, λέμε ότι ένας κανόνας $X \Rightarrow Y$ κρατά στη βάση δεδομένων D με υποστήριξη s εάν $\frac{|X \cup Y|}{N} > s$, όπου το N είναι ο αριθμός δοσοληψιών στη D.

Ενώ η υποστήριξη είναι ένα μέτρο της συχνότητας ενός κανόνα, η εμπιστοσύνη είναι ένα μέτρο της δύναμης της σχέσης μεταξύ των συνόλων αντικειμένων.

2.2.2. Ευαίσθητοι Κανόνες, Περιοριστικά Πρότυπα και Ευαίσθητες Συναλλαγές

Η προστασία της ευαίσθητης γνώσης στις βάσεις δεδομένων δοσοληψιών είναι η διαδικασία απόκρυψης ενός συνόλου κανόνων συσχέτισης που περιέχουν ευαίσθητη γνώση. Αναφερόμαστε σε αυτούς τους κανόνες ως *ευαίσθητους κανόνες συσχέτισης* και ορίζονται ως εξής:

> **Ορισμός 1 (Ευαίσθητοι Κανόνες Συσχέτισης)**: *Έστω D μια βάση δεδομένων δοσοληψιών, R είναι ένα σύνολο όλων των κανόνων συσχέτισης που μπορούν να εξαχθούν από την D βασιζόμενοι σε μια ελάχιστη υποστήριξη s, και R_h είναι ένα σύνολο κανόνων υποστήριξης απόφασης που πρέπει να κρυφτούν σύμφωνα με κάποιες πολιτικές ασφάλειας. Ένα σύνολο κανόνων συσχέτισης, S_R, λέγεται ότι είναι ευαίσθητο αν και μόνον αν $S_R \subset R$ και το S_R θα παρήγαγε το σύνολο R_h. $\sim S_R$ είναι το σύνολο των μη-ευαίσθητων κανόνων συσχέτισης και είναι τέτοιο ώστε $\sim S_R \cup S_R = R$.*

Ο παραπάνω ορισμός μπορεί να προσαρμοστεί στα πλαίσια των συχνών στοιχειοσυνόλων, αφού η εξαγωγή των κανόνων συσχέτισης στηρίζεται στα συχνά στοιχειοσύνολα. Έτσι, προκύπτει ο ορισμός των περιοριστικών προτύπων:

Ορισμός 2 (Περιοριστικά Πρότυπα): *Έστω D μια βάση δεδομένων δοσοληψιών, P είναι ένα σύνολο όλων των συχνών προτύπων που μπορούν να εξαχθούν από την D, και R_h είναι ένα σύνολο κανόνων υποστήριξης απόφασης που πρέπει να κρυφτούν σύμφωνα με κάποιες πολιτικές ασφάλειας. Ένα σύνολο προτύπων, R_P, λέγεται ότι είναι περιοριστικό αν και μόνον αν $R_P \subset P$ και το R_P θα παρήγαγε το σύνολο R_h. $\sim R_P$ είναι το σύνολο των μη-περιοριστικών προτύπων και είναι τέτοιο ώστε $\sim R_P \cup R_P = P$.*

Μια ομάδα ευαίσθητων κανόνων συσχέτισης εξάγεται από μια βάση δεδομένων *D* βασισμένη σε μια ειδική ομάδα δοσοληψιών. Αναφερόμαστε σε αυτές τις δοσοληψίες ως ευαίσθητες δοσοληψίες και ορίζονται ως εξής:

Ορισμός 3 (Ευαίσθητες Συναλλαγές): *Έστω το T είναι ένα σύνολο όλων των δοσοληψιών σε μια βάση δεδομένων δοσοληψιών D και το S_R είναι ένα σύνολο ευαίσθητων κανόνων συσχέτισης που εξάγονται από την D. Ένα σύνολο δοσοληψιών λέγεται ότι είναι ευαίσθητο, και δηλώνεται ως S_T, εάν $S_T \subset T$ και $\forall t \in S_T, \exists\, sr \in S_R$ τέτοιο ώστε $items(sr) \subset t$*

2.2.3. Η Διαδικασία Προστασίας Ευαίσθητης Γνώσης

Η διαδικασία προστασίας της ευαίσθητης γνώσης στις βάσεις δεδομένων δοσοληψιών αποτελείται από δύο σημαντικά βήματα: *καταστολή αναγνωριστή* και *καθαρισμός* , όπως φαίνεται και στην Εικόνα 2.

Εικόνα 2: Τα σημαντικότερα βήματα της διαδικασίας προστασίας της ευαίσθητης γνώσης

Βήμα 1: Καταστολή Αναγνωριστή

Το πρώτο βήμα είναι η καταστολή των αναγνωριστών (π.χ. IDs, ονόματα, κ.λ.π.) από τα δεδομένα που μοιράζονται. Η διαδικασία αφαίρεσης αναγνωριστών επιτρέπει στους ιδιοκτήτες βάσεων δεδομένων να αποκαλύψουν τη συμπεριφορά αγοράς των πελατών τους χωρίς αποκάλυψη των ταυτοτήτων τους [32]. Για να ολοκληρωθεί αυτό, οι ιδιοκτήτες βάσεων δεδομένων πρέπει να μετασχηματίσουν τα δεδομένα σε μορφές κατάλληλες για τη εξόρυξη.

Μετά από την αφαίρεση των identifiers, τα επιλεγμένα δεδομένα που υποβάλλονται στην εξόρυξη, μπορούν να καταχωρηθούν σε έναν ενιαίο πίνακα, αποκαλούμενο επίσης βάση δεδομένων δοσοληψιών. Η αφαίρεση των αναγνωριστών μπορεί να προστατέψει προσωπικές πληροφορίες, εντούτοις αμφισβητείται ότι η διαδικασία αυτή παρέχει πλήρη ιδιωτικότητα.

Βήμα 2: Καθαρισμός

Μετά από την αφαίρεση των αναγνωριστών από τα δεδομένα, ο στόχος είναι να μπορέσουμε να αποκρύψουμε αποτελεσματικά την ευαίσθητη γνώση, η οποία αντιπροσωπεύεται από τους ευαίσθητους κανόνες.

Στις περισσότερες περιπτώσεις, η έννοια της ευαίσθητης γνώσης δεν μπορεί να μαθευτεί εκ των προτέρων. Κι αυτό γιατί η διαδικασία αναγνώρισης της ευαίσθητης γνώσης απαιτεί την ανθρώπινη αξιολόγηση των ενδιάμεσων αποτελεσμάτων πριν από ττο διαμοιρασμό των δεδομένων για τη εξόρυξη. Σε αυτά τα πλαίσια, η ευαίσθητη γνώση αντιπροσωπεύεται από μια ειδική ομάδα κανόνων καλούμενων ευαίσθητοι κανόνες συσχέτισης.

Ένας αποτελεσματικός τρόπος απόκρυψης των ευαίσθητ ευαίσθητων κανόνω μετασχηματισμός μιας βάσης δεδομένων δοσοληψιών σε μια νέα που κρύβει τους ευαίσθητους κανόνες διατηρώντας τους περισσότερους από τους μη-ευαίσθητους. Η βάση δεδομένων καλείται καθαρισμένη βάση δεδομένων. Η διαδικασία sanitization

ενεργεί στα δεδομένα τροποποιώντας μερικές δοσοληψίες. Σε μερικές περιπτώσεις, διάφορα αντικείμενα διαγράφονται από μια ομάδα δοσοληψιών (ευαίσθητες δοσοληψίες) με σκοπό την απόκρυψη των ευαίσθητων κανόνων που προέρχονται από εκείνες τις δοσοληψίες. Με αυτό τον τρόπο, η υποστήριξη αυτών των ευαίσθητων κανόνων μειώνεται κάτω από ένα ορισμένο κατώφλι ευαισθησίας ψ. Ένας άλλος τρόπος απόκρυψης των ευαίσθητων κανόνων είναι να προστεθούν νέα αντικείμενα σε μερικές δοσοληψίες για να αλλάξει (μειωθεί) η εμπιστοσύνη των ευαίσθητων κανόνων. Παραδείγματος χάριν, σε έναν κανόνα $X \Rightarrow Y$, εάν τα αντικείμενα προστίθενται στο πρότερο μέρος X αυτού του κανόνα στις δοσοληψίες που υποστηρίζουν το X και όχι το Y, τότε η εμπιστοσύνη ενός τέτοιου κανόνα μειώνεται.

Αν και η διαδικασία καθαρισμού εκτελείται για να κρύψει τους ευαίσθητους κανόνες μόνο, η παρενέργεια αυτής της διαδικασίας είναι ότι μπορεί να κρύψει και μερικούς μη-ευαίσθητους κανόνες. Με τη διαγραφή μερικών αντικειμένων σε μια ομάδα δοσοληψιών, μειώνεται επίσης η υποστήριξη ή ακόμα και η εμπιστοσύνη των μη-ευαίσθητων κανόνων. Επομένως, ο καθαρισμός των αλγορίθμων πρέπει να εστιάσει στην απόκρυψη των ευαίσθητων κανόνων και, συγχρόνως, τη μείωση των παρενεργειών στους μη-ευαίσθητους κανόνες όσο το δυνατόν περισσότερο.

Κεφάλαιο 3

Θεμελίωση της Διατήρησης Ιδιωτικότητας

Στο σύντομο αυτό κεφάλαιο, θα αναφερθούμε στα θεμέλια της Διατήρησης Ιδιωτικότητας στην Εξόρυξη Γνώσης (ΔΙΕΓ). Πιο συγκεκριμένα, στην παράγραφο 3.1 γίνεται λόγος για τις διαφορετικές έννοιες της διατήρησης ιδιωτικότητας και πώς η ιδιωτικότητα μπορεί να παραβιαστεί στην εξόρυξη γνώσης. Στην παράγραφο 3.2 εισάγονται οι ιστορικές βάσεις της ΔΙΕΓ.

3.1. Οι Διαφορετικές Έννοιες της Διατήρησης Ιδιωτικότητας

3.1.1. Προβλήματα στον Ορισμό της Ιδιωτικότητας

Ανά τα χρόνια πολλοί διαφορετικοί ορισμοί έχουν δοθεί στην ιδιωτικότητα, οι οποίοι ποικίλλουν σύμφωνα με τα πλαίσια, τον πολιτισμό, και το περιβάλλον. Γενικά όμως όλοι οι ορισμοί προτείνουν ότι η ιδιωτικότητα εμφανίζεται ως μια κοινωνική και πολιτιστική έννοια. Εντούτοις, με την απανταχού παρουσία των υπολογιστών και την εμφάνιση του Παγκόσμιου Ιστού, η ιδιωτικότητα έχει γίνει επίσης ένα ψηφιακό πρόβλημα.. Με την επανάσταση του Ιστού και την εμφάνιση της εξόρυξης δεδομένων, οι ανησυχίες για παραβίαση της ιδιωτικότητας έχουν θέσει τεχνικές προκλήσεις πολύ διαφορετικές από εκείνες που εμφανίστηκαν πριν από την εποχή πληροφοριών. Στην εποχή της τεχνολογίας πληροφοριών, η ιδιωτικότητα αναφέρεται

στο δικαίωμα των χρηστών να κρύψουν τις προσωπικές πληροφορίες τους και να έχουν κάποιο βαθμό ελέγχου της χρήσης οποιωνδήποτε προσωπικών πληροφοριών που αποκαλύπτονται σε άλλους [15, 1, 28].

Σαφώς, η έννοια της ιδιωτικότητας είναι συχνά πιο σύνθετη από όσο την αντιλαμβανόμαστε. Ειδικότερα, στην εξόρυξη δεδομένων, ο ορισμός της διατήρησης ιδιωτικότητας είναι ακόμα πιο ασαφής, και υπάρχει πολύ λίγη βιβλιογραφία σχετική με αυτό το θέμα. Μια αξιοσημείωτη εξαίρεση είναι η δουλειά που παρουσιάζεται στο [13], όπου η ΔΙΕΓ ορίζεται ως «η εξαγωγή έγκυρων αποτελεσμάτων εξόρυξης γνώσης χωρίς την γνώση των υποκρυπτόμενων τιμών των δεδομένων». Παρόλα αυτά, κάθε υπάρχουσα τεχνική ΔΙΕΓ έχει τον δικό της ορισμό. Η πρωταρχική ανησυχία για τη ΔΙΕΓ είναι ότι οι αλγόριθμοι εξόρυξης πρέπει να αναλύονται για τις δευτερεύοντες παρενέργειες που υφίστανται στην ιδιωτικότητα δεδομένων. Επομένως ο ορισμός που υιοθετούμε είναι [48, 13] – «*Η ΔΙΕΓ περιλαμβάνει τον διπλό στόχο να ανταποκρίνεται στις απαιτήσεις ιδιωτικότητας και να παρέχει έγκυρα αποτελέσματα εξόρυξης γνώσης*». Ο ορισμός αυτός δίνει έμφαση στο δίλημμα της εξισορρόπησης μεταξύ διατήρησης ιδιωτικότητας και κοινοποίησης γνώσης.

3.1.2. Παραβίαση Ιδιωτικότητας στην Εξόρυξη Γνώσης

Για να αντιληφθούμε την ιδιωτικότητα στην εξόρυξη γνώσης πρέπει αρχικά να αντιληφθούμε πώς αυτή μπορεί να παραβιαστεί και όλα τα δυνατά μέσα για την παραβίαση. Γενικά, ένας σημαντικός παράγοντας που συμβάλλει στην παραβίαση ιδιωτικότητας στην εξόρυξη δεδομένων είναι η κακή χρήση των δεδομένων.

Η ιδιωτικότητα των χρηστών μπορεί να παραβιαστεί με διαφορετικούς τρόπους και με διαφορετικές προθέσεις. Αν και η εξόρυξη δεδομένων μπορεί να είναι εξαιρετικά πολύτιμη σε πολλές εφαρμογές (π.χ. επιχειρήσεις, ιατρική ανάλυση, κ.λ.π.), μπορεί επίσης, ελλείψει των επαρκών μέτρων προστασίας, να παραβιάσει την ενημερωτική ιδιωτικότητα. Η ιδιωτικότητα μπορεί να παραβιαστεί εάν τα προσωπικά δεδομένα χρησιμοποιούνται για άλλους λόγους από τους συμφωνημένους με την αρχική δοσοληψία μεταξύ ενός ατόμου και μιας οργάνωσης οπότε και συλλέχθησαν οι πληροφορίες.

Μια από τις πηγές παραβίασης της ιδιωτικότητας καλείται *μαγνήτες δεδομένων* [45]. Οι μαγνήτες δεδομένων είναι τεχνικές και εργαλεία που χρησιμοποιούνται για να συλλέξουν προσωπικά δεδομένα. Τα παραδείγματα των

μαγνητών δεδομένων περιλαμβάνουν συλλογή πληροφοριών μέσω της απευθείας σύνδεσης εγγραφής, που προσδιορίζει τους χρήστες μέσω των διευθύνσεων IP, τα λογισμικά download που απαιτούν την εγγραφή, και έμμεσα συλλογή των πληροφοριών για τη δευτεροβάθμια χρήση. Σε πολλές περιπτώσεις, οι χρήστες είτε μπορούν είτε όχι να γνωρίζουν ότι οι πληροφορίες συλλέγονται ή δεν ξέρουν πώς εκείνες οι πληροφορίες συλλέγονται [16, 34]. Θεωρείται χειρότερη η παραβίαση ιδιωτικότητας που προκαλείται από τη δευτεροβάθμια χρήση των δεδομένων όταν τα άτομα δεν γνωρίζουν για τις «παρασκηνιακές» τεχνικές εξόρυξης δεδομένων [29]. Πιο συγκεκριμένα, τα συλλεχθέντα προσωπικά δεδομένα μπορούν να χρησιμοποιηθούν για τη δευτεροβάθμια χρήση κατά ένα μεγάλο μέρος πέρα από τους νόμους ελέγχου και ιδιωτικότητας των χρηστών. Αυτό το σενάριο έχει οδηγήσει σε μια ανεξέλεγκτη παραβίαση ιδιωτικότητας όχι λόγω αυτής καθαυτής της εξόρυξης δεδομένων, αλλά κυρίως λόγω της κακής χρήσης των δεδομένων.

3.2. Τα Θεμέλια της ΔΙΕΓ

Λόγω του ότι η εξόρυξη γνώσης από δεδομένα έχει υιοθετηθεί ευρέως από τις δημόσιες και ιδιωτικές επιχειρήσεις, το θέμα της ΔΙΕΓ έχει λάβει ιδιαίτερη προσοχή.

3.2.1. Ορισμός της Διατήρησης Ιδιωτικότητας στην Εξόρυξη Γνώσης

Γενικά, η διατήρηση ιδιωτικότητας εμφανίζεται σε δύο σημαντικές διαστάσεις: προσωπικές πληροφορίες χρηστών και πληροφορίες σχετικά με τη συλλογική δραστηριότητά τους. Αναφερόμαστε στην πρώτη ως *μεμονωμένη διατήρηση ιδιωτικότητας* και την τελευταία ως *συλλογική διατήρηση ιδιωτικότητας*.

- **Μεμονωμένη διατήρηση ιδιωτικότητας**: Ο πρωταρχικός στόχος της ιδιωτικότητας δεδομένων είναι η προστασία των προσωπικών πληροφοριών. Γενικά, οι πληροφορίες θεωρούνται προσωπικά αναγνωρίσιμες από ένα μεμονωμένο πρόσωπο. Κατά συνέπεια, όταν υποβάλλονται τα προσωπικά δεδομένα στη εξόρυξη, οι τιμές ιδιοτήτων που συνδέονται με τα άτομα είναι ιδιωτικές και πρέπει να προστατευθούν από την κοινοποίηση.
- **Συλλογική διατήρηση ιδιωτικότητας**: Η προστασία των προσωπικών δεδομένων μπορεί να μην είναι αρκετή. Μερικές φορές, χρειάζεται προστασία

από την εκμάθηση της ευαίσθητης γνώσης που αντιπροσωπεύει τις δραστηριότητες μιας ομάδας. Αναφερόμαστε σε αυτό το είδος προστασίας της ευαίσθητης γνώσης ως συλλογική διατήρηση ιδιωτικότητας. Ο στόχος εδώ είναι αρκετά παρόμοιος με εκείνον για τις στατιστικές βάσεις δεδομένων, στις οποίες οι μηχανισμοί ελέγχου ασφαλείας παρέχουν τις συνολικές πληροφορίες για τις ομάδες (πληθυσμός) και, συγχρόνως, αποτρέπουν την κοινοποίηση των εμπιστευτικών πληροφοριών για τα άτομα. Εντούτοις, αντίθετα από το τι συμβαίνει στις στατιστικές βάσεις δεδομένων, ένας άλλος στόχος της συλλογικής διατήρησης ιδιωτικότητας είναι να διατηρηθούν (αποκρυφθούν) τα στρατηγικά πρότυπα τα οποία είναι κυρίαρχα για τις στρατηγικές αποφάσεις. Με άλλα λόγια, ο στόχος είναι εδώ όχι μόνο να προστατευθούν οι προσωπικά αναγνωρίσιμες πληροφορίες αλλά και μερικά πρότυπα και τάσεις που υποτίθεται ότι δεν θα ανακαλυφθούν

Στην περίπτωση της συλλογικής διατήρησης ιδιωτικότητας, οι οργανισμοί πρέπει να αντιμετωπίσουν μερικές ενδιαφέρουσες συγκρούσεις. Παραδείγματος χάριν, όταν υποβάλλονται οι προσωπικές πληροφορίες σε ανάλυση, οι διαδικασίες που παράγουν τα νέα γεγονότα προϊόντων για τα πρότυπα αγορών των χρηστών, χόμπι, ή προτιμήσεις, αυτά τα γεγονότα θα μπορούσαν να χρησιμοποιηθούν στα *συστήματα υποδείξεων* για να προβλέπουν ή να επηρεάσουν τα μελλοντικά πρότυπα αγορών τους. Γενικά, αυτό το σενάριο είναι εποικοδομητικό και για τους χρήστες και για τους οργανισμούς. Εντούτοις, όταν μοιράζονται οι οργανισμοί τα δεδομένα σε ένα πρόγραμμα συνεργασίας, ο στόχος είναι όχι μόνο να προστατευθούν προσωπικά αναγνωρίσιμες πληροφορίες, αλλά και να προστατευθούν μερικά στρατηγικά πρότυπα. Στον επιχειρησιακό κόσμο, τέτοια πρότυπα περιγράφονται ως γνώση που μπορεί να παρέχει ανταγωνιστικά πλεονεκτήματα, και επομένως πρέπει να προστατευθεί. Πιο προκλητική είναι η προστασία της γνώσης που ανακαλύπτεται από τις εμπιστευτικές πληροφορίες (π.χ. ιατρικές, οικονομικές και ποινικών μητρώων). Η απουσία μέτρων προστασίας της ιδιωτικότητας μπορεί εξίσου να θέσει σε κίνδυνο την ιδιωτικότητα των ατόμων. Ενώ η παραβίαση της μεμονωμένης ιδιωτικότητας είναι σαφής, η παραβίαση της συλλογικής ιδιωτικότητας μπορεί να οδηγήσει στην παραβίαση της ιδιωτικότητας του ατόμου.

3.2.2. Μερικά Χαρακτηριστικά Σενάρια σε ΔΙΕΓ

Στην παράγραφο αυτή παρουσιάζουμε δύο χαρακτηριστικά πραγματικά παραδείγματα όπου η ΔΙΕΓ θέτει διαφορετικούς φραγμούς, καθώς επίσης περιγράφουμε τις γενικές παραμέτρους χαρακτηρισμού των σεναρίων.

Σενάριο 1: Ένα νοσοκομείο μοιράζεται μερικά στοιχεία για ερευνητικούς λόγους (π.χ. σχετικά με μια ομάδα ασθενών που έχουν μια παρόμοια ασθένεια). Ο διοικητής ασφάλειας του νοσοκομείου μπορεί να καταστείλει κάποιο αναγνωριστικό (π.χ. όνομα, διεύθυνση, τηλεφωνικός αριθμός, κ.λ.π.) από τα αρχεία ασθενών για να καλύψει τις απαιτήσεις ιδιωτικότητας. Εντούτοις, τα δημοσιευμένα στοιχεία δεν μπορούν να προστατευθούν πλήρως. Ένα αρχείο ασθενούς είναι πιθανόν να περιέχει άλλες πληροφορίες που μπορούν να συνδεθούν με άλλα σύνολα δεδομένων για να αναγνωρίσουν ξανά τα άτομα ή τις οντότητες [46]. Πώς μπορούμε να προσδιορίσουμε τις ομάδες ασθενών με μια παρόμοια ασθένεια χωρίς αποκάλυψη των τιμών των ιδιοτήτων που συνδέονται με αυτούς;

Σενάριο 2: Δύο ή περισσότερες επιχειρήσεις έχουν ένα πολύ μεγάλο σύνολο αρχείων με δεδομένα των δραστηριοτήτων αγοράς των πελατών τους. Αυτές οι επιχειρήσεις αποφασίζουν να διευθύνουν συνεταιριστικά την εξόρυξη κανόνων συσχέτισης στα σύνολα δεδομένων τους με σκοπό το αμοιβαίο όφελός τους, δεδομένου ότι αυτή η συνεργασία τους αποφέρει ένα πλεονέκτημα έναντι των άλλων ανταγωνιστών. Εντούτοις, μερικές από αυτές τις επιχειρήσεις μπορούν να μην θελήσουν να μοιραστούν μερικά στρατηγικά πρότυπα που κρύβονται μέσα στα στοιχεία τους (επίσης αποκαλούμενα ευαίσθητοι κανόνες συσχέτισης) με τα άλλα συμβαλλόμενα μέρη. Θα επιθυμούσαν λοιπόν να μετασχηματίσουν τα στοιχεία τους κατά τέτοιο τρόπο ώστε αυτοί οι ευαίσθητοι κανόνες συσχέτισης να μην μπορούν να ανακαλυφθούν. Είναι δυνατό για αυτές τις επιχειρήσεις να ωφεληθούν από μια τέτοια συνεργασία με το διαμοιρασμό των στοιχείων τους διατηρώντας μερικούς ευαίσθητους κανόνες συσχέτισης;

Σημειώνεται ότι τα παραπάνω σενάρια περιγράφουν τα διαφορετικά προβλήματα διατήρησης ιδιωτικότητας. Κάθε σενάριο θέτει ένα σύνολο προκλήσεων. Παραδείγματος χάριν, το σενάριο 1 είναι ένα χαρακτηριστικό παράδειγμα της

διατήρησης ιδιωτικότητας του ατόμου, ενώ το σενάριο 2 αναφέρεται στη συλλογική διατήρηση ιδιωτικότητας.

Πώς μπορούμε όμως να χαρακτηρίσουμε τα σενάρια σε ΔΙΕΓ; Μια εναλλακτική είναι να περιγραφούν από την άποψη των γενικών παραμέτρων. Στο [14], μερικές παράμετροι προτείνονται ως εξής:

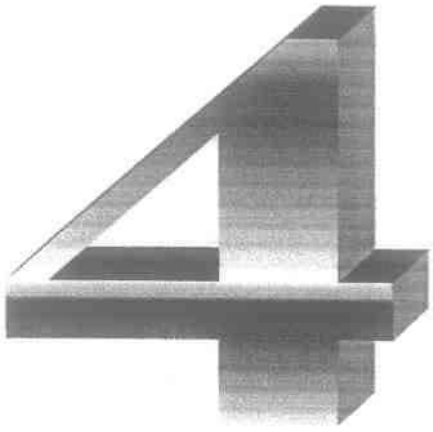
Έκβαση: Αναφέρεται στα επιθυμητά αποτελέσματα εξόρυξης δεδομένων. Παραδείγματος χάριν, κάποιος μπορεί να ψάξει τους κανόνες συσχέτισης που προσδιορίζουν τις σχέσεις μεταξύ των ιδιοτήτων, ή τις σχέσεις μεταξύ των συμπεριφορών αγοράς των πελατών όπως στο σενάριο 2, ή μπορεί ακόμη και να θελήσει να συσταδοποιήσει τα στοιχεία όπως στο σενάριο 1.

Διαμοιρασμός στοιχείων: Πώς διαθέτονται τα στοιχεία για την εξόρυξη: είναι συγκεντρωμένα ή διανέμονται σε πολλές περιοχές; Στην περίπτωση των στοιχείων που διανέμονται σε πολλές περιοχές, οι οντότητες περιγράφονται με το ίδιο σχήμα σε όλες τις περιοχές (οριζόντιες κατατμήσεις), ή οι διαφορετικές περιοχές περιέχουν διαφορετικές ιδιότητες για μια οντότητα (κάθετες κατατμήσεις);

Διατήρηση Ιδιωτικότητας: Ποιες είναι οι απαιτήσεις διατήρησης ιδιωτικότητας; Εάν η ανησυχία είναι απλώς ότι οι τιμές που συνδέονται με μια μεμονωμένη οντότητα δεν πρέπει να εκδοθούν (π.χ. προσωπικές πληροφορίες), τότε τεχνικές πρέπει να εστιάσουν στην προστασία αυτών των πληροφοριών. Σε άλλες περιπτώσεις, η «ευαίσθητη γνώση» δεν μπορεί να μαθευτεί εκ των προτέρων. Αυτό θα οδηγούσε στην ανθρώπινη αξιολόγηση των ενδιάμεσων αποτελεσμάτων πριν διατεθούν τα στοιχεία για την εξόρυξη.

3.3. Περίληψη

Σε αυτό το κεφάλαιο, καθορίσαμε μερικές θεμελιώδεις έννοιες της ΔΙΕΓ. Αν και η εργασία μας που περιγράφεται εδώ είναι προκαταρκτική και εννοιολογικής φύσης, υποστηρίζουμε ότι είναι μια ζωτικής σημασίας προϋπόθεση για την τυποποίηση της ΔΙΕΓ. Η απουσία συναίνεσης στους ορισμούς της διατήρησης, τις πολιτικές και τις απαιτήσεις ιδιωτικότητας για την ανάπτυξη των νέων τεχνικών ΔΙΕΓ οδηγεί στη σύγχυση μεταξύ των υπεύθυνων για την ανάπτυξη, των επαγγελματιών, και άλλων ενδιαφερόμενων σε αυτήν την τεχνολογία.

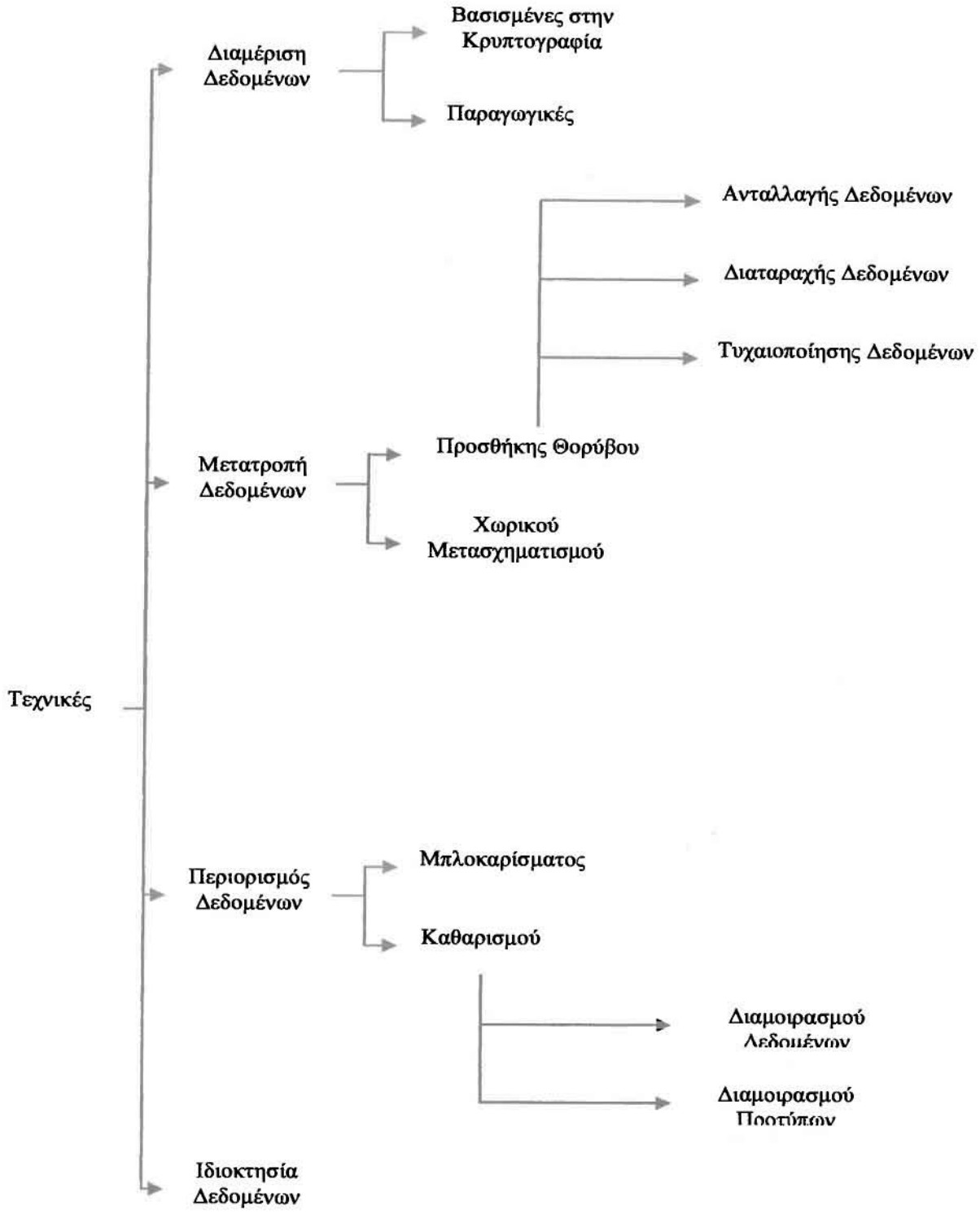


Κεφάλαιο 4

Τεχνικές Διατήρησης Ιδιωτικότητας στην Εξόρυξη Γνώσης

Όσον αφορά τη διατήρηση ιδιωτικότητας στην εξόρυξη γνώσης (ΔΙΕΓ) έχουν προκύψει αρκετά ζητήματα. Διάφορες επιτυχείς τεχνικές έχουν προταθεί για να επιστρέψουν έγκυρα αποτελέσματα εξόρυξης γνώσης διατηρώντας τα μέτρα προστασίας της ιδιωτικότητας. Σε αυτό το κεφάλαιο, κάνουμε μια αναφορά στις υπάρχουσες τεχνικές ΔΙΕΓ που προκύπτουν από τη βιβλιογραφία. Ταξινομούμε αυτές τις τεχνικές σε τέσσερις σημαντικές κατηγορίες: διαμέριση δεδομένων, μετατροπή δεδομένων, περιορισμός δεδομένων και ιδιοκτησία δεδομένων, όπως φαίνεται στην Εικόνα 3. Οι τεχνικές διαμέρισης δεδομένων σχεδιάζονται για να εξετάσουν μερικά σενάρια στα οποία τα διαθέσιμα δεδομένα για την εξόρυξη χωρίζονται σε πολλαπλές περιοχές (συμβαλλόμενα μέρη). Αντί της διαμοιρασμού των αρχικών δεδομένων μεταξύ των συμβαλλόμενων μερών, μόνο τα αποτελέσματα εξόρυξης δεδομένων είναι γνωστά σε κάθε συμβαλλόμενο μέρος. Γίνεται αναφορά σε αυτές τις τεχνικές στην παράγραφο 4.1. Όταν τα δεδομένα πηγής πρόκειται να μοιραστούν ή να ανταλλαχθούν, οι τεχνικές μετατροπής δεδομένων και περιορισμού δεδομένων είναι απαραίτητες. Οι τεχνικές μετατροπής δεδομένων μετατρέπουν μια αρχική βάση δεδομένων σε μια νέα η οποία υποβάλλεται στην εξόρυξη. Εξετάζουμε αυτές τις τεχνικές στην παράγραφο 4.2. Οι βασισμένες στον περιορισμό δεδομένων τεχνικές

εξετάζονται στην παράγραφο 4.3. Για να διατηρήσουν τις ιδιωτικές πληροφορίες σε μια βάση δεδομένων, αυτές οι τεχνικές καταστέλλουν κάποιες πληροφορίες από τα δεδομένα πριν την εξόρυξη. Η τέταρτη κατηγορία τεχνικών ΔΙΕΓ καλείται ιδιοκτησία δεδομένων. Αυτές οι τεχνικές στοχεύουν στην προστασία της ιδιοκτησίας των δεδομένων από τους ανθρώπους για τους οποίους τα δεδομένα συλλέχθησαν. Κατά το διαμοιρασμό εμπιστευτικών δεδομένων, αυτές οι τεχνικές μπορούν επίσης να χρησιμοποιηθούν για να εξασφαλίσουν ότι κανένας δεν μπορεί να διαβάσει τα εμπιστευτικά δεδομένα εκτός από το(ους) δέκτη(ες) που είναι εξουσιοδοτούμενοι . Γίνεται αναφορά σε τέτοιες τεχνικές στην παράγραφο 4.4.



Εικόνα 3: Μια ταξινόμηση των Τεχνικών ΔΙΕΓ

4.1. Τεχνικές Διαμέρισης Δεδομένων

Οι τεχνικές διαμέρισης δεδομένων έχουν εφαρμοστεί σε μερικά σενάρια στα οποία οι βάσεις δεδομένων διαθέσιμες για τη εξόρυξη διανέμονται σε διάφορες περιοχές, με κάθε περιοχή πρόθυμη να μοιραστεί μόνο τα αποτελέσματα της εξόρυξης δεδομένων, και όχι τα δεδομένα πηγής. Σε αυτές τις περιπτώσεις, τα δεδομένα διανέμονται είτε οριζόντια είτε κάθετα [14]. Στον οριζόντιο διαμερισμό, οι διαφορετικές οντότητες περιγράφονται με το ίδιο σχήμα σε όλα τα διαμερίσματα, ενώ στον κάθετο διαμερισμό οι ιδιότητες των ίδιων οντοτήτων χωρίζονται μεταξύ των διαμερισμάτων. Οι υπάρχουσες λύσεις μπορούν να κατηγοριοποιηθούν σε αυτές που βασίζονται στην κρυπτογραφία και στις παραγωγικές τεχνικές.

4.1.1. Τεχνικές Βασισμένες στην Κρυπτογραφία

Στα πλαίσια της ΔΙΕΓ για τα κατανεμημένα δεδομένα, έχουν αναπτυχθεί τεχνικές βασισμένες στην κρυπτογραφία για να λύσουν τα προβλήματα της ακόλουθης φύσης: δύο ή περισσότερα συμβαλλόμενα μέρη θέλουν να διεξάγουν έναν υπολογισμό βασισμένο στις ιδιωτικές εισόδους τους. Το ζήτημα είναι εδώ πώς να διεξαχθεί ένας τέτοιος υπολογισμός έτσι ώστε κανένα συμβαλλόμενο μέρος να μην ξέρει τίποτα άλλο εκτός από την είσοδό του και τα αποτελέσματα. Αυτό το πρόβλημα αναφέρεται ως Ασφαλές Πολυκομματικό Πρόβλημα Υπολογισμού [25, 17, 44].

Γενικά, ο ασφαλής πολυκομματικός υπολογισμός είναι ο κλάδος της κρυπτογραφίας που εξετάζει την πραγματοποίηση των κατανεμημένων στοιχειωδών εργασιών κατά τρόπο ασφαλή· σε αυτήν την περίπτωση, ο ορισμός της ασφάλειας μπορεί να έχει διαφορετικές σημασίες, όπως η διατήρηση της ιδιωτικότητας των δεδομένων ή η προστασία του υπολογισμού από κακόβουλες επιθέσεις [26]. Χαρακτηριστικά, ο ασφαλής πολυκομματικός υπολογισμός αποτελείται από τον υπολογισμό κάποιας συνάρτησης $f(x, y)$, όπου η είσοδος x είναι στα χέρια ενός συμμετέχοντος και η είσοδος y είναι στα χέρια άλλου. Για να είναι ασφαλής ο υπολογισμός, δεν αποκαλύπτονται άλλες πληροφορίες σε έναν συμμετέχοντα πέρα από όσα μπορούν να προκύψουν από την είσοδο εκείνου του συμμετέχοντος και την έξοδο της συνάρτησης (τα τελικά αποτελέσματα).

Στο αρχικό μοντέλο του ασφαλούς πολυκομματικού υπολογισμού [35], δύο συμβαλλόμενα μέρη που κατέχουν εμπιστευτικές βάσεις δεδομένων (π.χ.

εμπιστευτικά αρχεία ασθενών) επιθυμούν να τρέξουν έναν αλγόριθμο εξόρυξης δεδομένων στην ένωση των βάσεων δεδομένων τους χωρίς αποκάλυψη οποιωνδήποτε περιττών πληροφοριών. Το σύνολο εκπαίδευσης διανέμεται μεταξύ των δύο συμβαλλόμενων μερών. Αυτή η προσέγγιση μεταχειρίζεται την ΔΙΕΓ ως ειδική περίπτωση του ασφαλούς πολυκομματικού υπολογισμού, και όχι μόνο στοχεύει στη διατήρηση της μεμονωμένης ιδιωτικότητας αλλά και προσπαθεί να αποκόψει τη διαρροή οποιωνδήποτε πληροφοριών εκτός από το τελικό αποτέλεσμα. Η λύση είναι αποδοτική για τις εφαρμογές διαμερισμού δεδομένων και έχει υψηλές απαιτήσεις επικεφαλίδων επικοινωνίας και εύρους ζώνης.

Βεβαίως προτείνονται και άλλες λύσεις [30, 49] οι οποίες στοχεύουν να εξαγάγουν συνολικά τα έγκυρα αποτελέσματα από τα διανεμημένα δεδομένα χωρίς αποκάλυψη των πληροφοριών που συμβιβάζουν τη ιδιωτικότητα των μεμονωμένων πηγών. Παράδειγμα αποτελεί η εξόρυξη των κανόνων συσχέτισης πάνω σε οριζόντια διαμερισμένα δεδομένα [30]. Αυτή η προσέγγιση εξετάζει την ανακάλυψη των συσχετίσεων στις δοσοληψίες που είναι χωρισμένες στα μέρη, χωρίς αποκάλυψη του περιεχομένου των μεμονωμένων δοσοληψιών. Σε αυτό το μοντέλο, τα δεδομένα που είναι διαθέσιμα σε όλα τα συμβαλλόμενα μέρη έχουν το ίδιο σχήμα, και υποτίθεται ότι τρία ή περισσότερα συμβαλλόμενα μέρη εμπλέκονται για να ελαχιστοποιήσουν τη διαρροή των πληροφοριών. Η λύση είναι βασισμένη στον ασφαλή πολυκομματικό υπολογισμό για να ελαχιστοποιήσει τις κοινές πληροφορίες, μολονότι επιβαρύνει την εργασία της εξόρυξης. Αφ'ετέρου, υπάρχει το πρόβλημα εξόρυξης κανόνων συσχέτισης από δοσοληψίες που κατανέμονται στις πηγές [49]. Κάθε μέρος κρατά μερικές ιδιότητες κάθε δοσοληψίας, και τα μέρη επιθυμούν να συνεργαστούν για να προσδιορίσουν συνολικά τους έγκυρους κανόνες συσχέτισης. Σε αυτό το μοντέλο, δύο συμβαλλόμενα μέρη εμπλέκονται, ένα μέρος που υποδεικνύεται ως το πρωταρχικό, το οποίο είναι ο ιδρυτής του πρωτοκόλλου κι ένα άλλο που είναι ο αποκριτής. Υπάρχει ένα κοινό κλειδί και στις δύο βάσεις δεδομένων. Ο στόχος είναι να ανακαλυφθούν κανόνες συσχέτισης διαφορετικοί από το κοινό κλειδί.

4.1.2. Παραγωγικές Τεχνικές

Οι παραγωγικές τεχνικές έχουν ως σκοπό να εκτελέσουν κατανεμημένες εργασίες εξόρυξης. Σε αυτήν την προσέγγιση, κάθε συμβαλλόμενο μέρος μοιράζεται ακριβώς μια μικρή μερίδα του τοπικού μοντέλου του που χρησιμοποιείται για να

κατασκευάσει το καθολικό μοντέλο. Οι υπάρχουσες λύσεις χτίζονται πάνω σε οριζόντια διαμοιρασμένα δεδομένα.

Η λύση που προτείνεται στο [51] έχει να κάνει με τη διατήρηση της ιδιωτικότητας συχνών στοιχειοσυνόλων σε κατανεμημένες βάσεις δεδομένων. Κάθε μέρος *Si* $(3 < i < n)$ στέλνει τα συχνά στοιχειοσύνολά του σε έναν συνδυαστή που βρίσκει τα καθολικά συχνά στοιχειοσύνολα, βασιζόμενος στα τοπικά μοντέλα. Κάθε μέρος χρησιμοποιεί διαφορετική αναπαράσταση των στοιχειοσυνόλων με αποτέλεσμα ο συνδυαστής να μην είναι ικανός να αναγνωρίσει τα στοιχειοσύνολα με την προϋπόθεση ότι όλα τα μέρη χρησιμοποιούν την ίδια κωδικοποίηση. Αφού συνδυάσει τα τοπικά συχνά στοιχειοσύνολα, ο συνδυαστής στέλνει το ανώτερο όριο για τα καθολικά συχνά στοιχειοσύνολα σε όλα τα μέρη, και κάθε μέρος είναι σε θέση να αποκαταστήσει την κωδικοποίηση των αρχικών στοιχειοσυνόλων. Σε αυτό το σημείο, κάθε μέρος ξέρει μόνο τις πληροφορίες σχετικά με τα συχνά στοιχειοσύνολα του και τα ανώτερα όρια των καθολικών στοιχειοσυνόλων. Το μέρος S_1 τότε παράγει έναν τυχαίο αριθμό για κάθε ένα από τα στοιχειοσύνολα του. Αυτός ο αριθμός προστίθεται έπειτα στον μετρητή υποστήριξης κάθε στοιχειοσυνόλου και οι διαταραγμένες αριθμήσεις υποστήριξης στέλνονται στο μέρος S_2. Ο αλγόριθμος συνεχίζεται με τον ίδιο τρόπο όπως πριν μέχρι την τελευταία επανάληψη. Μετά την λήψη των τιμών των συνολικών τοπικών αριθμήσεων, το μέρος S_n ζητά από το μέρος S_1 τις τιμές των τυχαίων αριθμών και τα αντίστοιχα στοιχειοσύνολά τους. Το μέρος S_n απλά μειώνει κάθε καθολική αρίθμηση υποστήριξης κατά τον αντίστοιχο αριθμό και ελέγχει ποια στοιχειοσύνολα είναι τοπικά συχνά. Αποδεικνύεται ότι το καθολικό μοντέλο που παράγεται είναι ακριβές και το κόστος επικοινωνίας απαιτεί μόνο ένα γύρο του μηνύματος γύρω από τις περιοχές και μια λειτουργία μείωσης για να αθροίσει τα τελικά αποτελέσματα.

4.2. Τεχνικές Μετατροπής Δεδομένων

Οι τεχνικές μετατροπής δεδομένων τροποποιούν τις αρχικές τιμές μιας βάσης δεδομένων που πρέπει να μοιραστεί, και με αυτό τον τρόπο, εξασφαλίζεται η διατήρηση ιδιωτικότητας. Η μετασχηματισμένη βάση δεδομένων τίθεται στην διαδικασία της εξόρυξης και πρέπει να καλύπτει τις απαιτήσεις ιδιωτικότητας χωρίς την απώλεια του οφέλους της εξόρυξης. Γενικά, οι τεχνικές μετατροπής δεδομένων

στοχεύουν σε μια σωστή εξισορρόπηση μεταξύ της διατήρησης ιδιωτικότητας και της κοινοποίησης γνώσης. Οι πιο κλασσικές μέθοδοι για τη μετατροπή δεδομένων είναι οι τεχνικές προσθήκης θορύβου και οι τεχνικές χωρικού μετασχηματισμού.

4.2.1. Τεχνικές Προσθήκης Θορύβου

Στην εξόρυξη δεδομένων, η σημαντικότερη απαίτηση ενός μηχανισμού ελέγχου ασφάλειας (εκτός από την προστασία της ιδιωτικότητας) δεν είναι να εξασφαλιστούν ακριβείς και μη-προκατειλημμένες στατιστικές, αλλά να συντηρηθούν οι υψηλού επιπέδου περιγραφές της γνώσης που ανακαλύπτονται από τις μεγάλες βάσεις δεδομένων [7, 19]. Κατά συνέπεια, η ιδέα πίσω από τις τεχνικές προσθήκης θορύβου για ΔΙΕΓ είναι ότι κάποιος θόρυβος (π.χ. πληροφορίες μη παρούσες σε μια συγκεκριμένη πλειάδα ή δοσοληψία) προστίθεται στα αρχικά δεδομένα για να αποτρέψει την εξακρίβωση των εμπιστευτικών πληροφοριών σχετικά με ένα συγκεκριμένο άτομο. Σε άλλες περιπτώσεις, ο θόρυβος προστίθεται στις εμπιστευτικές ιδιότητες ανακατεύοντας τυχαία τις τιμές των ιδιοτήτων ώστε να αποκρυφθούν ορισμένα πρότυπα. Οι τεχνικές προσθήκης θορύβου ταξινομούνται σε τρεις ομάδες:

- τεχνικές ανταλλαγής δεδομένων,
- τεχνικές διαταραχής δεδομένων και
- τεχνικές τυχαιοποίησης δεδομένων.

Οι *τεχνικές ανταλλαγής δεδομένων* αντικαθιστούν την αρχική βάση δεδομένων με μια νέα που έχει την ίδια κατανομή πιθανότητας. Τέτοιες τεχνικές είναι κατάλληλες για την προστασία της ιδιωτικότητας στην ανακάλυψη γνώσης. Η ιδέα πίσω από την ανταλλαγή δεδομένων είναι ότι ανταλλάσσει τις τιμές στις καταχωρήσεις της βάσης δεδομένων κατά τέτοιο τρόπο ώστε να διατηρούνται οι στατιστικές για τις ομάδες (π.χ., συχνότητες, μέσοι όροι, κ.λ.π.).

Οι *τεχνικές διαταραχής δεδομένων* διαστρεβλώνουν τα δεδομένα για να προστατεύσουν την ιδιωτικότητα των ατόμων με την εισαγωγή ενός σφάλματος (θόρυβος) στα αρχικά δεδομένα. Ο θόρυβος χρησιμοποιείται για να παράγει τη νέα (διαστρεβλωμένη) βάση δεδομένων που υποβάλλεται στη εξόρυξη. Οι data miners

πρέπει να είναι σε θέση να επιτύχουν τα έγκυρα αποτελέσματα (π.χ. πρότυπα και τάσεις) από τα διαστρεβλωμένα δεδομένα.

Οι *τεχνικές τυχαιοποίησης δεδομένων* επιτρέπουν σε κάποιον να ανακαλύψει τα γενικά πρότυπα σε μια βάση δεδομένων με ένα όριο σφάλματος, προστατεύοντας ταυτόχρονα τις μεμονωμένες τιμές. Όπως οι τεχνικές ανταλλαγής δεδομένων και διαταραχής δεδομένων, οι τεχνικές τυχαιοποίησης σχεδιάζονται ώστε να βρουν έναν καλό συμβιβασμό μεταξύ της προστασίας ιδιωτικότητας και της ανακάλυψης γνώσης.

4.2.2. Τεχνικές Χωρικού Μετασχηματισμού

Οι τεχνικές χωρικού μετασχηματισμού έχουν ως σκοπό να εξετάσουν την διατήρηση ιδιωτικότητας στη συσταδοποίηση. Αυτές οι τεχνικές στοχεύουν στην προστασία των υποκείμενων τιμών δεδομένων που υποβάλλονται στη συσταδοποίηση χωρίς διακινδύνευση της ομοιότητας μεταξύ των αντικειμένων υπό ανάλυση. Κατά συνέπεια, μια τεχνική χωρικού μετασχηματισμού πρέπει όχι μόνο να καλύπτει τις απαιτήσεις ιδιωτικότητας αλλά και να εγγυάται τα έγκυρα αποτελέσματα συσταδοποίησης.

4.3. Τεχνικές Περιορισμού Δεδομένων

Οι τεχνικές περιορισμού δεδομένων εστιάζουν στον περιορισμό της πρόσβασης στα αποτελέσματα εξόρυξης μέσω της γενίκευσης ή της καταστολής των πληροφοριών (π.χ. αντικείμενα στις δοσοληψίες ή ιδιότητες στις σχέσεις), ή ακόμα και με την απαγόρευση της πρόσβασης σε μερικά πρότυπα που υποτίθεται πως δεν πρέπει να ανακαλυφθούν. Τέτοιες τεχνικές μπορούν να διαιρεθούν σε δύο ομάδες: *Τεχνικές Μπλοκαρίσματος* και *Τεχνικές Καθαρισμού*.

4.3.1. Τεχνικές Μπλοκαρίσματος

Οι τεχνικές μπλοκαρίσματος στοχεύουν στην απόκρυψη κάποιων ευαίσθητων πληροφοριών όταν μοιράζονται τα δεδομένα για τη εξόρυξη. Οι ιδιωτικές πληροφορίες περιλαμβάνουν τους ευαίσθητους κανόνες συσχέτισης και τους κανόνες κατηγοριοποίησης που πρέπει να παραμείνουν ιδιωτικοί. Πριν δημοσιεύσουν τα

δεδομένα για την εξόρυξη, οι κάτοχοι δεδομένων πρέπει να εξετάσουν πόσες πληροφορίες μπορούν να προκύψουν ή να υπολογιστούν από τις μεγάλες βάσεις δεδομένων και πρέπει να ψάξουν τρόπους για να ελαχιστοποιηθεί η διαρροή τέτοιων πληροφοριών. Γενικά, οι τεχνικές μπλοκαρίσματος είναι εφικτό να ανακτήσουν τα πρότυπα που είναι λιγότερο συχνά από ότι είναι αρχικά, δεδομένου ότι οι ευαίσθητες πληροφορίες είτε καταστέλλονται, είτε αντικαθίστανται με αγνώστους (unknowns) για να διατηρήσουν την ιδιωτικότητα.

Όσον αφορά τους κανόνες συσχέτισης, υπάρχει ένα σύνολο αλγορίθμων [5, 6] για να κρύψει τις ευαίσθητες πληροφορίες (ευαίσθητοι κανόνες) με την αντικατάσταση ορισμένων ιδιοτήτων των αντικειμένων δεδομένων με ένα σύμβολο «?» (άγνωστος), αντί της διαγραφής τέτοιων αντικειμένων. Με αυτό τον τρόπο, αυτή κρύβονται οι ευαίσθητες πληροφορίες, που αντιπροσωπεύουν μερικούς ευαίσθητους κανόνες συσχέτισης, και προστατεύονται οι miners από την εκμάθηση λανθασμένων κανόνων. Αυτή η προσέγγιση επιβάλλει μερικές αλλαγές στον ορισμό της υποστήριξης και της εμπιστοσύνης ενός κανόνα συσχέτισης. Συγκεκριμένα, η ελάχιστη υποστήριξη και η ελάχιστη εμπιστοσύνη θα αλλάξουν σε ένα ελάχιστο *διάστημα* υποστήριξης και ένα ελάχιστο *διάστημα* εμπιστοσύνης αντίστοιχα. Εφόσον βρίσκονται η υποστήριξη ή/και η εμπιστοσύνη ενός ευαίσθητου κανόνα κάτω από τη μέση αυτών των διαστημάτων τιμών, τότε αναμένεται ότι η εμπιστευτικότητα των δεδομένων δεν παραβιάζεται.

4.3.2. Τεχνικές Καθαρισμού

Σε αντίθεση με τις τεχνικές μπλοκαρίσματος που κρύβουν τις ευαίσθητες πληροφορίες με τον περιορισμό ή την αντικατάσταση μερικών αντικειμένων ή τιμών γνωρισμάτων με αγνώστους, οι τεχνικές καθαρισμού κρύβουν τις ευαίσθητες πληροφορίες με την καταστολή μερικών αντικειμένων στις συναλλακτικές βάσεις δεδομένων, ή ακόμα και με τη γενίκευση των πληροφοριών για να διατηρήσουν την ιδιωτικότητα στην κατηγοριοποίηση. Αυτές οι τεχνικές μπορούν να ταξινομηθούν σε δύο σημαντικές ομάδες: *τεχνικές διαμοιρασμού δεδομένων* και *τεχνικές διαμοιρασμού προτύπων*. Στην πρώτη περίπτωση, η διαδικασία καθαρισμού ενεργεί στα δεδομένα για να αφαιρέσει ή να κρύψει την ομάδα ευαίσθητων κανόνων συσχέτισης που περιέχουν την ευαίσθητη γνώση. Για να επιτευχθεί αυτό, ένας μικρός αριθμός

δοσοληψιών που περιέχουν τους ευαίσθητους κανόνες πρέπει να τροποποιηθούν διαγράφοντας ένα ή περισσότερα αντικείμενα από τις δοσοληψίες ή ακόμα και προσθέτοντας κάποιον θόρυβο, δηλαδή νέα αντικείμενα, όχι αρχικά παρόντα σε τέτοιες δοσοληψίες. Στην δεύτερη περίπτωση, οι αλγόριθμοι καθαρισμού ενεργούν πάνω στους κανόνες που εξάγονται από μια βάση δεδομένων, παρά στα ίδια τα δεδομένα. Ο αλγόριθμος αφαιρεί όλους τους ευαίσθητους κανόνες πριν από τη διαδικασία διαμοιρασμού.

Η ιδέα πίσω από τις τεχνικές διαμοιρασμού δεδομένων παρουσιάστηκε στο [3] και είναι η επιλεκτική απόκρυψη μερικών συχνών στοιχειοσυνόλων από τις μεγάλες βάσεις δεδομένων με όσο το δυνατόν λιγότερο αντίκτυπο σε άλλα μη-ευαίσθητα συχνά στοιχειοσύνολα (αυτό μπορεί να ερμηνευτεί ως η διαδικασία της μείωσης της υποστήριξης ενός δεδομένου συνόλου ευαίσθητων κανόνων, που εξάγεται από τη βάση δεδομένων, κάτω από μια ελάχιστη τιμή). Οι συγγραφείς εστίασαν σε μια θεωρητική προσέγγιση θεωρώντας πως ο μόνος τόπος να αποκρυφθεί ένας κανόνας είναι να μειωθεί η υποστήριξη των αντίστοιχων συχνών στοιχειοσυνόλων του. Επίσης απέδειξαν ότι ο βέλτιστος καθαρισμός είναι ένα NP-hard πρόβλημα.

Στο [4], οι συγγραφείς προσπάθησαν να προσεγγίσουν το πρόβλημα της απόκρυψης κανόνων συσχέτισης θεωρώντας πως για να αποκρυφθεί ένας κανόνας θα πρέπει η εμπιστοσύνη του κανόνα αυτού να πέσει κάτω από ένα, καθορισμένο από τον χρήστη, κατώφλι. Επομένως προσπαθούν να αποκρύψουν έναν κανόνα μειώνοντας είτε την υποστήριξη, είτε την εμπιστοσύνη του, διατηρώντας ταυτόχρονα ένα ασφαλές πλαίσιο μείωσης των παρενεργειών στους μη-ευαίσθητους κανόνες.

Ένα ενοποιημένο πλαίσιο για τους ευαίσθητους κανόνες συσχέτισης εισήχθη στο [40]. Αυτό το πλαίσιο συνδυάζει τεχνικές για αποτελεσματική απόκρυψη των ευαίσθητων προτύπων: μια μηχανή ανάκτησης δοσοληψίας που στηρίζεται σε ένα λεξικό και σε Boolean ερωτήσεις, ένα σύνολο αλγορίθμων, μια βάση δεδομένων και ένα σύνολο μετρικών για να υπολογιστεί ποσοτικά η κοινοποίηση των πληροφοριών και να αξιολογηθεί ο αντίκτυπος της διαδικασίας sanitization στη βάση δεδομένων. Οι αλγόριθμοι καθαρισμού απαιτούν δύο ανιχνεύσεις ανεξάρτητα από το μέγεθος της βάσης δεδομένων και τον αριθμό ευαίσθητων προτύπων που πρέπει να προστατευθούν. Η πρώτη ανίχνευση απαιτείται για να χτίσει ένα ευρετήριο (ένα λεξικό) για την επιτάχυνση της διαδικασίας καθαρισμού, ενώ η δεύτερη χρησιμοποιείται για να καθαρίσει την αρχική βάση δεδομένων. Αυτή η εργασία

επεκτάθηκε στο [41], στην οποία δύο νέοι αλγόριθμοι καθαρισμού εισήχθησαν με σκοπό να εξισορροπήσουν την ιδιωτικότητα και την κοινοποίηση γνώσης.

Ένας νέος αλγόριθμος καθαρισμού, προτάθηκε στο [42]. Η πρόταση αυτή απαιτεί μόνο ένα πέρασμα σε μια βάση δεδομένων δοσοληψιών ανεξάρτητα από το μέγεθος της βάσης δεδομένων και τον αριθμό των ευαίσθητων κανόνων ένωσης που πρέπει να προστατευθούν. Ειδικότερα, ανιχνεύει μια ομάδα από Κ δοσοληψίες και καθαρίζει έπειτα το σύνολο των ευαίσθητων κανόνων που μπορούν να εξαχθούν από αυτές τις Κ δοσοληψίες. Αυτός ο αλγόριθμος βελτιώνει την ισορροπία μεταξύ της προστασίας της ευαίσθητης γνώσης και της ανακάλυψης προτύπων, και είναι χρήσιμος για μεγάλες βάσεις δεδομένων δοσοληψιών.

Όσον αφορά τις τεχνικές διαμοιρασμού προτύπων, η μόνη γνωστή προσέγγιση που εμπίπτει σε αυτήν την κατηγορία εισήχθη στο [43]. Αυτό το πλαίσιο εξετάζει το διαμοιρασμό των κανόνων συσχέτισης μεταξύ δύο ή περισσότερων συμβαλλόμενων μερών. Σε αυτό το πρόβλημα, ένα συμβαλλόμενο μέρος μπορεί να αποφασίσει να αποκαλύψει μόνο μέρος της γνώσης και να κρύψει τα στρατηγικά πρότυπα, τα οποία καλούμε ευαίσθητους κανόνες. Αυτοί οι ευαίσθητοι κανόνες πρέπει να προστατευθούν πριν την διανομή, δεδομένου ότι είναι κυρίαρχοι για τις στρατηγικές αποφάσεις και πρέπει να παραμείνουν ιδιωτικοί. Το προτεινόμενο πλαίσιο αποτελείται από έναν αλγόριθμο καθαρισμού της ευαίσθητης γνώσης πριν την διανομή των κανόνων συσχέτισης, και από ένα σύνολο μετρικών για να αξιολογηθούν οι επιθέσεις ενάντια στην ευαίσθητη γνώση.

4.4. Τεχνικές Ιδιοκτησίας Δεδομένων

Οι τεχνικές ιδιοκτησίας δεδομένων μπορούν να εφαρμοστούν σε δύο διαφορετικά σενάρια: (α) για να προστατεύσουν την ιδιοκτησία των δεδομένων από τους ανθρώπους για τους οποίους τα δεδομένα συλλέχθησαν και (β) για να προσδιορίσουν την οντότητα που λαμβάνει εμπιστευτικά δεδομένα όταν τέτοια δεδομένα μοιράζονται ή ανταλλάσσονται.

Στα πλαίσια της εξόρυξης δεδομένων, η πρώτη προσέγγιση προς μια τεχνική λύση που θα εγγυάται την ιδιωτικότητα των κατόχων δεδομένων προτάθηκε στο [23]. Η ιδέα πίσω από αυτήν την προσέγγιση είναι ότι ένας κάτοχος δεδομένων μπορεί να επιτρέψει τη χρησιμοποίηση των δεδομένων για ορισμένους μόνο λόγους. Για να το

επιτύχει αυτό, αυτή η λύση στηρίζεται στην κωδικοποίηση αδειών στην χρήση των δεδομένων.

Μια διαφορετική προσέγγιση για το διαμοιρασμό των εμπιστευτικών δεδομένων [36], εξασφαλίζει ότι κανένας δεν μπορεί να διαβάσει τα εμπιστευτικά δεδομένα εκτός από το(ους) δέκτη(ες). Μπορεί να χρησιμοποιηθεί σε σενάρια όπως στατιστικοί ή ερευνητικοί σκοποί, εξόρυξη γνώσης, και σε ενδοεπιχειρησιακές (B2B) αλληλεπιδράσεις. Το πλαίσιο αυτό αποτελείται από ένα «δακτυλικό αποτύπωμα», κωδικοποιητή, αποκωδικοποιητή και έναν αλγόριθμο ανίχνευσης.

4.5. Περίληψη

Σε αυτό το κεφάλαιο, κάναμε μια αναφορά στις υπάρχουσες τεχνικές ΔΙΕΓ που προκύπτουν από τη βιβλιογραφία. Ταξινομήσαμε αυτές τις τεχνικές σε τέσσερις σημαντικές κατηγορίες: διαμέριση δεδομένων, μετατροπή δεδομένων, περιορισμός δεδομένων και ιδιοκτησία δεδομένων.

Οι τεχνικές διαμέρισης δεδομένων εξετάζουν τα σενάρια στα οποία τα δεδομένα προς εξόρυξη χωρίζονται στις πολλαπλές περιοχές. Οι υπάρχουσες λύσεις μπορούν να κατηγοριοποιηθούν σε τεχνικές βασισμένες στην κρυπτογραφία και σε παραγωγικές τεχνικές. Όσον αφορά τις τεχνικές μετατροπής δεδομένων, μετατρέπουν μια αρχική βάση δεδομένων σε μια νέα η οποία υποβάλλεται στην εξόρυξη. Η βάση δεδομένων ισορροπεί μεταξύ της διατήρησης ιδιωτικότητας και της ανακάλυψης γνώσης. Οι τεχνικές μετατροπής δεδομένων μπορούν να κατηγοριοποιηθούν σε δύο ομάδες: τεχνικές προσθήκης θορύβου και τεχνικές χωρικού μετασχηματισμού. Οι μεν έχουν ως σκοπό τη διατήρηση ιδιωτικότητας στην εξόρυξη κανόνων συσχέτισης ενώ οι δε τη διατήρηση ιδιωτικότητας στη συσταδοποίηση. Η τρίτη κατηγορία τεχνικών ΔΙΕΓ που εισαγάγαμε σε αυτό το κεφάλαιο ονομάζεται Περιορισμός Δεδομένων. Αυτή η κατηγορία περιλαμβάνει τις τεχνικές μπλοκαρίσματος και τις τεχνικές καθαρισμού. Ο στόχος τέτοιων τεχνικών είναι να περιοριστεί η πρόσβαση στη γνώση που εξάγεται από τις βάσεις δεδομένων μέσω της γενίκευσης ή της καταστολής των πληροφοριών. Γενικά, οι τεχνικές μπλοκαρίσματος κρύβουν τις ευαίσθητες πληροφορίες με τον περιορισμό ή την αντικατάσταση μερικών αντικειμένων ή τιμών ιδιοτήτων με αγνώστους, ενώ οι τεχνικές καθαρισμού κρύβουν τις ευαίσθητες πληροφορίες με την καταστολή μερικών αντικειμένων στις συναλλακτικές βάσεις δεδομένων. Η τέταρτη κατηγορία τεχνικών ΔΙΕΓ ονομάζεται Ιδιοκτησία Δεδομένων.

Αυτές οι τεχνικές εφαρμόζουν έναν μηχανισμό που επιβάλλει την ιδιοκτησία δεδομένων από τα άτομα στα οποία ανήκουν τα δεδομένα. Επίσης, κατά το διαμοιρασμό εμπιστευτικών δεδομένων, αυτές οι τεχνικές μπορούν να χρησιμοποιηθούν για να εξασφαλίσουν ότι κανένας δεν μπορεί να διαβάσει τα εμπιστευτικά δεδομένα εκτός από τον(ους) εξουσιοδοτημένο(ους) δέκτη(ες).

Κεφάλαιο 5

Μέθοδοι Για Διατήρηση Ιδιωτικότητας Στην Εξόρυξη Κανόνων Συσχέτισης

Ο διαμοιρασμός των κανόνων συσχέτισης είναι αρκετά ωφέλιμη στη βιομηχανία, αλλά απαιτεί ισχυρά μέτρα προστασίας της ιδιωτικότητας. Κάποιος μπορεί να αποφασίσει να αποκαλύψει μόνο μέρος της γνώσης που εξάγεται από τις βάσεις δεδομένων, και να προστατεύσει την ευαίσθητη γνώση που αντιπροσωπεύεται από τους ευαίσθητους κανόνες. Αυτοί οι ευαίσθητοι κανόνες πρέπει να παραμείνουν ιδιωτικοί δεδομένου ότι είναι ουσιαστικοί για τις στρατηγικές αποφάσεων. Μερικές επιχειρήσεις προτιμούν να μοιραστούν τα δεδομένα τους στα πλαίσια της συνεργασίας, ενώ άλλες προτιμούν να μοιραστούν μόνο τα πρότυπα που ανακαλύπτονται από τα δεδομένα τους. Οι αλγόριθμοι που θα παρουσιαστούν στη συνέχεια του κεφαλαίου εμπίπτουν στην κατηγορία των αλγορίθμων Περιορισμού Δεδομένων και λαμβάνουν υπόψη αυτές τις δύο σημαντικές πτυχές, δηλαδή το διαμοιρασμό των δεδομένων και το διαμοιρασμό των προτύπων.

Αυτό το κεφάλαιο είναι οργανωμένο ως εξής: Στην παράγραφο 5.1, γίνεται μια εκτενέστερη παρουσίαση των αλγορίθμων που εμπίπτουν στις μεθόδους του προηγούμενου κεφαλαίου. Η παρουσίαση αυτή ακολουθεί μια χρονολογική αλλά και

ιεραρχική συνέχεια με σκοπό να μπορέσει να αποδωθεί η σειρά με την οποία προτάθηκαν οι αλγόριθμοι.

Στην παράγραφο 5.1, εισάγεται το πλαίσιο για την ευαίσθητη γνώση στις βάσεις δεδομένων δοσοληψιών. Αυτό το πλαίσιο αποτελείται από μια δομή ανάκτησης (π.χ. ευρετήριο), ένα σύνολο αλγορίθμων καθαρισμού μιας βάσης δεδομένων, και ένα σύνολο μετρικών για να μετρήσει πόσες ιδιωτικές πληροφορίες αποκαλύπτονται καθώς επίσης και την επιρροή των αλγορίθμων καθαρισμού στα έγκυρα αποτελέσματα εξόρυξης. Στην παράγραφο 5.2, εισάγονται οι αλγόριθμοι καθαρισμού διαμοιρασμού δεδομένων. Η διαδικασία καθαρισμού ενεργεί στα δεδομένα για να αφαιρέσει ή να κρύψει την ομάδα ευαίσθητων κανόνων συσχέτισης. Μετά από τον καθαρισμό μια βάσης δεδομένων, η βάση δεδομένων διανέμεται για την εξόρυξη κανόνων συσχέτισης. Μια διαφορετική προσέγγιση στην απόκρυψη ευαίσθητης γνώσης εισάγεται στην παράγραφο 5.3, αποκαλούμενη διαμοιρασμός προτύπων. Σε αυτήν την προσέγγιση, οι αλγόριθμοι καθαρισμού δρουν στους κανόνες που εξάγονται από μια βάση δεδομένων αντί στα ίδια τα δεδομένα. Αντί λοιπόν οι κάτοχοι δεδομένων να διανέμουν τα ίδια τα δεδομένα τους, μπορούν αρχικά να εξορύξουν τα δεδομένα τους και στη συνέχεια να μοιραστούν πρότυπα που προκύπτουν από την εξόρυξη.

5.1. Παρουσίαση των Αλγορίθμων Περιορισμού Δεδομένων

Σε προηγούμενο κεφάλαιο (κεφάλαιο 2, παράγραφος 2.2) δόθηκε ο ορισμός του προβλήματος της εξόρυξης κανόνων συσχέτισης, καθώς επίσης και ο ορισμός του προβλήματος καθαρισμού μιας βάσης δεδομένων. Στο κεφάλαιο 4, έγινε μια παρουσίαση των τεχνικών που προσπαθούν να προσεγγίσουν το πρόβλημα αυτό, ενώ στο παρόν πεδίο θα γίνει μια εκτενέστερη περιγραφή των αλγορίθμων και των ευρετικών που επινοήθηκαν και που εμπίπτουν στις προαναφερθείσες τεχνικές.

Θα γίνει παρουσίαση των αλγορίθμων των Τεχνικών Περιορισμού Δεδομένων, λόγω του ότι αποτελούν μία πολύ αντιπροσωπευτική ομάδα αλγορίθμων πάνω στους οποίους στηρίχτηκαν, αλλά και στηρίζονται, οι υλοποιήσεις μεταγενέστερων αλγορίθμων που προσπαθούν να προσεγγίσουν το πρόβλημα του καθαρισμού. Η παράθεση των αλγορίθμων γίνεται κατά κατηγορία, όπως ακριβώς αναφέρθηκαν στο κεφάλαιο 4, και κατά χρονολογική σειρά υλοποίησης.

5.1.1. Αλγόριθμοι Μπλοκαρίσματος

5.1.1.1. Απόκρυψη Ευαίσθητων Κανόνων με Χρήση Αγνώστων

Σε προηγούμενες εργασίες [3, 4], οι συγγραφείς έδειξαν ένα τρόπο να αποκρύπτονται ευαίσθητοι κανόνες συσχέτισης μειώνοντας είτε την υποστήριξη, είτε την εμπιστοσύνη τους. Αυτό το πέτυχαν μετατρέποντας τις μηδενικές τιμές σε άσσους, αλλά είχε ως αποτέλεσμα την εισαγωγή θορύβου στις βάσεις δεδομένων, που για κάποια πραγματικά σενάρια (π.χ. καρτέλες ασθενών) ήταν πολύ σημαντικό. Η προσέγγιση που παρουσιάζεται στα [5, 6] προσπαθεί να αποκρύψει τους ευαίσθητους κανόνες αντικαθιστώντας γνωστές τιμές γνωρισμάτων με αγνώστους «?», ενώ παράλληλα μειώνει τις παρενέργειες στους μη-ευαίσθητους κανόνες.

Με την νέα προσέγγιση που περιέχει αγνώστους ο ορισμός της υποστήριξης άλλαξε: αντί για μια μοναδική τιμή υποστήριξης ενός στοιχειοσυνόλου X, πλέον έχουμε ένα διάστημα υποστήριξης $[\min\sup(X), \text{maxsup(X)}]$ Αντίστοιχα και η εμπιστοσύνη ενός κανόνα πλέον δεν έχει μια μοναδική τιμή, αλλά ένα διάστημα εμπιστοσύνης $[\min conf(X \Rightarrow Y), \max conf(X \Rightarrow Y)]$.

Υλοποιήθηκαν δύο αλγόριθμοι για την απόκρυψη των κανόνων. Ο πρώτος εστιάζει στο κρύψιμο των κανόνων με τη μείωση της ελάχιστης υποστήριξης των itemsets που παρήγαγαν αυτούς τους κανόνες (δηλαδή που παράγουν). Ο δεύτερος εστιάζει στη μείωση της ελάχιστης εμπιστοσύνης των κανόνων. Με βάση τις έννοιες της υποστήριξης διαστήματος και της εμπιστοσύνης διαστήματος που εισήχθησαν στα [5, 6], επιθυμείται η μείωση της ελάχιστης υποστήριξης και των ελάχιστων τιμών εμπιστοσύνης κάτω από το MST, και το MCT αντίστοιχα από ένα ορισμένο περιθώριο ασφάλειας SM.

5.2.1.1.1 Ο Αλγόριθμος RSTsQ

Ο αλγόριθμος RSTSQ κρύβει τους ευαίσθητους κανόνες με τη μείωση της ελάχιστης υποστήριξης itemsets που τους παράγουν έως ότου είναι η ελάχιστη υποστήριξη κάτω από το MST κατά SM. Το αντικείμενο με τη μεγαλύτερη ελάχιστη υποστήριξη είναι κρύβεται στην δοσοληψία με το μικρότερο μήκος. Τα itemsets που παράγουν τους υπό απόκρυψη κανόνες αποθηκεύονται στο σύνολο L_h και αποκρύπτονται ένα προς ένα μειώνοντας μειώνοντας την ελάχιστη υποστήριξή τους. Τα itemsets στο L_h ταξινομούνται αρχικά κατά φθίνουσα σειρά μεγέθους και

ελάχιστης υποστήριξης. Στη συνέχεια αποκρύπτονται ξεκινώντας από το μεγαλύτερο itemset. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [5].

5.2.1.1.2 Ο Αλγόριθμος RCTcTsQ

Προτείνονται δύο προσεγγίσεις για την απόκρυψη κανόνων συσχέτισης με μείωση της εμπιστοσύνης τους. Η πρώτη αντικαθιστά τους άσσους με «?», ενώ η δεύτερη αντικαθιστά τα μηδενικά με «?».

Ο RCTCTSQ μειώνει την υποστήριξη του ακόλουθου τμήματος του κανόνα και η διαδικασία συνεχίζεται έως ότου η τιμή *minsup(Y)* πέσει κάτω από το MST ή η $\min conf(X \Rightarrow Y)$ κάτω από την τιμή MCT κατά SM. Τα βήματα του αλγορίθμου είναι τα εξής:

1. Ο αλγόριθμος βρίσκει όλες τις δοσοληψίες που υποστηρίζουν τον κανόνα υπό απόκρυψη, και
2. Στη συνέχεια υπολογίζεται ο αριθμός των αντικειμένων που υποστηρίζονται από κάθε δοσοληψία.
3. Οι δοσοληψίες που βρέθηκαν στο προηγούμενο βήμα ταξινομούνται κατά αύξουσα σειρά μεγέθους.
4. Τοποθετείται «?» στο αντικείμενο με τη μεγαλύτερη υποστήριξη στη μικρότερη δοσοληψία.

Η δεύτερη εκδοχή του RCTCTSQ, κρύβει έναν κανόνα αυξάνοντας το *maxsup(lhr)*, αντικαθιστώντας τα μηδενικά με «?». Η διαδικασία τερματίζεται όταν η τιμή $\min conf(X \Rightarrow Y)$ πέσει κάτω από την τιμή MCT κατά SM. Τα βήματα του αλγορίθμου είναι τα ακόλουθα:

1. Ο αλγόριθμος βρίσκει τις δοσοληψίες που υποστηρίζουν μερικώς το πρότερο τμήμα του κανόνα αλλά δεν υποστηρίζουν το ακόλουθο.
2. Στη συνέχεια υπολογίζεται ο αριθμός των αντικειμένων του πρότερου τμήματος που περιέχονται σε κάθε δοσοληψία.
3. Οι δοσοληψίες που βρέθηκαν στο προηγούμενο βήμα ταξινομούνται κατά φθίνουσα σειρά αριθμού αντικειμένων και επιλέγεται η πρώτη.
4. Τοποθετείται «?» στα αντικείμενα του πρότερου που δεν υποστηρίζονται από την δοσοληψία που επιλέχθηκε στο προηγούμενο βήμα.

5.1.1.2. Απόκρυψη Ευαίσθητων Κανόνων με Προσθήκη Αβεβαιότητας

Στα ίδια πλαίσια που κινήθηκαν οι προηγούμενες εργασίες κινείται και το [52]. Και εδώ η λογική είναι να αντικατασταθούν οι άσσοι και τα μηδενικά στις δοσοληψίες μιας βάσης με αγνώστους «?» έτσι ώστε να μπορέσουν να αποκρυφθούν κάποιοι ευαίσθητοι κανόνες. Εισάχθηκε ένας νέος αλγόριθμος μπλοκαρίσματος ο οποίος και παρουσιάζεται στην συνέχεια.

5.2.1.2.1 Ο Αλγόριθμος RCTcQ

Ο αλγόριθμος αυτός προσθέτει αβεβαιότητα στη βάση δεδομένων με την προσθήκη των «?» με έναν τρόπο ώστε η βάση δεδομένων να είναι χρησιμοποιήσιμη και ταυτοχρόνως ένας αντίπαλος δεν μπορεί να συμπεράνει τους ευαίσθητους κανόνες που ο RCTcQ θα κρύψει. Ο αλγόριθμος στοχεύει να επιτύχει τους ακόλουθους δύο στόχους:

1. Μείωση της ελάχιστης εμπιστοσύνης των ευαίσθητων κανόνων κάτω από (MCT-SM).
2. Η ελάχιστη εμπιστοσύνη των μη-ευαίσθητων κανόνων να παραμείνει άθικτη.

Εάν ο αντίπαλος βρει τη μέγιστη εμπιστοσύνη όλων των κανόνων στην τροποποιημένη βάση δεδομένων, θα βρει πολλούς νέους κανόνες που δεν υπήρχαν στην αρχική βάση δεδομένων. Έτσι, ο αντίπαλος δεν μπορεί να υποθέσει με βεβαιότητα ποιοι κανόνες που έχουν μέγιστη εμπιστοσύνη πάνω από MCT ήταν οι ευαίσθητοι κανόνες. Αφ' ετέρου, ένας κάποιος θέλει να βρει τις χρήσιμες πληροφορίες από τη βάση δεδομένων μπορεί να βρει την ελάχιστη εμπιστοσύνη όλων των κανόνων, αποκλείοντας με αυτόν τον τρόπο τους ευαίσθητους κανόνες από τις πληροφορίες του.

5.1.2. Αλγόριθμοι Καθαρισμού

Οι αλγόριθμοι της κατηγορίας αυτής αποκρύπτουν τις ευαίσθητες πληροφορίες με την καταστολή ορισμένων αντικειμένων από τις βάσεις δεδομένων. Μπορούν να ταξινομηθούν σε δύο κατηγορίες: *αλγόριθμοι διαμοιρασμού δεδομένων* - η διαδικασία καθαρισμού ενεργεί στα δεδομένα - και *αλγόριθμοι διαμοιρασμού*

προτύπων - η διαδικασία καθαρισμού ενεργεί στους κανόνες συσχέτισης που εξάγονται με την διαδικασία της εξόρυξης.

5.2.2.1. Αλγόριθμοι Διαμοιρασμού Δεδομένων

5.2.2.1.1 Η Πρώτη Προσέγγιση στο πρόβλημα του Καθαρισμού

Η ιδέα πίσω από τους αλγορίθμους αυτής της υποκατηγορίας εισήχθη στο [3], όπου οι Atallah et. al. με μία θεωρητική προσέγγιση έδωσαν την βάση για εκτενέστερη έρευνα σε αυτήν την περιοχή. Πιο συγκεκριμένα, το ευρετικό που πρότειναν στηρίζεται στην δομή του *γράφου στοιχειοσυνόλων*. Η είσοδος στον αλγόριθμο καθαρισμού είναι ένα σύνολο από συχνά στοιχειοσύνολα που πρέπει να αποκρυφθούν. Ο αλγόριθμος αρχικά ταξινομεί τα στοιχειοσύνολα αυτά με βάση την υποστήριξή τους και έπειτα προσπαθεί να τα κρύψει όλα, ένα ανά την φορά. Μετά από κάθε πέρασμα., ο αλγόριθμος παρακολουθεί τα πρόσφατα κρυμμένα συχνά στοιχειοσύνολα, και εκτελεί μια αναζήτηση στον κατάλογο εναπομεινάντων συχνών στοιχειοσυνόλων. Εάν υπάρχει ένα στοιχειοσύνολο στον κατάλογο το οποίο κρύβεται μετά από το παρόν βήμα, ο αλγόριθμος αφαιρεί αυτό το itemset από τον κατάλογο εναπομεινάντων στοιχειοσυνόλων. Βασικά, ο αλγόριθμος διαπερνά τον κατάλογο των στοιχειοσυνόλων, και εκτελεί μία από-κάτω-προς-τα-πάνω που ακολουθείται μία από-πάνω-προς-τα-κάτω διάσχιση του γράφου. Σε κάθε διάσχιση, η υποστήριξη του υπό ανίχνευση συχνού στοιχειοσυνόλου μειώνεται κατά ένα.

5.2.2.1.2 Η Επέκταση της Αρχικής Ιδέας

Συνέχεια της προηγούμενης ιδέας αποτελεί το [4], όπου οι συγγραφείς παρουσιάζουν έναν τρόπο μετασχηματισμού μιας βάσης δεδομένων D σε μια νέα D' η οποία *μεγιστοποιεί* τον αριθμό των κανόνων στο $R–R_h$ οι οποίοι μπορούν να ανακαλυφθούν. Υπάρχουν δύο βασικές προσεγγίσεις οι οποίες μπορούν να υιοθετηθούν όταν προσπαθούμε να αποκρύψουμε ένα σύνολο κανόνων R_h, σύμφωνα με τους συγγραφείς: μπορούμε είτε να κρύψουμε τα συχνά σύνολα από τα οποία προέρχονται, είτε να μειώσουμε την εμπιστοσύνη τους κάτω από ένα ορισμένο από τον χρήστη κατώφλι (*min_conf*). Πιο συγκεκριμένα γίνονται οι εξής πέντε υποθέσεις:

- Θέλουμε να αποκρύψουμε κανόνες συσχέτισης μειώνοντας είτε την υποστήριξή τους, είτε την εμπιστοσύνη τους.
- Επιλέγουμε να μειώσουμε είτε την υποστήριξη, είτε την εμπιστοσύνη με βάση τις παρενέργειες στην πληροφορία που δεν είναι ευαίσθητη.
- Κρύβουμε έναν κανόνα την φορά.
- Μείνουμε κατά μία μονάδα την υποστήριξη (ή την εμπιστοσύνη).
- Κρύβουμε μόνο ξένους κανόνες.

Σύμφωνα με την πρώτη υπόθεση μπορούμε να επιλέξουμε να κρύψουμε έναν κανόνα με την αλλαγή είτε της εμπιστοσύνης του, είτε της υποστήριξής του, αλλά όχι και των δύο. Με τη χρησιμοποίηση αυτής της υπόθεσης, μπορούμε με συνέπεια να αξιολογήσουμε κάθε τεχνική χωρίς οποιεσδήποτε αλληλεπιδράσεις από άλλα ευρετικά.

Με βάση τη δεύτερη υπόθεση, προκειμένου να μειωθούν η εμπιστοσύνη ή η υποστήριξη ενός κανόνα, είτε μετατρέπουμε σε 0 την τιμή ενός μη-μηδενικού αντικειμένου σε μια συγκεκριμένη δοσοληψία, ή μετατρέπουμε σε 1 όλα τα μηδενικά αντικείμενα σε μια δοσοληψία που υποστηρίζει μερικώς ένα itemset.

Η τρίτη υπόθεση δηλώνει ότι η απόκρυψη ενός κανόνα πρέπει να θεωρηθεί ως ατομική λειτουργία. Αυτό υπονοεί ότι το κρύψιμο δύο χωριστών κανόνων πρέπει να πραγματοποιηθεί κατά τρόπο διαδοχικό, με το κρύψιμο ενός κανόνα μετά από τον άλλο.

Η τέταρτη υπόθεση είναι βασισμένη στο minimality των αλλαγών στην αρχική βάση δεδομένων. Με την αλλαγή της εμπιστοσύνης ή της υποστήριξης κάθε κανόνα, ένα βήμα τη φορά, ενεργούμε φιλενεργά στην ελαχιστοποίηση των παρενεργειών των ευρετικών απόκρυψης.

Η πέμπτη υπόθεση δηλώνει ότι κρύβουμε μόνο τους κανόνες που περιλαμβάνουν ξένα σύνολα αντικειμένων. Σε μια διαφορετική κατάσταση, οι αλληλεπιδράσεις μεταξύ των κανόνων (δηλαδή κοινά υποσύνολα των αντικειμένων) πρέπει να εξεταστούν εκ των προτέρων.

Έχοντας λοιπόν τις παραπάνω υποθέσεις και την σχέση της εμπιστοσύνης με την υποστήριξη $Conf(X \Rightarrow Y) = \frac{Supp(X \cup Y)}{Supp(X)}$, καταλήγουμε στις εξής τρεις στρατηγικές για την απόκρυψη των κανόνων συσχέτισης:

1. Μειώνουμε την εμπιστοσύνη του κανόνα
   (a) με την αύξηση της υποστήριξης του πρότερου X, μέσω των δοσοληψιών που υποστηρίζουν μερικώς και το X και το Y.
   (b) με τη μείωση της υποστήριξης του ακόλουθου Y, στις δοσοληψίες που υποστηρίζουν και το X και το Y.
2. Μειώνουμε την υποστήριξη του κανόνα
   (a) με τη μείωση της υποστήριξης είτε του πρότερου X, είτε του ακόλουθου Y.

Με βάση αυτές τις στρατηγικές οι Danessi et.al. πρότειναν τρεις αλγορίθμους, έναν για κάθε μία στρατηγική, οι οποίοι και παρουσιάζονται στην συνέχεια.

5.2.2.1.2.a. Ο Αλγόριθμος RCTc

Ο αλγόριθμος που παρουσιάζεται εδώ προσπαθεί να κρύψει τους κανόνες με βάση την πρώτη στρατηγική: για κάθε επιλεγμένο κανόνα, αυξάνει την υποστήριξη του πρότερου τμήματος του κανόνα (*lhs(U)*), έως ότου η εμπιστοσύνη του κανόνα πέσει κάτω από το κατώφλι *min_conf*.

Πιο συγκεκριμένα ο αλγόριθμος μετρά πόσα από αντικείμενα του πρότερου τμήματος είναι σε κάθε δοσοληψία του T, όπου T είναι το σύνολο των δοσοληψιών που υποστηρίζουν μερικώς το πρότερο τμήμα. Στη συνέχεια, ταξινομεί τις δοσοληψίες κατά φθίνοντα αριθμό αντικειμένων που περιέχονται στο πρότερο τμήμα, και επιλέγει την δοσοληψία με τον μεγαλύτερο αριθμό αντικειμένων. Τέλος, στην δοσοληψία που επιλέχθηκε μετατρέπει όλα τα bits σε άσσους όλα τα αντικείμενα που αντιπροσωπεύουν το πρότερο τμήμα, αυξάνει την υποστήριξη κατά μια μονάδα και ξαναϋπολογίζει την εμπιστοσύνη. Έτσι όλοι οι ευαίσθητοι κανόνες καθαρίζονται ώστε να έχουν εμπιστοσύνη μικρότερη από το *min_conf*. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [4].

5.2.2.1.2.b. Ο Αλγόριθμος RCTc2

Ο αλγόριθμος που παρουσιάζεται εδώ κρύβει τους κανόνες με βάση την δεύτερη στρατηγική. Μειώνει την υποστήριξη κάθε επιλεγμένου κανόνα ελαττώνοντας τη συχνότητα του ακόλουθου τμήματος (*rhs(U)*) στις δοσοληψίες που

υποστηρίζουν τον κανόνα. Αυτή η διαδικασία συνεχίζεται έως ότου η εμπιστοσύνη του κανόνα πέσει κάτω από το ελάχιστο κατώφλι.

Πιο συγκεκριμένα, ταξινομεί το T κατά αύξοντα αριθμό μεγέθους δοσοληψιών και επιλέγει αυτή με το μικρότερο μέγεθος. Στη συνέχεια, επιλέγει το αντικείμενο του ακόλουθου τμήματος του κανόνα με την μικρότερη επίπτωση στα (|rhs(U)| -1)-στοιχειοσύνολα. Τέλος, στην δοσοληψία που επιλέχθηκε μετατρέπει σε μηδέν το bit που αντιστοιχεί στο αντικείμενο που επιλέχθηκε στο προηγούμενο βήμα. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [4].

5.2.2.1.2.c. Ο Αλγόριθμος RSTcTs

Ο συγκεκριμένος αλγόριθμος μειώνει την συχνότητα των ευαίσθητων κανόνων έως ότου είτε η εμπιστοσύνη πέσει κάτω από το ελάχιστο κατώφλι *min_conf*, είτε η υποστήριξη πέσει κάτω από το ελάχιστο κατώφλι *min_supp*.
Πιο συγκεκριμένα, ο αλγόριθμος αυτός ταξινομεί το T κατά αύξοντα αριθμό μεγέθους δοσοληψιών και επιλέγει αυτή με το μικρότερο μέγεθος. Στη συνέχεια, επιλέγει το αντικείμενο του κανόνα με την μικρότερη επίπτωση στα (|U|-1)-στοιχειοσύνολα. Τέλος, θέτει σε μηδέν το bit που αντιστοιχεί στο αντικείμενο που επελέγει στο προηγούμενο βήμα. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [4].

5.2.2.1.3 Απόκρυψη Κανόνων με Αφαίρεση Ανεξάρτητων Αντικειμένων από τις Δοσοληψίες

Στα πλαίσια της εργασίας που εισήχθη στο [40], οι συγγραφείς δεν εισάγουν θόρυβο στην βάση δεδομένων μετατρέποντας κάποια αντικείμενα από 0 σε 1 σε κάποιες δοσοληψίες, αλλά αφαιρούν επιλεκτικά ανεξάρτητα αντικείμενα από ευαίσθητες δοσοληψίες, αποτρέποντας έτσι την κοινοποίηση κάποιων προτύπων, ενώ ταυτοχρόνως διατηρούν όσο το δυνατόν περισσότερη από την αρχική πληροφορία για τις υπόλοιπες εφαρμογές. Για να το πετύχουν αυτό, προτείνουν ένα πλαίσιο το οποίο αποτελείται από την βάση δεδομένων, ένα ευρετήριο, ένα σύνολο από αλγορίθμους καθαρισμού και μια μηχανή ανάκτησης δοσοληψιών.

Το ευρετήριο είναι μια δομή που περιλαμβάνει το λεξιλόγιο και τα περιστατικά και αποτελεί μια πολύ αποδοτική μέθοδο ευρετηρίασης μιας βάσης

δεδομένων, με σκοπό την επιτάχυνση της στοιχειώδους εργασίας έρευνας. Στο πλαίσιο που παρουσιάζεται, το λεξιλόγιο αποτελείται από όλα τα διαφορετικά αντικείμενα στη βάση δεδομένων, και για κάθε αντικείμενο υπάρχει ένας αντίστοιχος κατάλογος IDs δοσοληψιών στον οποίο το αντικείμενο είναι παρόν. Για ένα δεδομένο αντικείμενο, μια πρόσβαση αρκεί για να βρεθεί ο κατάλογος με όλα τα IDs δοσοληψιών που περιέχουν το αντικείμενο. Τα περιστατικά με τα IDs δοσοληψιών δημιουργούνται και ταυτόχρονα ταξινομούνται κατά αύξουσα σειρά IDs. Κατά συνέπεια, στην αναζήτηση του ID μιας δοσοληψίας ενός ιδιαίτερου αντικειμένου, χρησιμοποιούμε μια δυαδική αναζήτηση.

Η μηχανή ανάκτησης δοσοληψιών Αποδέχεται τα αιτήματα για τις δοσοληψίες από έναν αλγόριθμο καθαρισμού, καθορίζει πώς αυτά τα αιτήματα μπορούν να εκπληρωθούν (συμβουλευμένη το ευρετήριο), επεξεργάζεται τις ερωτήσεις χρησιμοποιώντας μια γλώσσα βασισμένη στο Boolean μοντέλο, και επιστρέφει τα αποτελέσματα στον αλγόριθμο καθαρισμού. Η διαδικασία για τις ευαίσθητες δοσοληψίες μέσω της βάσης δεδομένων λειτουργεί στο ευρετήριο.

Οι αλγόριθμοι καθαρισμού που προτείνονται για να καθαρίσουν μια βάση δεδομένων απαιτούν μια επιπλέον ανίχνευση στη αρχική βάση D έτσι ώστε να αλλάξει κάποιες ευαίσθητες δοσοληψίες, ενώ θα διατηρήσει τις υπόλοιπες άθικτες. Επιπλέον, μια αρχική ανίχνευση είναι απαραίτητη για να χτίσει το ευρετήριο. Στις περισσότερες περιπτώσεις, μια ευαίσθητη δοσοληψία περιέχει περισσότερα από ένα περιοριστικά πρότυπα. Αναφερόμαστε σε αυτές τις δοσοληψίες ως *συγκρουόμενες δοσοληψίες* αφού η τροποποίηση μιας από αυτές έχει αντίκτυπος σε άλλα περιοριστικά πρότυπα ή ακόμα και μη-περιοριστικά. Ο βαθμός των συγκρούσεων μιας ευαίσθητης δοσοληψίας ορίζεται ως ο αριθμός των περιοριστικών προτύπων που μπορούν να εξαχθούν από την ευαίσθητη δοσοληψία.

Όλοι οι αλγόριθμοι έχουν ουσιαστικά τέσσερα σημαντικά βήματα:

1. Προσδιορισμός των ευαίσθητων δοσοληψιών για κάθε περιοριστικό πρότυπο.
2. Για κάθε περιοριστικό πρότυπο, προσδιορισμός ενός αντικειμένου που πρέπει να αποβληθεί από τις ευαίσθητες δοσοληψίες. Αυτό το υποψήφιο αντικείμενο καλείται αντικείμενο-θύμα.
3. Με βάση ένα κατώφλι κοινοποίησης ψ που καθορίζεται από τον χρήστη, υπολογίζεται για κάθε περιοριστικό πρότυπο ο αριθμός των ευαίσθητων δοσοληψιών που πρέπει να καθαριστούν και

4. Με βάση τον αριθμό που βρίσκεται στο βήμα 3, προσδιορίζονται για κάθε περιοριστικό πρότυπο οι ευαίσθητες δοσοληψίες που πρέπει να καθαριστούν και αφαιρούνται τα αντικείμενα-θύματα από αυτές.

Οι αλγόριθμοι καθαρισμού διαφέρουν κυρίως στο βήμα 2, με τον τρόπο δηλαδή που προσδιορίζουν ένα αντικείμενο-θύμα για να το αφαιρέσουν από τις ευαίσθητες δοσοληψίες για κάθε περιοριστικό πρότυπο, και στο βήμα 4 όπου επιλέγονται οι ευαίσθητες δοσοληψίες που καθαρίζονται. Τα βήματα 1 και 3 παραμένουν ουσιαστικά τα ίδια για όλες τις προσεγγίσεις

5.2.2.1.3.α. Ο Αλγόριθμος AllPV

Η βασική ιδέα πίσω από τον αλγόριθμο AllPV είναι να επιλεχτούν όλα τα αντικείμενα σε ένα δεδομένο περιοριστικό πρότυπο ως θύματα. Η λογική πίσω από αυτήν την επιλογή είναι ότι με την αφαίρεση από τις ευαίσθητες δοσοληψίες των αντικειμένων ενός περιοριστικού προτύπου, ένα τέτοιο πρότυπο θα κρυφτεί. Εάν μια ευαίσθητη δοσοληψία περιέχει ακριβώς τα ίδια αντικείμενα με ένα περιοριστικό πρότυπο, ο αλγόριθμος AllPV αφαιρεί όλα τα αντικείμενα αυτής της δοσοληψίας εκτός από το αντικείμενο με την υψηλότερη συχνότητα στη βάση δεδομένων. Επειδή ένα αντικείμενο πρέπει να κρατηθεί, ο αριθμός δοσοληψιών δεν αλλάζει.

Η επιλογή των ευαίσθητων δοσοληψιών που θα καθαριστούν είναι βασισμένη απλά στο βαθμό των συγκρούσεων. Λαμβάνοντας υπόψη τον αριθμό ευαίσθητων δοσοληψιών που αλλάζουν, και με βάση το ψ, αυτή η προσέγγιση επιλέγει για κάθε περιοριστικό πρότυπο τις δοσοληψίες με το μικρότερο βαθμό συγκρούσεων. Η λογική είναι, όπως ανωτέρω, να ελαχιστοποιήσει τον αντίκτυπο του καθαρισμού στην ανακάλυψη των νόμιμων προτύπων.

Τα τέσσερα βήματα σε αυτόν τον αλγόριθμο αντιστοιχούν στα τέσσερα βήματα που περιγράφονται ανωτέρω για όλους του αλγορίθμους. Το πρώτο βήμα χτίζει ένα ευρετήριο του αντικειμένου στη D σε μια ανίχνευση της βάσης δεδομένων. Η υποστήριξη κάθε αντικειμένου στη βάση δεδομένων υπολογίζεται επίσης κατά τη διάρκεια αυτής της ανίχνευσης και συνδέεται με τα αντίστοιχα αντικείμενα στο ευρετήριο. Αυτή η υποστήριξη των αντικειμένων χρησιμοποιείται στο δεύτερο βήμα για να προσδιορίσει τα αντικείμενα-θύματα για κάθε περιοριστικό πρότυπο. Για τον αλγόριθμο AllPV, όλα τα αντικείμενα σε ένα δεδομένο περιοριστικό πρότυπο

επιλέγονται. Στο τρίτο βήμα χρησιμοποιείται το ψ για να υπολογιστεί ο αριθμός των δοσοληψιών που θα καθαριστούν. Υπάρχει πραγματικά μόνο μια ανίχνευση της βάσης δεδομένων στην εφαρμογή του τέταρτου βήματος. Συναλλαγές που δεν χρειάζονται καθαρισμό αντιγράφονται άμεσα από τη D στη D', ενώ άλλες καθαρίζονται πριν αντιγραφούν στη D'. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [40].

5.2.2.1.3.b. Ο Αλγόριθμος MinFPV

Η βασική ιδέα πίσω από τον MinFPV, είναι να επιλεχτεί ως αντικείμενο-θύμα,, για ένα δεδομένο περιοριστικό πρότυπο, το περιοριστικό αντικείμενο προτύπων με τη μικρότερη υποστήριξη στο πρότυπο. Η λογική πίσω από αυτήν την επιλογή είναι ότι με την αφαίρεση του αντικειμένου από τις ευαίσθητες δοσοληψίες με τη μικρότερη υποστήριξη θα ασκήσει μικρότερη επίδραση στη βάση δεδομένων και τα νόμιμα πρότυπα.

Η επιλογή των ευαίσθητων δοσοληψιών που θα καθαριστούν είναι απλά βασισμένη στο βαθμό των συγκρούσεών τους. Λαμβάνοντας υπόψη τον αριθμό ευαίσθητων δοσοληψιών που αλλάζουν, και με βάση το ψ, αυτή η προσέγγιση επιλέγει για κάθε περιοριστικό πρότυπο τις δοσοληψίες με το μικρότερο βαθμό συγκρούσεων. Η λογική είναι, όπως ανωτέρω, να ελαχιστοποιήσει τον αντίκτυπο του καθαρισμού στην ανακάλυψη των νόμιμων προτύπων.

Τα τέσσερα βήματα αυτού του αλγορίθμου αντιστοιχούν σε εκείνα του AllPV αλγορίθμου. Η μόνη διαφορά είναι ότι ο MinFPV επιλέγει ακριβώς ένα αντικείμενο-θύμα, όπως προαναφέρθηκε. Αντίθετα από τον MinFPV, η ιδέα πίσω από τον MaxFIA, είναι να επιλεγεί ως αντικείμενο-θύμα, για ένα δεδομένο περιοριστικό πρότυπο, το αντικείμενο με τη μέγιστη υποστήριξη. Οι αλγόριθμοι MinFPV και MaxFIA είναι έτσι εννοιολογικά πολύ παρόμοιοι. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [40].

5.2.2.1.3.c. Ο Αλγόριθμος GrPV

Η βασική ιδέα πίσω από τον GrPV, είναι να ομαδοποιηθούν τα περιοριστικά πρότυπα σε ομάδες προτύπων που μοιράζονται τα ίδια στοιχειοσύνολα. Εάν δύο πρότυπα τέμνονται, με τον καθαρισμό των ευαίσθητων δοσοληψιών που περιέχουν

και τα δύο περιοριστικά πρότυπα, κάποιος θα μπορούσε να κρύψει αυτά τα δύο πρότυπα και αμέσως να μειώσει την επιρροή στη βάση δεδομένων. Παρόλα αυτά, η συσταδοποίηση των περιοριστικών προτύπων βασισμένων στις τομές μεταξύ των αντικειμένων στα πρότυπα οδηγεί σε ομάδες που επικαλύπτονται δεδομένου ότι η τομή των στοιχειοσυνόλων δεν είναι μεταβατική. Με τον υπολογισμό της επικάλυψης μεταξύ των συστάδων και την απομόνωση των ομάδων, μπορούμε να χρησιμοποιήσουμε έναν αντιπρόσωπο του στοιχειοσυνόλου που συνδέει τα περιοριστικά πρότυπα στην ίδια ομάδα, δηλαδή ένα αντικείμενο-θύμα για όλα τα πρότυπα στην ομάδα. Με την αφαίρεση του αντικειμένου-θύματος από τις ευαίσθητες δοσοληψίες σχετικές με τα πρότυπα στην ομάδα, όλα τα περιοριστικά πρότυπα στην ομάδα θα αποκρυφθούν σε ένα βήμα. Αυτό πάλι θα ελαχιστοποιούσε την επιρροή στη βάση δεδομένων και θα μείωνε το πιθανό τυχαίο κρύψιμο των νόμιμων προτύπων.

Σε αυτόν τον αλγόριθμο, τα βήματα 1 και 3 είναι ίδια με τα αντίστοιχα του MinFPV. Το βήμα 4 είναι ελαφρώς αλλαγμένο από το βήμα 4 του MinFPV αφού πλέον οι ευαίσθητες δοσοληψίες ταξινομούνται σε φθίνουσα σειρά βαθμού συγκρούσεων έτσι ώστε περισσότερες συγκρουόμενες δοσοληψίες να επιλέγονται για καθαρισμό. Ο λόγος είναι ότι αφού το αντικείμενο-θύμα αντιπροσωπεύει τώρα ένα σύνολο περιοριστικών προτύπων (από την ίδια ομάδα), ο καθαρισμός μιας συγκρουόμενης δοσοληψίας θα επιτρέψει σε πολλά περιοριστικά πρότυπα να τακτοποιηθούν ανά καθαρισμένη δοσοληψία. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [40].

5.2.2.1.4 Αλγόριθμοι για την Εξισορρόπηση Μεταξύ Κοινοποίησης και Προστασίας Γνώσης

Το [41] αποτελεί μια επέκταση στην ουσία του [40], αφού πλέον γίνεται λόγος για ευαίσθητους κανόνες συσχέτισης αντί για περιοριστικά πρότυπα, αν και αυτές οι δύο έννοιες είναι αλληλένδετες. Έτσι λοιπόν, το πλαίσιο προσαρμόζεται στους κανόνες συσχέτισης, δηλαδή όλες οι πράξεις γίνονται σε κανόνες.

Οι αλγόριθμοι καθαρισμού τροποποιούν μερικές δοσοληψίες για να κρύψουν τους ευαίσθητους κανόνες με βάση το κατώφλι κοινοποίησης ψ που ελέγχεται από τον ιδιοκτήτη της βάσης δεδομένων. Αυτό το κατώφλι ελέγχει έμμεσα την ισορροπία μεταξύ της κοινοποίησης γνώσης και της προστασίας γνώσης με τον έλεγχο του

ποσοστού των δοσοληψιών που καθαρίζονται. Παραδείγματος χάριν, εάν ψ = 50%, τότε οι μισές από τις ευαίσθητες δοσοληψίες θα καθαριστούν, όταν ψ = 0%, όλες οι ευαίσθητες δοσοληψίες θα καθαριστούν, και όταν ψ = 100% δεν θα καθαριστεί καμία ευαίσθητη δοσοληψία. Με άλλα λόγια, αντιπροσωπεύει την αναλογία των ευαίσθητων δοσοληψιών που πρέπει να αφεθούν άθικτες. Το πλεονέκτημα αυτού του κατωφλίου είναι ότι επιτρέπει έναν συμβιβασμό μεταξύ της απόκρυψης των κανόνων συσχέτισης, μη γνωρίζοντας τους μη-ευαίσθητους, και της εύρεσης όλων των μη-ευαίσθητων κανόνων συσχέτισης αλλά αποκαλύπτοντας τους ευαίσθητους.

Οι αλγόριθμοι καθαρισμού εφαρμόζονται στην αρχική βάση δεδομένων για να παραγάγουν την καινούρια.

Όλοι οι αλγόριθμοι έχουν ουσιαστικά τέσσερα σημαντικά βήματα:

5. Προσδιορισμός των ευαίσθητων δοσοληψιών για κάθε ευαίσθητο κανόνα.
6. Για κάθε ευαίσθητο κανόνα, προσδιορισμός ενός αντικειμένου που πρέπει να αποβληθεί από τις ευαίσθητες δοσοληψίες. Αυτό το υποψήφιο αντικείμενο καλείται αντικείμενο-θύμα.
7. Με βάση το κατώφλι κοινοποίησης ψ που καθορίζεται από τον χρήστη, υπολογίζεται για κάθε ευαίσθητο κανόνα ο αριθμός των ευαίσθητων δοσοληψιών που πρέπει να καθαριστούν και
8. Με βάση τον αριθμό που βρίσκεται στο βήμα 3, προσδιορίζονται για κάθε ευαίσθητο κανόνα οι ευαίσθητες δοσοληψίες που πρέπει να καθαριστούν και αφαιρούνται τα αντικείμενο-θύματα από αυτές.

Οι αλγόριθμοι καθαρισμού διαφέρουν κυρίως στο βήμα 2, με τον τρόπο δηλαδή που προσδιορίζουν ένα αντικείμενο-θύμα για να το αφαιρέσουν από τις ευαίσθητες δοσοληψίες για κάθε ευαίσθητο κανόνα, και στο βήμα 4 όπου επιλέγονται οι ευαίσθητες δοσοληψίες που καθαρίζονται. Τα βήματα 1 και 3 παραμένουν ουσιαστικά τα ίδια για όλες τις προσεγγίσεις.

Οι αλγόριθμοι που εισήχθησαν σε αυτήν την προσέγγιση περιγράφονται στην συνέχεια.

5.2.2.1.4.a. Ο Αλγόριθμος SrbPV

Η βασική ιδέα πίσω από το SrbPV, είναι ότι αντί να επιλέγουμε ένα μοναδικό αντικείμενο-θύμα ανά δεδομένο ευαίσθητο κανόνα συσχέτισης, επιλέγουμε

διαφορετικά αντικείμενα-θύματα σε κάθε γύρο, αρχίζοντας από το πρώτο αντικείμενο, έπειτα το δεύτερο και ου το καθεξής σε κάθε ευαίσθητη δοσοληψία. Η διαδικασία αρχίζει πάλι από το πρώτο αντικείμενο του ευαίσθητου κανόνα ως αντικείμενο-θύμα κάθε φορά που φτάνουμε στο τελευταίο αντικείμενο. Η λογική πίσω από αυτήν την επιλογή είναι ότι η αφαίρεση ενός αντικειμένου τη φορά από τις ευαίσθητες δοσοληψίες θα ελαχιστοποιήσει τον αριθμό μη-ευαίσθητων κανόνων που αφαιρούνται ως παρενέργεια, δεδομένου ότι αυτή η στρατηγική προσπαθεί να ισορροπήσει τη μείωση της υποστήριξης των αντικειμένων στους ευαίσθητους κανόνες συσχέτισης.

Η επιλογή των ευαίσθητων δοσοληψιών που θα καθαριστούν είναι απλά βασισμένη στο βαθμό των συγκρούσεών τους. Λαμβάνοντας υπόψη τον αριθμό ευαίσθητων δοσοληψιών που αλλάζουν, και με βάση το ψ, αυτή η προσέγγιση επιλέγει για κάθε ευαίσθητο κανόνα τις δοσοληψίες των οποίων ο βαθμός συγκρούσεων ταξινομείται σε φθίνουσα σειρά. Η λογική είναι να επιταχυνθεί η διαδικασία καθαρισμού και να ελαχιστοποιηθεί ο αντίκτυπος στην ανακάλυψη των νόμιμων κανόνων.

Τα τέσσερα βήματα αυτού του αλγορίθμου αντιστοιχούν στα τέσσερα βήματα που περιγράφονται στο προηγούμενο τμήμα. Το πρώτο βήμα χτίζει ένα ευρετήριο των αντικειμένων στη D σε μια ανίχνευση της βάσης δεδομένων. Στο βήμα 2, το αντικείμενο-θύμα επιλέγεται κατά **Round Robin**, για κάθε ευαίσθητο κανόνα συσχέτισης. Στο βήμα 3 χρησιμοποιείται το ψ για να υπολογίσει αριθμός των δοσοληψιών που θα καθαριστούν. Υπάρχει πραγματικά μόνο μια ανίχνευση της βάσης δεδομένων στην εφαρμογή του βήματος 4. Συναλλαγές που δεν χρειάζονται καθαρισμό αντιγράφονται άμεσα από τη D στη D', ενώ άλλες καθαρίζονται πριν αντιγραφούν στη D'. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [41].

5.2.2.1.4.b. Ο Αλγόριθμος SrPV

Η βασική ιδέα πίσω από τον SrPV είναι η τυχαία επιλογή ενός αντικειμένου από μια δοσοληψία ως αντικείμενο-θύμα. Τα επιλεγμένα αντικείμενα για κάθε κανόνα αφαιρούνται, ένα κάθε φορά, από τις ευαίσθητες δοσοληψίες που συνδέονται με τον κανόνα. Όπως ο SrbPV, η λογική πίσω από αυτήν την επιλογή είναι ότι η αφαίρεση των διαφορετικών αντικειμένων από τις ευαίσθητες δοσοληψίες θα μείωνε

ελαφρώς την υποστήριξη των μη-ευαίσθητων κανόνων συσχέτισης που θα ήταν διαθέσιμοι για να εξαχθούν στην καθαρισμένη βάση δεδομένων.

Η επιλογή των ευαίσθητων δοσοληψιών για καθαρισμό είναι απλά βασισμένη στο βαθμό των συγκρούσεών τους. Η επιλογή των ευαίσθητων δοσοληψιών γίνεται κατά φθίνουσα σειρά.

Τα τέσσερα βήματα αυτών των αλγορίθμων αντιστοιχούν σε εκείνοι στο SrbPV. Η μόνη διαφορά είναι ότι ο SrPV επιλέγει το αντικείμενο-θύμα τυχαία, ενώ ο SrbPV επιλέγει το αντικείμενο-θύμα εκ περιτροπής. Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [41].

5.2.2.1.5 Απόκρυψη Ευαίσθητων Κανόνων Ανεξαρτήτως Μεγέθους της Βάσης Δεδομένων

Το επόμενο βήμα στην εξέλιξη των αλγορίθμων αποτελεί η προσέγγιση που εισήχθη στο [42]. Πρόκειται για έναν αποδοτικό αλγόριθμο ο οποίος απαιτεί μόνο ένα πέρασμα στη βάση δεδομένων ανεξάρτητα από το μέγεθος της και τον αριθμό των ευαίσθητων κανόνων συσχέτισης που πρέπει να προστατευθούν. Αυτό αντιπροσωπεύει μια σημαντική βελτίωση πέρα από τους προηγούμενους αλγορίθμους, οι οποίοι απαιτούν διάφορες ανιχνεύσεις ανάλογα με τον αριθμό κανόνων συσχέτισης που πρέπει να κρυφτούν.

Επιπλέον εισάγεται η έννοια του κατωφλίου κοινοποίησης για *κάθε* ενιαίο πρότυπο που περιορίζει. Με άλλα λόγια, αντί να κατέχουμε ένα ενιαίο κατώφλι ψ για ολόκληρη τη διαδικασία καθαρισμού, μπορούμε να έχουμε διαφορετικό κατώφλι ψ_i για κάθε πρότυπο i που τίθεται υπό περιορισμό. Αυτό παρέχει μια μεγαλύτερη ευελιξία που επιτρέπει σε έναν κάτοχο δεδομένων να βάλει διαφορετικά βάρη σε διαφορετικούς κανόνες.

Ο αλγόριθμος για τον οποίο έγινε λόγος, παρουσιάζεται στην συνέχεια.

5.2.2.1.5.α. Ο Αλγόριθμος WPVTp

Η κεντρική ιδέα πίσω από τον WPVTp είναι να ανιχνεύσει μια ομάδα από K δοσοληψίες (μέγεθος παραθύρου) και να καθαρίσει έπειτα το σύνολο των ευαίσθητων κανόνων που μπορούν να εξαχθούν από αυτές τις K δοσοληψίες.

Η διαδικασία έχει στην ουσία πέντε βήματα τα οποία και περιγράφονται στην συνέχεια:

1. Για κάθε δοσοληψία που διαβάζεται από τη βάση δεδομένων D, προσδιορίζουμε εάν είναι ευαίσθητη. Αν όχι, η δοσοληψία αντιγράφεται άμεσα στην καθαρισμένη βάση δεδομένων D'.
2. Επιλέγουμε το αντικείμενο-θύμα στους ευαίσθητους κανόνες συσχέτισης σχετικούς με την παρούσα ευαίσθητη δοσοληψία, με την υψηλότερη συχνότητα. Διαφορετικά, το αντικείμενο-θύμα επιλέγεται τυχαία.
3. Λαμβάνοντας υπόψη το κατώφλι κοινοποίησης ψ, υπολογίζουμε τον αριθμό δοσοληψιών που καθαρίζονται.
4. Ταξινομούμε, κατά αύξουσα σειρά μεγέθους, τις ευαίσθητες δοσοληψίες που υπολογίζονται στο προηγούμενο βήμα, για κάθε ευαίσθητο κανόνα. Κατά συνέπεια, αρχίζουμε από τις πιο σύντομες δοσοληψίες δεδομένου ότι οι πιο σύντομες δοσοληψίες έχουν τους λιγότερους συνδυασμούς κανόνων συσχέτισης. Αυτό ελαχιστοποιεί τον αντίκτυπο στην καθαρισμένη βάση δεδομένων.
5. Κάθε περιοριστικός κανόνας έχει τώρα έναν κατάλογο IDs ευαίσθητων δοσοληψιών με το αντίστοιχο επιλεγμένο αντικείμενο-θύμα τους. Κάθε φορά που αφαιρούμε ένα αντικείμενο-θύμα από μια ευαίσθητη δοσοληψία, εκτελείται μια διαδικασία πρόβλεψης για να ελεγχθεί εάν εκείνη η δοσοληψία έχει επιλεγεί ως ευαίσθητη δοσοληψία για άλλους ευαίσθητους κανόνες. Σε αυτή την περίπτωση, και αν το αντικείμενο-θύμα που αφαιρέθηκε ακριβώς από την παρούσα δοσοληψία είναι επίσης μέρος του άλλου ευαίσθητου κανόνα, αφαιρείται η δοσοληψία από τον κατάλογο IDs δοσοληψιών. Με αυτό τον τρόπο, η δοσοληψία θα καθαριστεί, και θα αντιγραφεί έπειτα στην αποστειρωμένη βάση δεδομένων D'.
6. Η διαίσθηση πίσω από τον WPVTp είναι ότι ανιχνεύει μια ομάδα δοσοληψιών K, σε ένα πέρασμα. Κατόπιν, καθαρίζει το σύνολο των ευαίσθητων δοσοληψιών με βάση ένα κατώφλι ψ. Για κάθε ευαίσθητο κανόνα συσχέτισης υπάρχει ένα ψ που ανατίθεται σε αυτό.

Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [42].

5.2.2.2. Αλγόριθμοι Διαμοιρασμού Προτύπων

5.2.2.2.1 Ασφαλής Διαμοιρασμός Κανόνων Συσχέτισης

Το μόνο αντιπροσωπευτικό δείγμα εργασίας αυτής της κατηγορίας αλγορίθμων αποτελεί το [43], όπου εισάγεται η έννοια του καθαρισμού κανόνων. Στην προσέγγιση αυτή πλέον δεν γίνεται προσπάθεια καθαρισμού των δοσοληψιών, αλλά των κανόνων που προκύπτουν από μια βάση δεδομένων. Έτσι λοιπόν, μπορούμε να ορίσουμε το πρόβλημα ως εξής:

> *Έστω D μια βάση δεδομένων δοσοληψιών, R είναι ένα σύνολο όλων των κανόνων συσχέτισης που μπορούν να εξαχθούν από την D βασιζόμενοι σε μια ελάχιστη υποστήριξη s, και S_R είναι ένα σύνολο κανόνων υποστήριξης απόφασης που πρέπει να προστατευτούν σύμφωνα με κάποιες πολιτικές ασφάλειας. Ο στόχος είναι να μετασχηματιστεί το R στο R', όπου το R' παριστάνει το σύνολο των κανόνων που διαμοιράζονται.*

Στους Αλγορίθμους Διαμοιρασμού Προτύπων, εμφανίζεται ένα κανάλι συμπεράσματος όταν κάποιος εξάγει ένα καθαρισμένο σύνολο κανόνων και, βασισμένος στους μη-ευαίσθητους κανόνες, συνάγει έναν ή περισσότερους ευαίσθητους κανόνες που υποτίθεται ότι δεν πρέπει να ανακαλυφθούν.
Ο αλγόριθμος που προσδοκεί να επιλύσει το προηγούμενο πρόβλημα παρουσιάζεται στην συνέχεια.

5.2.2.2.1.a. Ο Αλγόριθμος GPSh

Η ιδέα πίσω από τον GPSh, είναι να καθαριστούν μερικοί ευαίσθητοι κανόνες εμποδίζοντας επίσης και τα κανάλια συμπεράσματος. Για να εμποδίσει τα κανάλια συμπεράσματος, ο GPSh αφαιρεί τουλάχιστον ένα υποσύνολο κάθε ευαίσθητου στοιχειοσυνόλου στο επίπεδο 1 του γράφου στοιχειοσυνόλων. Η αφαίρεση γίνεται κατ' επανάληψη μέχρι το επίπεδο 1. Ο GPSh αρχίζει από το επίπεδο 1 επειδή υποθέτουμε ότι οι κανόνες συσχέτισης που ανακτώνται από τα καθαρισμένα στοιχειοσύνολα (κοινά στοιχειοσύνολα) έχουν τουλάχιστον 2 αντικείμενα.
Η διαδικασία έχει τρία βήματα τα οποία είναι τα εξής:

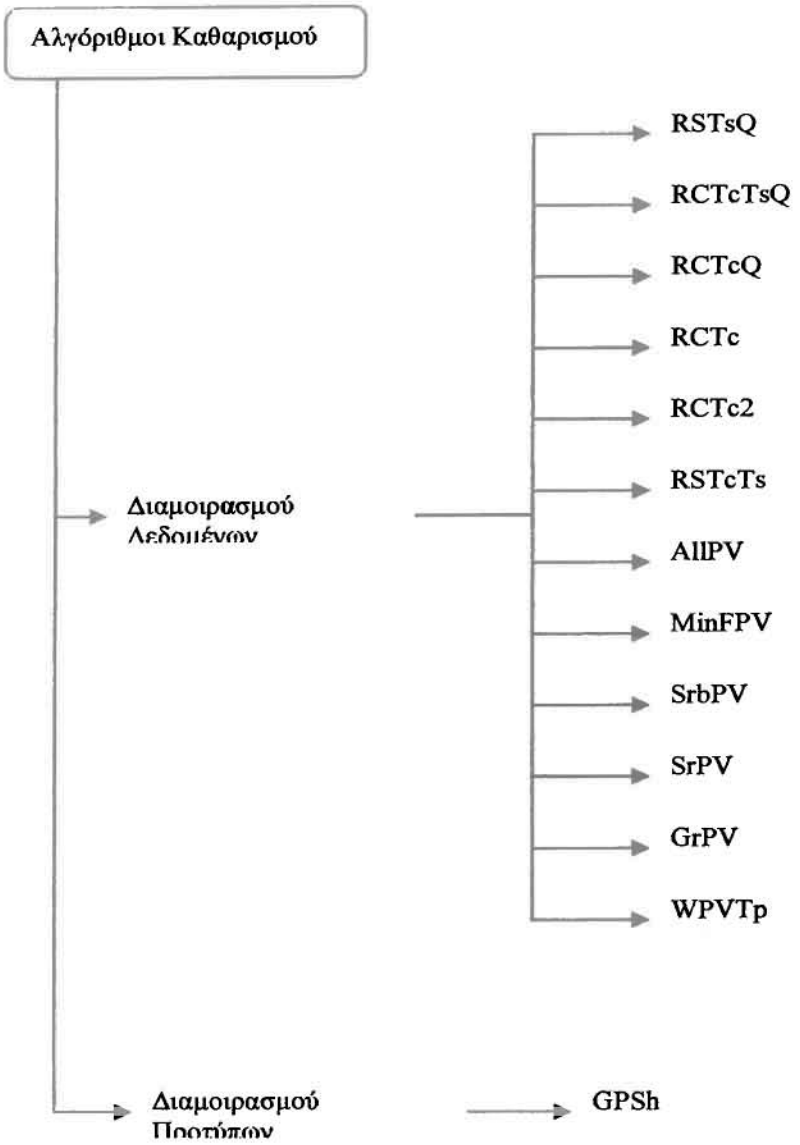
1. Μετατροπή κάθε ευαίσθητου κανόνα σε ένα αντίστοιχο στοιχειοσύνολο.

2. Για κάθε στοιχειοσύνολο του προηγούμενου βήματος, υπολογίζονται τα υποσύνολα του. Γενικά, τα υποσύνολα για κάθε κανόνα επιλέγονται από το επίπεδο 1 του γράφου στοιχειοσυνόλων.
3. Αφαίρεση όλων των υπερσυνόλων των κανόνων που πρέπει να καθαριστούν.

Ο ψευδοκώδικας του αλγορίθμου μπορεί να βρεθεί στο [43].

5.3. Η Βιβλιοθήκη των Αλγορίθμων Καθαρισμού

Στο εδάφιο αυτό δίνεται μια διαγραμματική παρουσίαση όλων των αλγορίθμων που παρουσιάστηκαν στο προηγούμενο εδάφιο. Στην Εικόνα 4 φαίνεται μια ταξινόμηση των αλγορίθμων καθαρισμού.



Εικόνα 4: Ταξινόμηση των αλγορίθμων καθαρισμού

Στους μεν, οι πράξεις διαδικασίας καθαρισμού δρουν στα δεδομένα για να αφαιρεθεί ή να αποκρυφθεί η ομάδα των ευαίσθητων κανόνων συσχέτισης που αντιπροσωπεύουν την ευαίσθητη γνώση. Για να ολοκληρωθεί αυτό, ένας μικρός αριθμός δοσοληψιών που συμμετέχουν στην παραγωγή των ευαίσθητων κανόνων πρέπει να είναι μετατραπεί με τη διαγραφή ενός ή περισσότερων αντικειμένων από αυτούς. Με αυτό τον τρόπο, οι αλγόριθμοι κρύβουν τους ευαίσθητους κανόνες με τη μείωση είτε της υποστήριξής τους είτε της εμπιστοσύνης τους κάτω από ένα κατώφλι ιδιωτικότητας (κατώφλι κοινοποίησης). Στους δε, οι πράξεις αλγορίθμου καθαρισμού δρουν στους κανόνες που εξάγονται από μια βάση δεδομένων, αντί στα ίδια τα

δεδομένα. Ο αλγόριθμος αφαιρεί όλους τους ευαίσθητους κανόνες πριν από τη διαδικασία διαμοιρασμού.

Κεφάλαιο 6

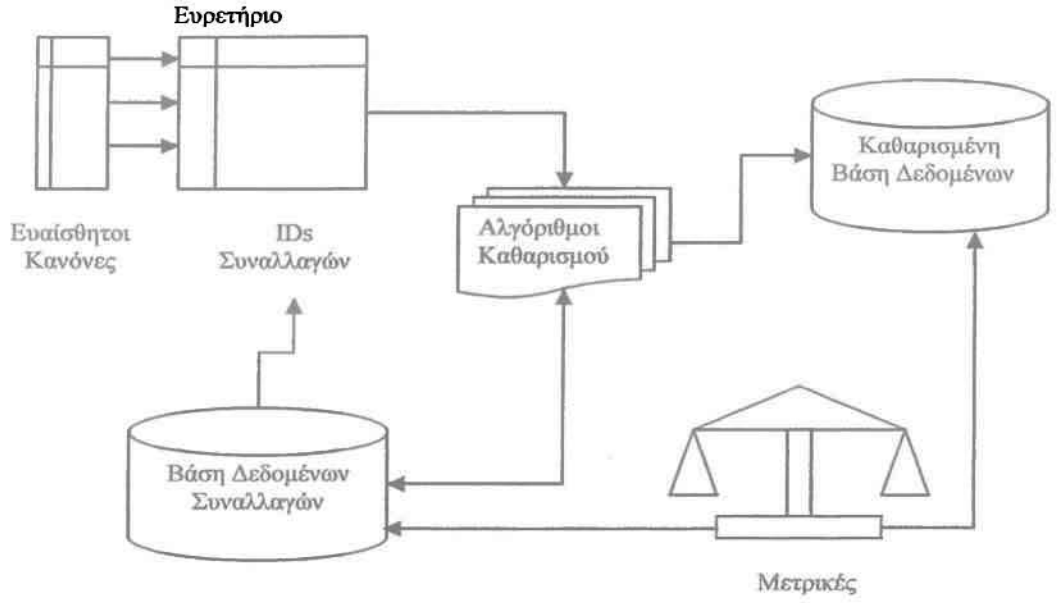
Αξιολόγηση των Αλγορίθμων Καθαρισμού

Για να γίνουν πιο σαφή τα όσα περιγράφτηκαν στα προηγούμενα κεφάλαια, εκτελέσαμε μια σειρά από πειράματα πάνω στους αλγορίθμους καθαρισμού. Πιο συγκεκριμένα, επιλέξαμε ένα αντιπροσωπευτικό υποσύνολο των αλγορίθμων του κεφαλαίου 5, και με βάση κάποιες μετρικές, οι οποίες ορίζονται στο 6.1, προσπαθήσαμε να αξιολογήσουμε την απόδοση και την αποτελεσματικότητα των εν λόγω αλγορίθμων. Στην παράγραφο 6.2 περιγράφονται οι βάσεις δεδομένων που χρησιμοποιήθηκαν για τον πειραματισμό, οι αλγόριθμοι που επιλέχθηκαν και η μεθοδολογία πάνω στην οποία στηρίχτηκαν τα πειράματά μας. Στην παράγραφο 6.3 γίνεται η αξιολόγηση των αλγορίθμων καθαρισμού και η παρουσίαση των αποτελεσμάτων. Τέλος, στην παράγραφο 6.4 παρατίθενται τα συμπεράσματα που προκύπτουν από τα πειράματά μας και γίνεται μια συζήτηση πάνω σε αυτά.

6.1. Το Σύνολο των Μετρικών

Σε αυτό το τμήμα, εισάγουμε το σύνολο των μετρικών που ποσολογούν όχι μόνο πόση ευαίσθητη γνώση έχει αποκαλυφθεί, αλλά και την αποτελεσματικότητα των προτεινόμενων αλγορίθμων από την άποψη της απώλειας πληροφοριών και από την άποψη των μη-ευαίσθητων κανόνων που αφαιρούνται ως παρενέργεια της

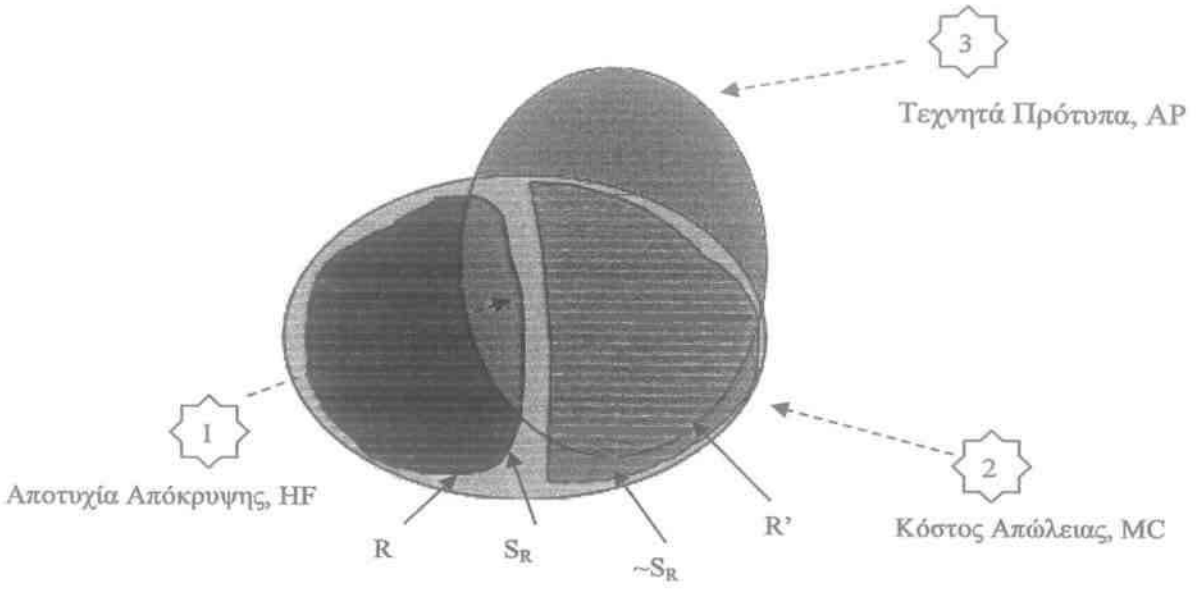
διαδικασίας μετασχηματισμού [40]. Ο τρόπος που εφαρμόζονται οι τεχνικές φαίνεται στην Εικόνα 5.



Εικόνα 5: Αναπαράσταση του πλαισίου για τη Διατήρηση Ιδιωτικότητας στην Εξόρυξη Κανόνων Συσχέτισης

Οι μετρικές που παρουσιάζονται συσχετίζονται με τα προβλήματα που διευκρινίζονται στην Εικόνα 6.

Αυτή η εικόνα εμφανίζει τη σχέση μεταξύ του συνόλου R όλων των κανόνων συσχέτισης στη βάση δεδομένων D, των ευαίσθητων κανόνων S_R, των μη-ευαίσθητων κανόνων συσχέτισης $\sim S_R$, καθώς επίσης και του συνόλου R' των κανόνων που ανακαλύπτονται από την καθαρισμένη βάση D'.



Εικόνα 6: Προβλήματα που προκύπτουν από την διαδικασία καθαρισμού (πηγή: [40])

Οι κύκλοι με τους αριθμούς 1, 2 και 3 είναι πιθανά προβλήματα που αντιπροσωπεύουν αντίστοιχα τους ευαίσθητους κανόνες συσχέτισης που απέτυχαν να κρυφτούν, τους νόμιμους κανόνες που απέτυχαν να κρυφτούν, και τους τεχνητούς κανόνες συσχέτισης που δημιουργούνται με τη διαδικασία καθαρισμού, αντίστοιχα.

Το πρόβλημα 1 εμφανίζεται όταν ανακαλύπτονται μερικοί ευαίσθητοι κανόνες συσχέτισης στην καθαρισμένη βάση δεδομένων. Καλείται *Αποτυχία Απόκρυψης* (HF), και μετριέται με το ποσοστό των ευαίσθητων κανόνων συσχέτισης που ανακαλύπτονται από την D'.

$$HF = \frac{\#S_R(D')}{\#S_R(D)},$$

όπου $\#S_R(D)$ δηλώνει τον αριθμό των ευαίσθητων κανόνων συσχέτισης που ανακαλύπτονται από την βάση D. Ιδανικά, το HF πρέπει να είναι 0%.

Το πρόβλημα 2 εμφανίζεται όταν κρύβονται μερικοί νόμιμοι κανόνες συσχέτισης ως παρενέργεια της διαδικασίας sanitization. Αυτό συμβαίνει όταν μερικοί μη-ευαίσθητοι κανόνες συσχέτισης χάνουν υποστήριξη στη βάση δεδομένων λόγω της διαδικασίας καθαρισμού. Το πρόβλημα καλείται *Κόστος Απώλειας* (MC), και μετριέται με το ποσοστό των νόμιμων κανόνων συσχέτισης που δεν ανακαλύπτονται από την D'. Στην ιδανική περίπτωση, αυτό πρέπει επίσης να είναι 0%. Το Κόστος Απώλειας υπολογίζεται ως εξής:

$$MC = \frac{\#\sim S_R(D) - \#\sim S_R(D')}{\#\sim S_R(D)},$$

όπου $\#\sim S_R(D)$ δηλώνει τον αριθμό των μη-ευαίσθητων κανόνων συσχέτισης που ανακαλύπτονται από την βάση D.

Παρατηρούμε ότι υπάρχει ένας συμβιβασμός μεταξύ του MC και του HF. Όσο πιο πολλούς ευαίσθητους κανόνες κρύβουμε, τόσο πιο πολλούς μη-ευαίσθητους κανόνες χάνουμε. Αυτό καθορίζεται βασικά από το κατώφλι κοινοποίησης, το οποίο μας δίνει την δυνατότητα να βρούμε την ισορροπία μεταξύ της ιδιωτικότητας και της κοινοποίησης των πληροφοριών όποτε η εφαρμογή το επιτρέπει.

Το πρόβλημα 3 εμφανίζεται όταν παράγονται μερικοί τεχνητοί κανόνες συσχέτισης από την D' ως προϊόν της διαδικασίας καθαρισμού. Καλούμε το πρόβλημα αυτό Τεχνητά Πρότυπα (AP), και μετριέται με το ποσοστό των ανακαλυπτόμενων κανόνων συσχέτισης που είναι τεχνητοί, δηλαδή κανόνες που δεν είναι παρόντες στην αρχική βάση δεδομένων. Οι τεχνητοί κανόνες παράγονται όταν προστίθενται νέα αντικείμενα σε μερικές δοσοληψίες για να αλλάξουν (μειωσουν) την εμπιστοσύνη των ευαίσθητων κανόνων. Παραδείγματος χάριν, σε έναν κανόνα $X \Rightarrow Y$, εάν τα αντικείμενα προστίθενται στο πρότερο τμήμα X αυτού του κανόνα, στις δοσοληψίες που υποστηρίζουν το X και όχι το Y, τότε η εμπιστοσύνη ενός τέτοιου κανόνα μειώνεται. Τα Τεχνητά Πρότυπα μετριούνται ως εξής:

$$AP = \frac{|R'| - |R \cap R'|}{|R'|},$$

όπου |R|, δηλώνει τον αριθμό στοιχείων συνόλου του R.

6.2. Τα Βασικά Στοιχεία των Πειραμάτων

6.2.1. Οι Βάσεις Δεδομένων των Πειραμάτων

Ο έλεγχος των αλγορίθμων έγινε με χρήση πραγματικών βάσεων δεδομένων οι οποίες αποκτήθηκαν από το UCI Repository of Machine Learning Databases [53], το Frequent Itemset Mining Dataset Repository [54], καθώς επίσης και από τον IBM Quest Market-Basket Synthetic DataGenerator [55]. Πιο συγκεκριμένα, οι πραγματικές βάσεις που χρησιμοποιήσαμε είναι οι: Chess, Mushroom, Pumsb, Connect, Accidents, Kosarak ενώ αυτές που πήραμε από το εργαλείο της IBM είχαν μεταβλητό μέγεθος εγγραφών από 150K εως 900K εγγραφές. Γενικές πληροφορίες

για κάθε βάση δεδομένων μπορεί να βρεθεί στην εκάστοτε τοποθεσία. Ο παρακάτω πίνακας δείχνει συγκεντρωτικά στοιχεία για τις βάσεις δεδομένων. Οι στήλες αντιπροσωπεύουν το όνομα της βάσης δεδομένων, τον αριθμό των εγγραφών, τον αριθμό των αντικειμένων, το μέσο αριθμό αντικειμένων ανα εγγραφή (δοσοληψία), το μέγεθος της μικρότερης εγγραφής, και το μέγεθος της μεγαλύτερης εγγραφής, αντίστοιχα.

Βάση Δεδομένων	**Πλήθος Εγγραφών**	**Πλήθος Αντικειμένων**	**Μέσο Μέγεθος**	**Μικρότερη Εγγραφή**	**Μεγαλύτερη Εγγραφή**
Chess	3.196	75	37	37	37
Mushroom	8.124	119	23	23	23
Pumsb	49.046	2.113	74	74	74
Connect	67.557	129	43	43	43
Accidents	340.183	468	33.81	18	51
Kosarak	990.573	41.270	8.10	1	1.065

Πίνακας 3: Τα χαρακτηριστικά των βάσεων δεδομένων των πειραμάτων

6.2.2. Οι Αλγόριθμοι Καθαρισμού

Οι αλγόριθμοι του κεφαλαίου 5 που χρησιμοποιήθηκαν για να γίνουν οι συγκρίσεις είναι οι εξής:

Ο GrPV ομαδοποιεί τους ευαίσθητους κανόνες συσχέτισης σε ομάδες κανόνων που μοιράζονται τα ίδια στοιχειοσύνολα. Αν δύο ή περισσότεροι κανόνες τέμνονται, καθαρίζοντας το κοινό αντικείμενο αυτών των ευαίσθητων κανόνων μπορούν να αποκρυφθούν αυτοί οι κανόνες σε ένα βήμα.

Ο SrbPV επιλέγει διαφορετικά αντικείμενα-θύματα κάθε φορά, ξεκινώντας από το πρώτο, έπειτα το δεύτερο και ου το καθεξίς στο σύνολο των ευαίσθητων δοσοληψιών. Η διαδικασία ξεκινά ξανά από το πρώτο αντικείμενο του ευαίσθητου κανόνα που επιλέγεται ως αντικείμενο-θύμα κάθε φορά που φτάνουμε στο τελευταίο αντικείμενο.

Ο SrPV επιλέγει τυχαία ένα αντικείμενο-θύμα για ένα δεδομένο ευαίσθητο κανόνα. Για κάθε ευαίσθητη δοσολοψία που συσχετίζεται με έναν ευαίσθητο κανόνα ο SrPV επιλέγει

Ο WPVTp σαρώνει ένα σύνολο από K δοσοληψίες τη φορά και καθαρίζει τους ευαίσθητους κανόνες που βρίσκονται στις ευαίσθητες δοσοληψίες με βάση ένα κατώφλι κοινοποίησης που το ορίζει ο χρήστης. Η διαφορά είναι ότι μπορεί να οριστεί διαφορετικό κατώφλι για κάθε ευαίσθητο κανόνα.
Ο RSTcTs κρύβει τους ευαίσθητους κανόνες μειώνοντας την υποστήριξή τους.
Ο GPSh ενεργεί στους κανόνες που προκύπτουν από την βάση δεδομένων παρά στην ίδια τα δεδομένα της βάσης. Κρύβει τους κανόνες πριν τον διαμοιρασμό τους και έτσι η υποστήριξη και η εμπιστοσύνη των μη-ευαίσθητων κανόνων παραμένει αμετάβλητη

Ο λόγος που επιλέχθηκαν οι παραπάνω αλγόριθμοι είναι διότι αποτελούν ένα αντιπροσωπευτικό υποσύνολο των αλγορίθμων που μας βοηθάει να βγάλουμε γενικά συμπεράσματα για την συμπεριφορά των αλγορίθμων στο σύνολο τους.

6.2.3. Η Μεθοδολογία των Πειραμάτων

Όλα τα πειράματα έγιναν σε PC με επεξεργαστή Intel Pentium 4, με 1 GB μνήμης και λειτουργικό σύστημα SUSE Linux 9.2. Εκτελέσαμε δύο σειρές πειραμάτων. Η πρώτη σειρά είχε ως σκοπό να αξιολογηθεί η αποδοτικότητας των αλγορίθμων υπό εξέταση, ενώ η δεύτερη σειρά στόχευε στην αξιολόγηση της αποτελεσματικότητα τους. Και στις δύο περιπτώσεις προσπαθήσαμε να συμπεράνουμε αν οι αλγόριθμοι ανταποκρίνονται στον ορισμό της ΔΙΕΓ.

Τα πειράματά μας βασίστηκαν πάνω σε διαφορετικά σενάρια. Αρχικά, οι ευαίσθητοι κανόνες επιλέχθηκαν τυχαία από το σύνολο των κανόνων συσχέτισης της εκάστοτε βάσης δεδομένων. Έπειτα, επιλέξαμε τους ευαίσθητους κανόνες με βάση την μέγιστη τιμή υποστήριξης τους.

Με βάση λοιπόν τα παραπάνω σενάρια, τα βήματα της διαδικασίας σύγκρισης των αλγορίθμων ήταν:

1. Επιλογή των βάσεων δεδομένων στις οποίες θα εκτελούσαμε την διαδικασία καθαρισμού.
2. Εφαρμογή ενός αλγορίθμου εξόρυξης κανόνων συσχέτισης από τις αρχικές βάσεις δεδομένων. Ο αλγόριθμος αυτός είναι ο Apriori ο οποίος ανακτήθηκε από το [56].

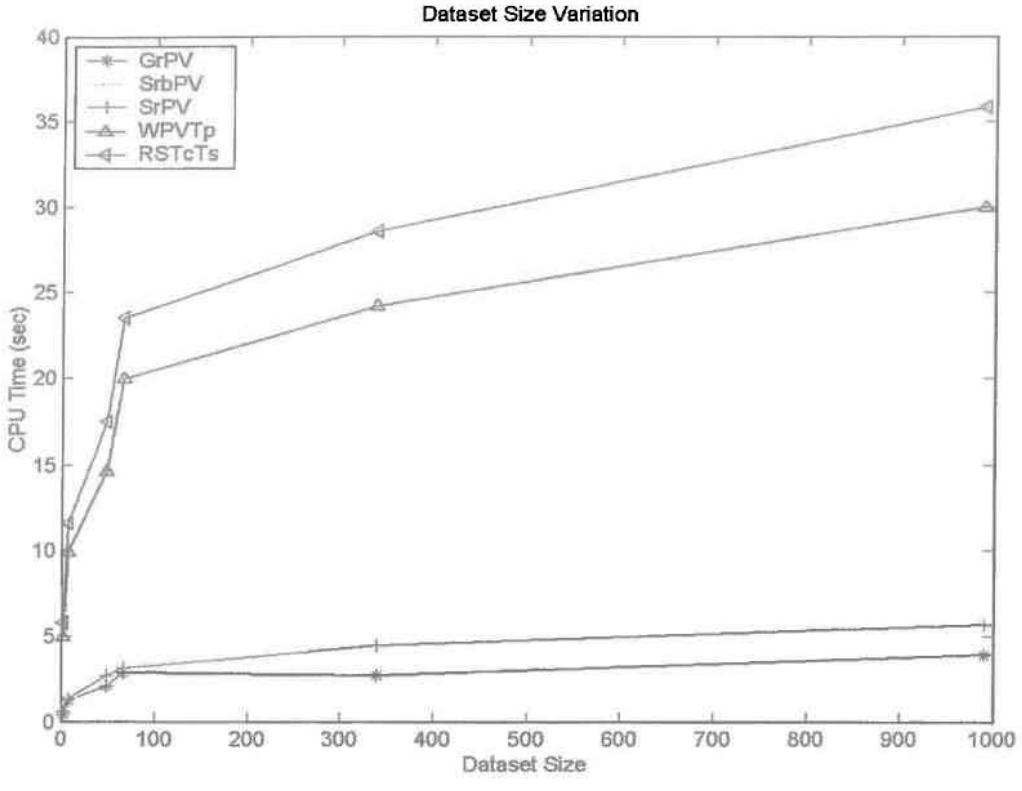
3. Εφαρμογή των αλγορίθμων που αναφέρθηκαν στο εδάφιο 6.2.2 στις βάσεις δεδομένων του εδαφίου 6.2.1 καθώς και σε βάσεις δεδομένων που παρήχθησαν με το [55].
4. Σύγκριση των αλγορίθμων καθαρισμού με βάση τους χρόνους εκτέλεσης και τις μετρικές που εισήχθησαν στην παράγραφο 6.1.

6.3. Αξιολόγηση των Αλγορίθμων Καθαρισμού

6.3.1. Αποδοτικότητα των Αλγορίθμων

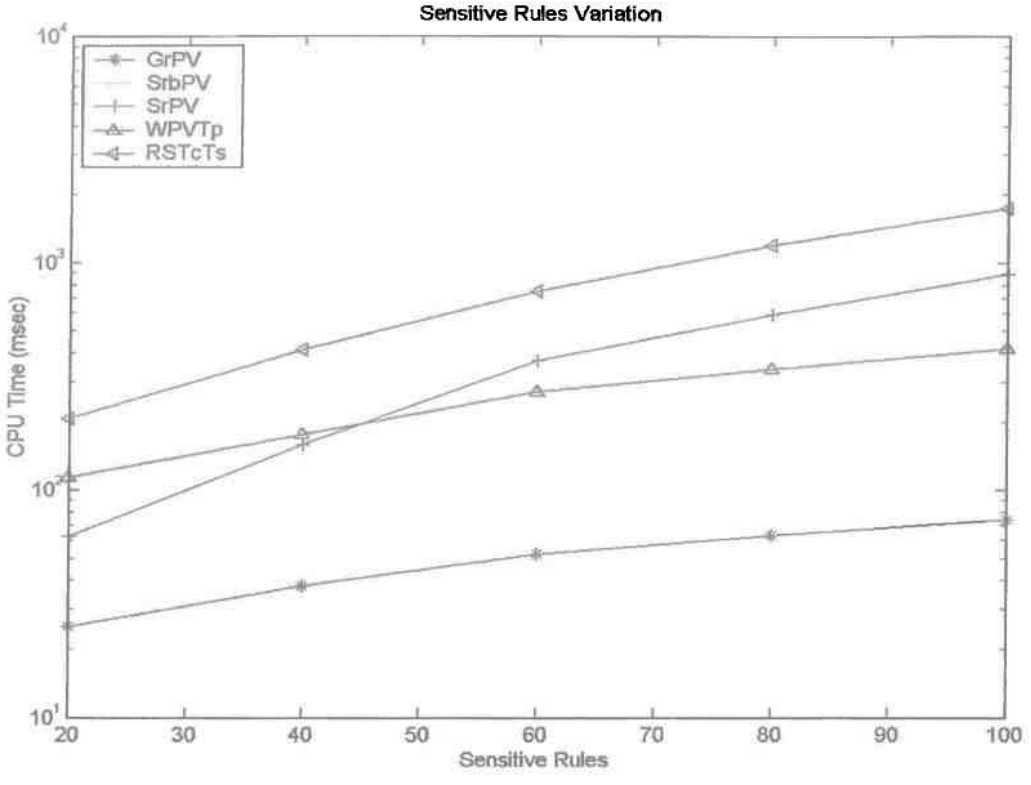
Για να εξετάσουμε τους χρόνους εκτέλεσης των αλγορίθμων, εκτελέσαμε πειράματα με διαφορετικού μεγέθους βάσεις δεδομένων, καθώς επίσης και με διαφορετικού πλήθους ευαίσθητους κανόνες.

Μεταβάλλαμε το μέγεθος της βάσης δεδομένων από 3K εως 900K περίπου θέλωντας να αποκρύψουμε 5 ευαίσθητους κανόνες συσχέτισης. Το κατώφλι κοινοποίησης διατηρήθηκε σταθερό στο 0%. Τα αποτελέσματα φαίνονται στην Εικόνα 7. Οι αλγόριθμοι GrPV, SrbPV, και SrPV πέτυχαν καλύτερους χρόνους απ'ότι οι RSTcTs και WPVTp. Πιο συγκεκριμένα ο RSTcTs απαιτεί 5 σαρώσεις στην αρχική βάση δεδομένων (μία για κάθε ευαίσθητο κανόνα), ενώ οι GrPV, SrbPV και SrPV απαιτούν μόνο 2. Όσον αφορά τον WPVTp, ο οποίος απαιτεί μόνο 1 σάρωση, εκτελεί πολλές εργασίες στην μνήμη (π.χ. ταξινόμηση των δοσοληψιών σε αύξουσα σειρά για κάθε παράθυρο) με αποτέλεσμα να έχει μεγαλύτερο χρόνο εκτέλεσης από τους GrPV, SrbPV, SrPV που ταξινομούν τις δοσοληψίες μόνο μια φορά.



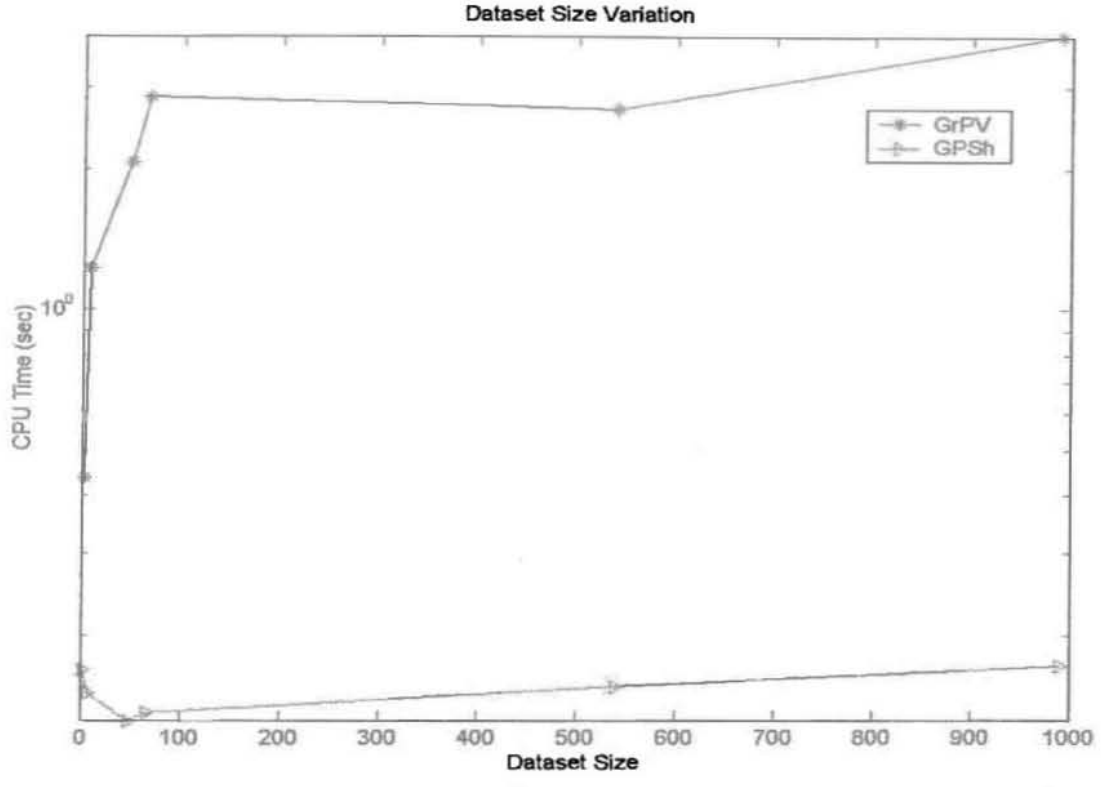
Εικόνα 7: Χρόνοι εκτέλεσης της διαδικασίας καθαρισμού με μεταβλητό μέγεθος βάσεων δεδομένων

Στην περίπτωση των πολλαπλών εκτελέσεων με διαφορετικού πλήθους ευαίσθητους κανόνες, χρησιμοποιήσαμε την βάση δεδομένων Connect. Μεταβάλλαμε το πλήθος των ευαίσθητων κανόνων προς απόκρυψη από 20 εως 100. Το κατώφλι κοινοποίησης διατηρήθηκε σταθερό στο 0%. Όπως φαίνεται στην Εικόνα 8, οι αλγόριθμοι συμπεριφέρονται πολύ ικανοποιητικά, με εξαίρεση τον RSTcTs ο οποίος απαιτεί πολλές σαρώσεις. Όσον αφορά τον GrPV, και σε αυτήν την περίπτωση συμπεριφέρεται καλύτερα από τον WPVTp, αν και απαιτεί δύο σαρώσεις. Ο λόγος είναι και πάλι ότι ο WPVTp εκτελεί πολλές εργασίες στην μνήμη. Επίσης, είναι αξιοσημείωτο ότι ο WPVTp μετά τους 40 κανόνες συμπεριφέρεται καλύτερα από τους SrbPV και SrPV, κι αυτό λόγω του ότι η λογική πίσω από τον WPVTp τον βελτιστοποιεί όταν υπάρχουν κανόνες με τομές αντικειμένων. Σημειώνεται ότι όταν αυξάνεται ο αριθμός των κανόνων, αυξάνεται επίσης και ο αριθμός των αντικειμένων που τέμνονται. Σε αυτήν την περίπτωση, ο WPVTp θα «αγγίξει» λιγότερες δοσοληψίες.

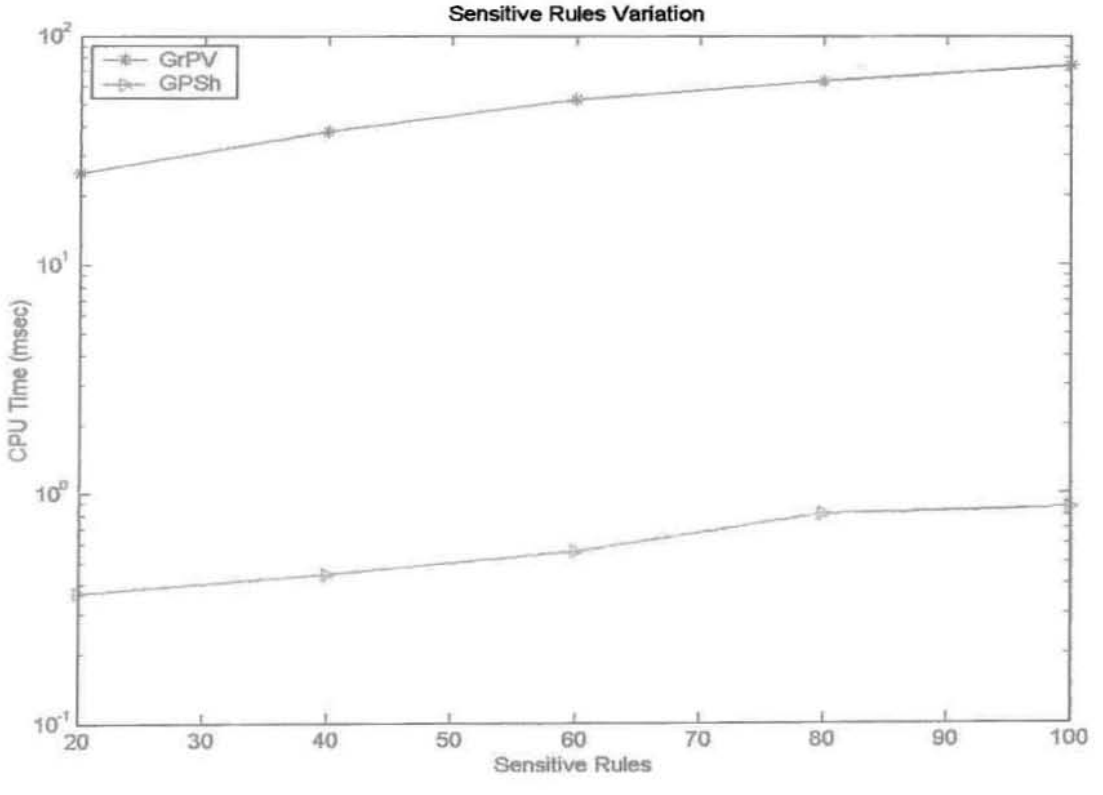


Εικόνα 8: Χρόνοι εκτέλεσης της διαδικασίας καθαρισμού με μεταβλητό πλήθος ευαίσθητων κανόνων συσχέτισης

Για να γίνει η σύγκριση των αλγορίθμων καθαρισμού πιο ολοκληρωμένη, συγκρίνουμε τον αλγόριθμο GrPV, που εμφάνισε τα καλύτερα αποτελέσματα από τους αλγορίθμους διαμοιρασμού δεδομένων, με τον αλγόριθμο της κατηγορίας διαμοιρασμού προτύπων, τον GPSh. Τα αποτελέσματα που επιστρέφονται για τις παραπάνω δύο περιπτώσεις φαίνονται στις Εικόνες 9 και 10 αντίστοιχα.



Εικόνα 9: Σύγκριση GrPV – GPSh για μεταβλητού μεγέθους βάσεις δεδομένων



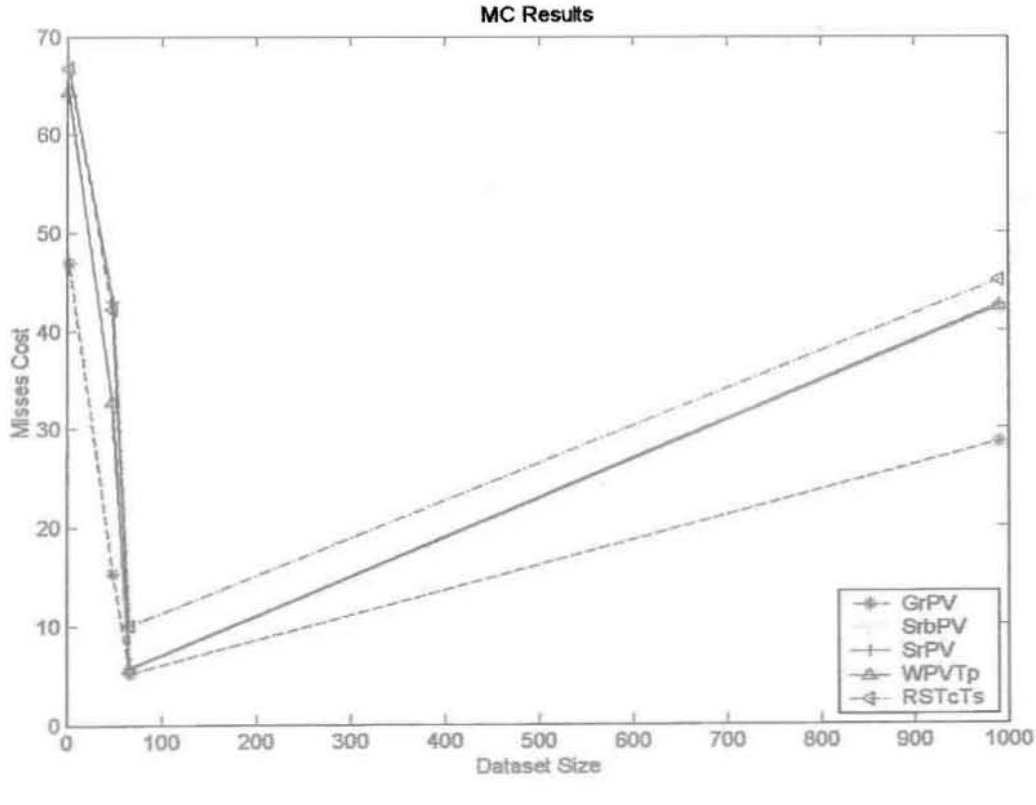
Εικόνα 10: Σύγκριση GrPV – GPSh για μεταβλητού πλήθους ευαίσθητους κανόνες

6.3.2. Αποτελεσματικότητα των Αλγορίθμων

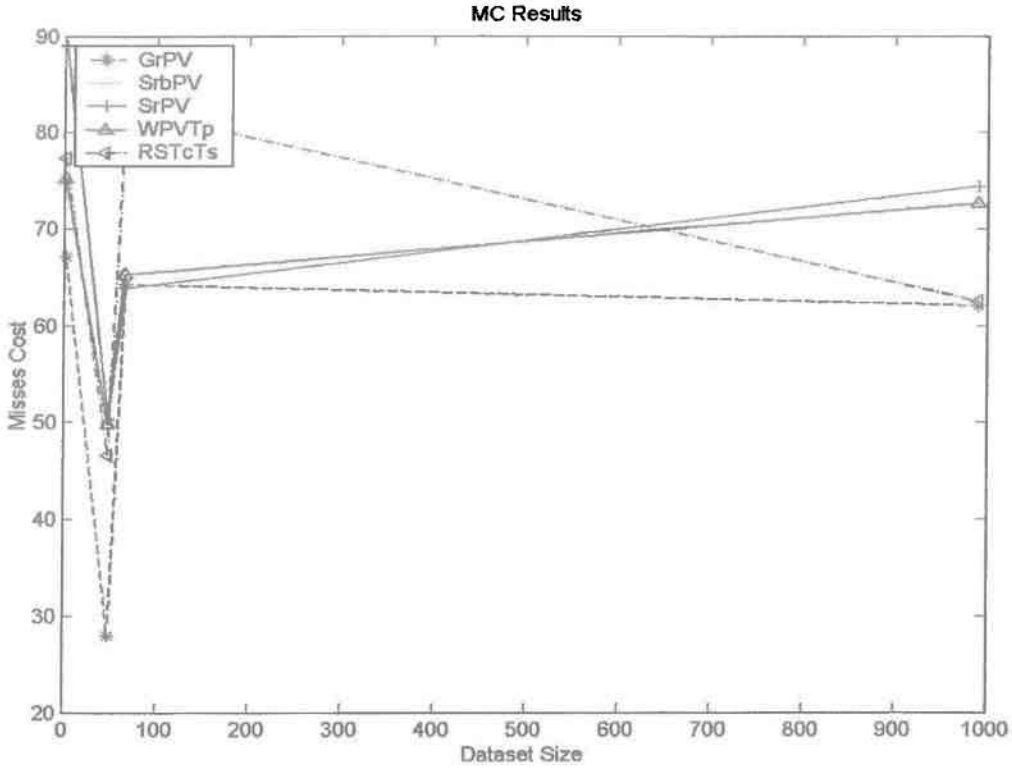
Η αποτελεσματικότητα των αλγορίθμων μετριέται σε αντιστοιχία προς το πλήθος των ευαίσθητων κανόνων συσχέτισης που αποκρύφθηκαν επιτυχώς, καθώς επίσης και προς το ποσοστό των μη-ευαίσθητων κανόνων που αποκρύφθηκαν κατά λάθος κατά την διαδικασία του καθαρισμού.

Για να εξετάσουμε την αποτελεσματικότητα των αλγορίθμων, αρχικά θέσαμε σταθερά το κατώφλι κοινοποίησης, την υποστήριξη, την εμπιστοσύνη και το πλήθος των ευαίσθητων κανόνων ($1^η$ περίπτωση). Έπειτα, μεταβάλλαμε το πλήθος των κανόνων ($2^η$ περίπτωση).

Διατηρώντας λοιπόν το κατώφλι στο 0%, την υποστήριξη στο 0.8, την εμπιστοσύνη στο 0.9 και το πλήθος των κανόνων στους 5 τα αποτελέσματα που παίρνουμε φαίνονται στην Εικόνα 11. Όπως παρατηρούμε, τα καλύτερα αποτελέσματα τα εμφανίζει ο GrPV. Στην περίπτωση που επιλέγονται κανόνες με τη μεγαλύτερη υποστήριξη τα αποτελέσματα φαίνονται στην Εικόνα 12, όπου και πάλι τα καλύτερα αποτελέσματα τα επιστρέφει ο GrPV με εξαίρεση την βάση δεδομένων Connect όπου ο SrPV έχει μικρότερο MC.

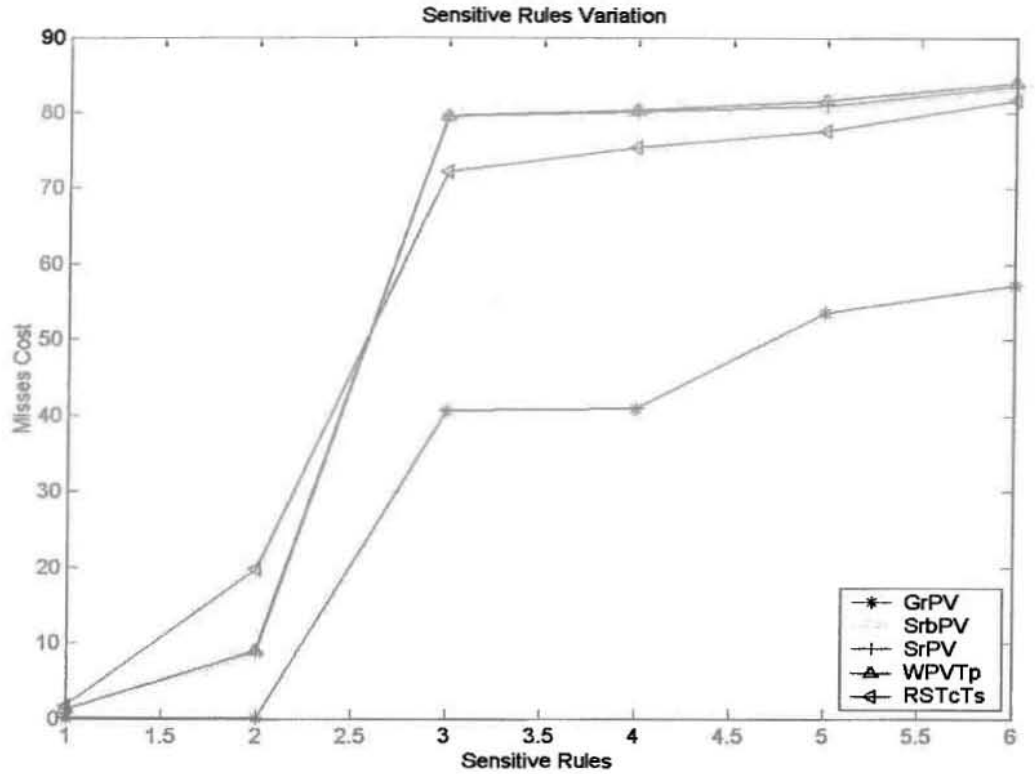


Εικόνα 11: Κόστος Απώλειας σε σχέση με το μέγεθος των βάσεων δεδομένων (τυχαίοι κανόνες)

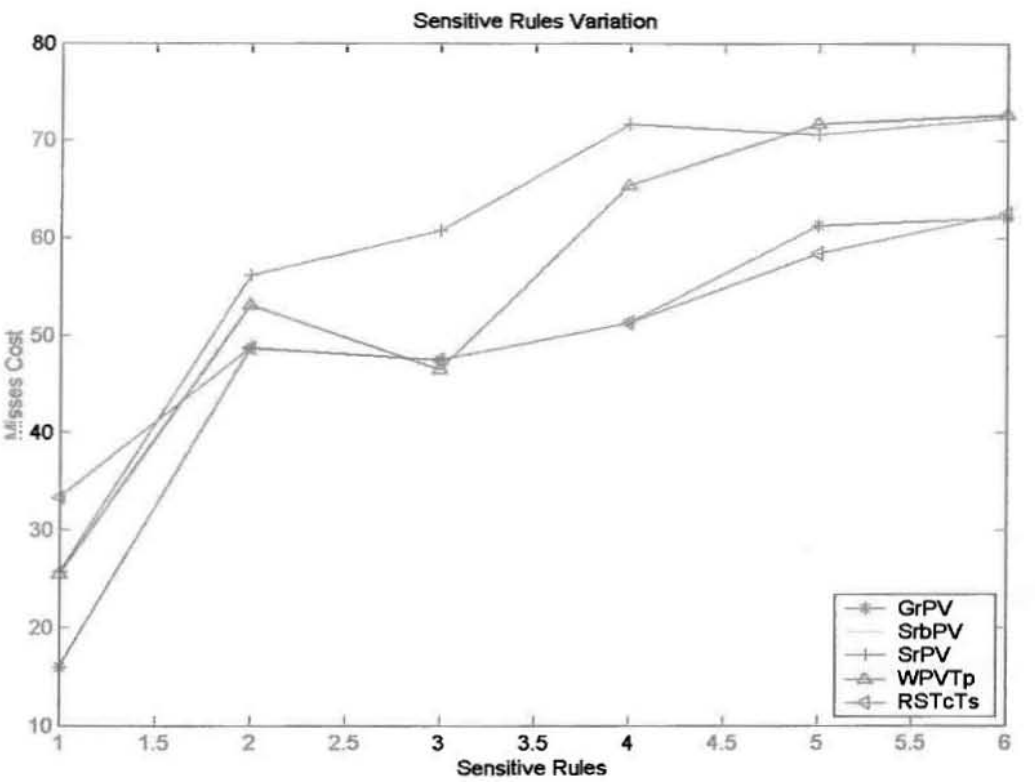


Εικόνα 12: Κόστος Απώλειας σε σχέση με το μέγεθος των βάσεων δεδομένων (κανόνες με υψηλή υποστήριξη)

Στην δεύτερη περίπτωση η παράμετρος που αλλάζουμε είναι το πλήθος των ευαίσθητων κανόνων. Η βάση δεδομένων που χρησιμοποιήθηκε και πάλι είναι η Connect. Τα αποτελέσματα που επιστρέφονται φαίνονται στις Εικόνες 13 και 14. Αυτό που παρατηρούμε είναι πως όσον αφορά το Κόστος Απώλειας, στις περισσότερες των περιπτώσεων ο αλγόριθμος που εμφανίζει τα καλύτερα αποτελέσματα είναι ο GrPV.

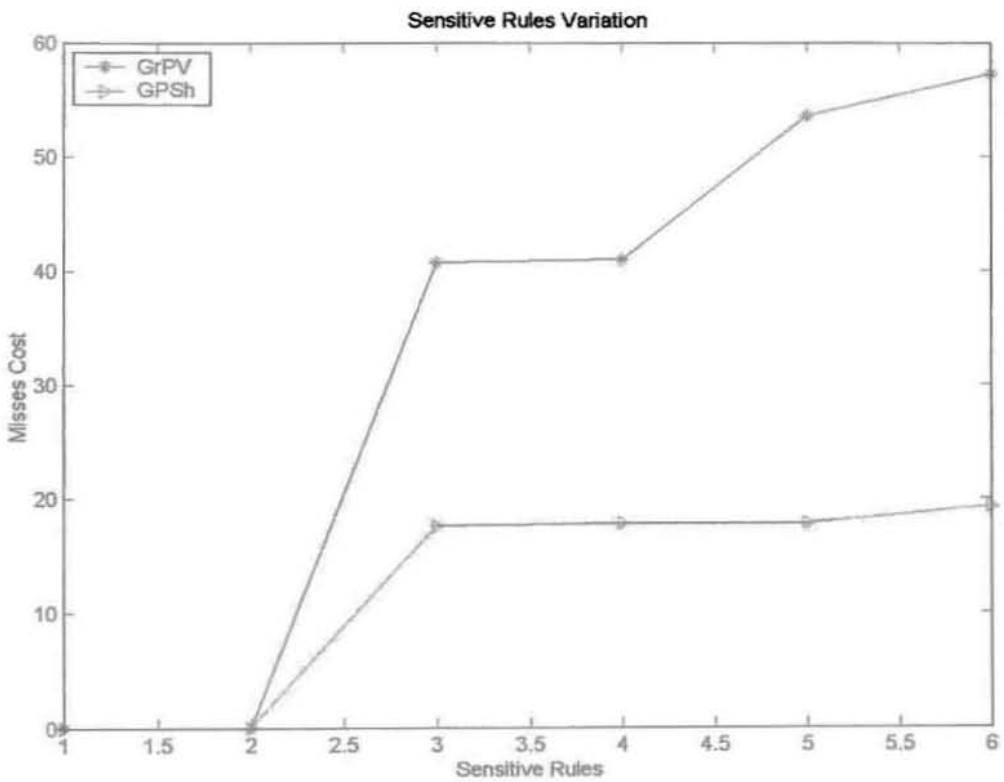


Εικόνα 13: Κόστος Απώλειας με μεταβλητό πλήθος κανόνων (τυχαίοι κανόνες)

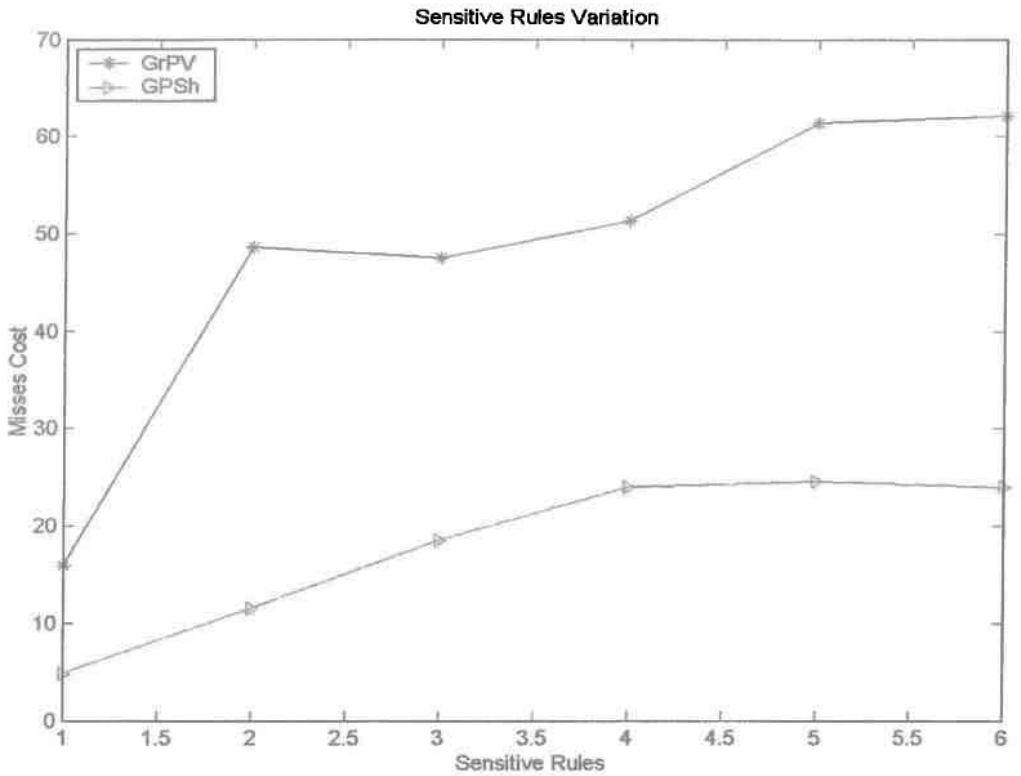


Εικόνα 14: Κόστος Απώλειας με μεταβλητό πλήθος κανόνων (κανόνες με υψηλή υποστήριξη)

Όπως και στην αξιολόγηση της αποδοτικότητας, έτσι και εδώ παραθέτουμε τα συγκριτικά αποτελέσματα του GrPV με τον GPSh. Στις Εικόνες 15 και 16 παρατηρούμε πως ο GPSh συμπεριφέρεται καλύτερα από τον GrPV καθώς μεταβάλλουμε το πλήθος των κανόνων που θέλουμε να κρύψουμε.



Εικόνα 15: Σύγκριση Κόστους Απώλειας GrPV – GPSh για μεταβλητού πλήθους ευαίσθητους κανόνες (τυχαίοι κανόνες)



Εικόνα 16: Σύγκριση Κόστους Απώλειας GrPV – GPSh για μεταβλητού πλήθους ευαίσθητους κανόνες (κανόνες με υψηλή υποστήριξη)

6.4. Συμπεράσματα και Συζήτηση

Έχοντας ως κύριο στόχο την αξιολόγηση των αλγορίθμων καθαρισμού, προσπαθήσαμε να εκτελέσουμε μια σειρά από εκτενή πειράματα που θα έφερναν στην επιφάνεια σημαντικά αποτελέσματα για την αποδοτικότητα και την αποτελεσματικότητα των αλγορίθμων. Τα πειράματα έγιναν πάνω σε πραγματικά δεδομένα καθώς επίσης και σε δεδομένα που παρήχθησαν από το εργαλείο της IBM [55]. Επιλέγοντας ένα αντιπροπωπευτικό υποσύνολο των αλγορίθμων καθαρισμού παραθέσαμε κάποια συγκριτικά αποτελέσματα τα οποία μας οδήγησαν στα εξής συμπεράσματα.

- Η διαδικασία καθαρισμού δεν είναι μια απλή διαδικασία και πρέπει να γίνεται με μεγάλη προσοχή και μεθοδικότητα έτσι ώστε η καθαρισμένη βάση δεδομένων να είναι χρήσιμη και μετά την διαδικασία. Γι' αυτόν τον λόγο, τα πειράματά μας έλαβαν υπ'όψιν διαφορετικά σενάρια, ώστε να προκύψουν μεγαλύτερου εύρους αποτελέσματα.

- Οι μεγάλες βάσεις δεδομένων δεν αποτελούν πρόβλημα, γιατί όπως παρατηρήσαμε υπάρχουν αλγόριθμοι (π.χ. ο GrPV) που από άποψης αποδοτικότητας και αποτελεσματικότητας επιστρέφουν πολύ ικανοποιητικά αποτελέσματα.
- Από άποψης κλιμακώσεως οι αλγόριθμοι GrPV, SrbPV, SrPV και WPVTp συμπεριφέρονται πολύ ικανοποιητικά αφού απαιτούν 2, 2, 2 και 1 σάρωση αντίστοιχα, ενώ ο RSTcTs στον αντίποδα απαιτεί τόσες σαρώσεις όσο το πλήθος των ευαίσθητων κανόνων.
- Σε γενικές γραμμές ο αλγόριθμος GrPV αποδεικνύει μέσω των πειραμάτων την πολύ καλή του απόδοση. Σε σχεδόν όλες τις περιπτώσεις επέστρεψε καλύτερα αποτελέσματα με εξαίρεση την περίπτωση που θέλουμε να κρύψουμε πολλούς κανόνες όπου ο WPVTp επωφελείται από τις τομές των αντικειμένων.
- Όσον αφορά την σύγκριση του αντιπροσώπου των αλγορίθμων διαμοιρασμού δεδομένων (GrPV) με τον αλγόριθμο διαμοιρασμού προτύπων (GPSh) τα αποτελέσματα δείχνουν πως ο δεύτερος είναι και πιο αποδοτικός και πιο αποτελεσματικός, διότι εμφανίζει μικρότερο χρόνο εκτέλεσης σε όλα τα σενάρια και μικρότερο Κόστος Απώλειας επίσης σε όλα τα σενάρια.

Σε γενικές γραμμές, θα μπορούσαμε να πούμε πως οι αλγόριθμοι που επιλέγουν αντικείμενα-θύματα για να αφαιρεθούν από τις ευαίσθητες δοσοληψίες έχουν πολύ καλή απόδοση, ενώ συγκεκριμένα οι GrPV και GPSh στο μεγαλύτερο ποσοστό των περιπτώσεων αποδίδουν τα μέγιστα. Τα αποτελέσματα εμφανίζονται ακόμα πιο ικανοποιητικά για μεγάλες βάσεις δεδομένων όπου αυξάνονται οι επικαλύψεις υποψήφιων αντικειμένων-θυμάτων.

Κεφάλαιο 7

Επίλογος

Η διατήρηση της ιδιωτικότητας κατά την Εξόρυξη Γνώσης από Δεδομένα είναι μια από τις νεώτερες τάσεις στο ερευνητικό πεδίο της ιδιωτικότητας και της ασφάλειας. Οδηγείται από ένα από τα σημαντικότερα ζητήματα της εποχής πληροφοριών - το δικαίωμα στην ιδιωτικότητα. Αν και αυτό το ερευνητικό πεδίο είναι πολύ νέο, έχει προκύψει μεγάλο ενδιαφέρον για αυτό: α) παρατηρείται μεγάλη εξέλιξη στις τεχνικές διατήρησης ιδιωτικότητας τα τελευταία χρόνια, β) το ενδιαφέρον από τον ακαδημαϊκό κόσμο και τη βιομηχανία έχει αυξηθεί γρήγορα και γ) αφιερώνονται πολλά συνέδρια πάνω σε αυτό το θέμα.

Τα ζητήματα ιδιωτικότητας έχουν θέσει νέες προκλήσεις για τις νέες χρήσεις της τεχνολογίας εξόρυξης δεδομένων. Αυτές οι τεχνικές προκλήσεις δεν μπορούν απλά να εξεταστούν με τον περιορισμό της συλλογής δεδομένων ή ακόμα και με τον περιορισμό της δευτεροβάθμιας χρήσης της τεχνολογίας πληροφοριών. Μια κατά προσέγγιση λύση θα μπορούσε να είναι ικανοποιητική, ανάλογα με την εφαρμογή, δεδομένου ότι το κατάλληλο επίπεδο ιδιωτικότητας μπορεί να ερμηνευθεί σε διαφορετικά πλαίσια. Στη συγκεκριμένη ομάδα εφαρμογών που εξετάστηκε σε αυτήν τη διπλωματική, τους κανόνες συσχέτισης, πρέπει να υπάρχει μια σωστή ισορροπία μεταξύ της ανάγκης για ιδιωτικότητα και της ανακάλυψης γνώσης.

Σε αυτήν την διπλωματική, έγινε μια αναφορά στις βασικές έννοιες που διέπουν την διατήρηση ιδιωτικότητας, έτσι ώστε να δωθεί μια εννοιολογικής φύσης προσέγγιση στο ζήτημα Επίσης, έγινε μια έρευνα και παρουσίαση των υπαρχουσών

τεχνικών στην βιβλιογραφία που εξετάζουν το πρόβλημα της διατήρησης ιδιωτικότητας στην εξόρυξη κανόνων συσχέτισης. Πιο συγκεκριμένα, οι τεχνικές που πραγματεύονται το συγκεκριμένο αντικείμενο εξετάζουν το πρόβλημα μετατροπής μια αρχικής βάσης δεδομένων σε μια νέα που κρύβει τις ευαίσθητες πληροφορίες, δαιτηρώντας παρόλα αυτά τα γενικά πρότυπα και τις τάσεις από την αρχική βάση δεδομένων. Οι ευαίσθητες πληροφορίες δεν περιορίζονται μόνο σε προσωπικά στοιχεία, αλλά μπορούν να απεικονίσουν, για παράδειγμα, τη συμπεριφορά αγορών των πελατών, οικονομικές πληροφορίες, στοιχεία ιατρικών φακέλλων ασθενών, στοιχεία ασφαλιστικής ευθύνης και ευαίσθητα πρότυπα, τα οποία θεωρούνται στρατηγικής ή ανταγωνιστικής σημασίας για τον κάτοχο των στοιχείων.

Στα πλαίσια των τεχνικών διατήρησης ιδιωτικότητας έγινε μια αναφορά στους αλγορίθμους καθαρισμού της κατηγορίας των Τεχνικών Περιορισμού Δεδομένων, όπου για τον εκάστοτε αλγόριθμο περιγράφεται ο τρόπος με τον οποίο αυτός προσπαθεί να αποκρύψει το σύνολο των ευαίσθητων κανόνων συσχέτισης.

Έγινε μια μεθοδική έρευνα και αξιολόγηση της αποδοτικότητας και της αποτελεσματικότητας ενός αντιπροσωπευτικού υποσυνόλου των αλγορίθμων καθαρισμού και έτσι παρουσιάστηκε και εμπειρικά η δυνατότητα πραγματοποίησης και επίτευξης της διατήρησης της ιδιωτικότητας.

Καταλήγοντας, είμαστε σε θέση να πούμε, πως η διατήρηση ιδιωτικότητας κατά την εξόρυξη κανόνων συσχέτισης είναι εφικτή και πως μπορεί να βρεθεί ένα ικανό σημείο ισορροπίας μεταξύ προστασίας και ανακάλυψης γνώσης.

Αναφορές

[1] M. Ackerman, L. Cranor, and J. Reagle. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In *Proc. of the ACM Conference on Electronic Commerce*, pages 1-8, Denver, Colorado, USA, November 1999.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic Databases. In *Proc. Of the 28th Conference on Very Large Data Bases*, Hong Kong, China, August 2002.

[3] M. Atallah, E. Bertino, A. Elmagarmid, M. Ibrahim, and V. Verykios. Disclosure Limitation of Sensitive Rules. In *Proc. of IEEE Knowledge and Data Engineering Workshop*, pages 45-52, Chicago, Illinois, November 1999.

[4] E. Dasseni, V. S. Verykios, A. K. Elmagarmid, and E. Bertino. Hiding Association Rules by Using Confidence and Support. In *Proc. of the 4th Information Hiding Workshop*, pages 369-383, Pittsburg, PA, April 2001.

[5] Y. Saygin, V. S. Verykios, and C. Clifton. Using Unknowns to Prevent Discovery of Association Rules. *SIGMOD Record*, 30(4):45-54, December 2001.

[6] Y. Saygin, V. S. Verykios, and A. K. Elmagarmid. Privacy Preserving Association Rule Mining. In *Proc. of the 12th International Workshop on Research Issues in Data Engineering: Engineering E-Commerce/E-Business Systems (RIDE'02)*, pages 151-158, San Jose, CA, USA, February 2002.

[7] L. Brankovic and V. Estivill-Castro. Privacy Issues in Knowledge Discovery and Data Mining. In *Proc. of Australian Institute of Computer Ethics Conference (AICEC99)*, Melbourne, Victoria, Australia, July 1999.

[8] S. Castano, M. Fugini, G. Martella, and P. Samarati. *Database Security*. Addison-Wesley Longman Limited, England, 1995.

[9] M.-S. Chen, J. Han, and P. S. Yu. Data Mining: An Overview from a Database Perspective. *IEEE Transactions on Knowledge and Data Engineering*, 8(6):866-883, 1996.

[10] Z. Chen. *Data Mining and Uncertain Reasoning*. John Wiley and Sons, Inc. New York, NY, 2001.

[11] C. Clifton. Using Sample Size to Limit Exposure to Data Mining. *Journal of ComputerSecurity*, 8(4):281-307, November 2000.

[12] C. Clifton, W. Du, M. Atallah, M. Kantarcio_glu, X. Lin, and J. Vaidya. Distributed Data Mining to Protect Information Privacy. Proposal to the National Science Foundation, December 2001.

[13] C. Clifton, M. Kantarcioglu, and J. Vaidya. Defining Privacy For Data Mining. In *Proc. of the National Science Foundation Workshop on Next Generation Data Mining*, pages 126-133, Baltimore, MD, USA, November 2002.

[14] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu. Tools For Privacy Preserving Distributed Data Mining. *SIGKDD Explorations*, 4(2):28-34, December 2002.

[15] S. Cockcroft and P. Clutterbuck. Attitudes Towards Information Privacy. In *Proc.of the 12th Australasian Conference on Information Systems*, Coffs Harbour, NSW, Australia, December 2001.

[16] M. J. Culnan. How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information. *MIS Quartely*, 17(3):341-363, September 1993.

[17] W. Du and M. J. Atallah. Secure Multi-Party Computation Problems and their Applications: A Review and Open Problems. In *Proc.of 10th ACM/SIGSAC 2001 New Security Paradigms Workshop*, pages 13-22, Cloudcroft, New Mexico, September 2001.

[18] S. Dzeroski. Data Mining in a Nutshell, Chapter 1 of Relational Data Mining", S. Dzeroski and N. Lavrac (eds.), Springer-Verlag, Germany, 2001, pages 3-27.

[19] V. Estivill-Castro and L. Brankovic. Data Swapping: Balancing Privacy Against Precision in Mining for Logic Rules. In *Proc. of Data Warehousing and Knowledge Discovery DaWaK-99*, pages 389-398, Florence, Italy, August 1999.

[20] V. Estivill-Castro, L. Brankovic, and D. L. Dowe. Privacy in Data Mining. *Privacy Law and Policy Reporter*, 6(3):33-35, September 1999.

[21] U. Fayyad. Knowledge Discovery in Databases: An Overview, Chapter 2 of "Relational Data Mining", S. Dzeroski and N. Lavrac (eds.), Springer-Verlag, Germany, 2001, pages 28-47.

[22] U. M. Fayyad, G. Piatetsky-Shapiro, and P. Smyth. From Data Mining to Knowledge Discovery: An Overview. In *Advances in Knowledge Discovery and Data Mining. U. M. Fayyad, G. Piatetsky-Shapiro, P. Smith, and R. Uthurusamy (eds.)*, pages 1-34, MIT Press, Cambridge, MA, 1996.

[23] A. P. Felty and S. Matwin. Privacy-Oriented Data Mining by Proof Checking. In *Proc. of the 6th European Conference on Principles of Data Mining and Knowledge Discovery (PKDD)*, pages 138-149, Helsinki, Finland, August 2002.

[24] D. F. Ferraiolo and R. Kuhn. Role-Based Access Control: Features and Motivations. In *Proc. of the 11th Annual Computer Security Applications Conference*, pages 241-248, New Orleans, LA, USA, Dec. 1995.

[25] O. Goldreich, S. Micali, and A. Wigderson. How to Play Any Mental Game – A Completeness Theorem for Protocols with Honest Majority. In *Proc. of the 19th Annual ACM Symposium on Theory of Computing*, pages 218-229, New York City, USA, May 1987.

[26] S. Goldwasser. Multi-party Computations: Past and Present. In *Proc. of the 16th Annual ACM Symposium on Principles of Distributed Computing*, pages 1-6, Santa Barbara, CA, August 1997.

[27] J. Han and M. Kamber. *Data Mining: Concepts and Techniques*. Morgan Kaufmann Publishers, San Francisco, CA, 2001.

[28] P. Jefferies. Multimedia, Cyberspace & Ethics. In *Proc. of International Conference on Information Visualisation (IV2000)*, pages 99-104, London, England, July 2000.

[29] G. H. John. Behind-the-Scenes Data Mining. *Newletter of ACM.SIG on KDDM*, 1(1):9-11, June 1999.

[30] M. Kantarcioglu and C. Clifton. Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data. In *Proc. of The ACM.SIGMOD Workshop on 'Research Issues on Data 'Mining and Knowledge Discovery*, Madison, Wisconsin, June 2002.

[31] M. Kantarcioglu, J. Jin, and C. Clifton. When Do Data Mining Results Violate Privacy? In *Proc. of the 10th ACM.SIGKDD International Conference on Knowledge Discovery and Data 'Mining*, pages 599{604, Seattle, WA, USA, August 2004.

[32] W. Klosgen. Anonymization Techniques for Knowledge Discovery in Databases. In *Proc. of the First International Conference on Knowledge Discovery and Data Mining (KDD-95)*, pages 186{191, Montreal, Canada, August 1995.

[33] W. Klosgen. KDD: Public and Private Concerns. *IEEE 'EXPERT*, 10(2):55-57, April 1995.

[34] K. C. Laudon. Markets and Privacy. *Communication of the ACM*, 39(9):92-104, September 1996.

[35] Y. Lindell and B. Pinkas. Privacy Preserving Data Mining. In *Crypto 2000, Springer-Verlag (LNCS 1880)*, pages 36-54, Santa Barbara, CA, August 2000.

[36] A. Mucsi-Nagy and S. Matwin. Digital Fingerprinting for Sharing of Confidential Data. In *Proc. of the Workshop on Privacy and Security Issues in Data Mining*, pages 11-26, Pisa, Italy, September 2004.

[37] Office of the Information and Privacy Commissioner. Data Mining: Staking a Claim on Your Privacy, Toronto, Ontario, January 1998.

[38] D. E. O'Leary. Some Privacy Issues in Knowledge Discovery: The OECD Personal Privacy Guidelines. *IEEE EXPERT*, 10(2):48-52, April 1995.

[39] S. R. M. Oliveira and O. R. Zaïane. Foundations for an Access Control Model for Privacy Preservation in Multi-Relational Association Rule Mining. In *Proc. of the*

IEEE ICDM Workshop on Privacy, Security, and Data Mining, pages 19-26, Maebashi City, Japan, December 2002.

[40] S. R. M. Oliveira and O. R. Zaïane. Privacy Preserving Frequent Itemset Mining. In *Proc. of the IEEE ICDM Workshop on Privacy, Security, and Data Mining*, pages 43-54, Maebashi City, Japan, December 2002.

[41] S. R. M. Oliveira and O. R. Zaïane. Algorithms for Balancing Privacy and Knowledge Discovery in Association Rule Mining. In *Proc. of the 7th International Database Engineering and Applications Symposium (IDEAS'03)*, pages 54-63, Hong Kong, China, July 2003.

[42] S. R. M. Oliveira and O. R. Zaïane. Protecting Sensitive Knowledge By Data Sanitization. In *Proc. of the 3rd IEEE International Conference on Data Mining (ICDM'03)*, pages 613-616, Melbourne, Florida, USA, November 2003.

[43] S. R. M. Oliveira, O. R. Zaïane, and Y. Saygin. Secure Association Rule Sharing. In *Proc. of the 8th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD'04)*, pages 74-85, Sydney, Australia, May 2004.

[44] B. Pinkas. Cryptographic Techniques For Privacy-Preserving Data Mining. *SIGKDD Explorations*, 4(2):12-19, December 2002.

[45] A. Rezgui, A. Bouguettaya, and M. Y. Eltoweissy. Privacy on the Web: Facts, Challenges, and Solutions. *IEEE Security & Privacy*, 1(6):40-49, Nov-Dec 2003.

[46] P. Samarati. Protecting Respondents' Identities in Microdata Release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6):1010-1027, 2001.

[47] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-Based Access Control Models. *IEEE Computer*, 20(2):38-47, 1996.

[48] F. D. Schoeman. Philosophical Dimensions of Privacy, Cambridge Univ. Press, 1984.

[49] J. Vaidya and C. Clifton. Privacy Preserving Association Rule Mining in Vertically Partitioned Data. In *Proc. of the 8th ACM SIGKDD Intl. Conf. on*

Knowledge Discovery and Data Mining, pages 639-644, Edmonton, AB, Canada, July 2002.

[50] J. Vaidya and C. Clifton. Privacy-Preserving K-Means Clustering Over Vertically Partitioned Data. In *Proc. of the 9th ACM SIGKDD Intl. Conf. on Knowledge Discovery and Data Mining*, pages 206-215, Washington, DC, USA, August 2003.

[51] A. A. Veloso, W. Meira Jr., S. Parthasarathy, and M. B. Carvalho. Efficient, Accurate and Privacy-Preserving Data Mining for Frequent Itemsets in Distributed Databases. In *Proc. of the 18th Brazilian Symposium on Databases*, pages 281-292, Manaus, Brazil, October 2003.

[52] E. D. Pontikakis, A.A. Tsitsonis, V. S. Verykios, Y. Theodoridis and L. Chang. A Qualitative and Quantitative Analysis of Blocking in Association Rule Mining.

[53] The UCI Repository of Machine Learning site. http://www.ics.uci.edu/~mlearn/MLRepository.html

[54] The Frequent Itemset Mining Dataset Repository. http://fimi.cs.helsinki.fi/data/ .

[55] The IBM Quest Market-Basket Synthetic DataGenerator. http://www.almaden.ibm.com/software/quest/Resources/index.shtml .

[56] Apriori Implementation of Ferenc Bodon. http://www.cs.bme.hu/~bodon/en/apriori/ .

Παράρτημα

Στο συνοδευτικό DVD της εργασίας περιέχεται όλος ο πηγαίος κώδικας των αλγορίθμων καθώς και τα αποτελέσματα της εκτέλεσής τους. Πιο συγκεκριμένα, υπάρχει ένα αρχείο sanitization.zip το οποίο περιέχει τον κώδικα για όλους τους αλγορίθμους*. Κάνοντας extract αυτό το αρχείο, παίρνουμε τους κώδικες καθώς και ένα αρχείο README που περιέχει πληροφορίες για το complilation και το execution των αλγορίθμων. Σημειώνεται πως το complilation πρέπει να γίνει σε λειτουργικό σύστημα Linux Red Hat 8.0 ή ανώτερο. Τα εκτελέσιμα αρχεία στην συνέχεια χρησιμοποιούνται σε κάθε φάκελλο

Όλες οι βάσεις που χρησιμοποιήθηκαν για τα πειράματα βρίσκονται στον φάκελλο /Datasets.

Ο φάκελλος /Apriori περιέχει υλοποιήσεις του ομόνυμου αλγορίθμου ο οποίος χρησιμοποιήθηκε για την εξόρυξη των κανόνων συσχέτισης από τις αρχικές βάσεις δεδομένων και από τις καθαρισμένες βάσεις δεδομένων για να βγουν τα συμπεράσματα για την αποδοτικότητα και την αποτελεσματικότητα των αλγορίθμων με βάση τις μετρικές. Καλό είναι να χρησιμοποιηθεί η ίδια υλοποίηση για όλες τις βάσεις δεδομένων.

Ο φάκελλος /Dasseni περιέχει όλα τα σχετικά με τα αποτελέσματα εκτέλεσης του αλγορίθμου Dasseni (RSTcTs). Ομοίως οι φάκελλοι /SWA (WPVTp) και /DSA (GPSh). Όσον αφορά τον φάκελλο /Sanitizing, αυτός περιέχει όλα τα αποτελέσματα σχετικά με την εκτέλεση των αλγορίθμων:

- AllPV
- MinFPV
- GrPV
- SrbPV
- SrPV

Ο φάκελλος /Metrics περιέχει τον κώδικα και το εκτελέσιμο αρχείο για τις μετρικές που αναφέρθηκαν στην παράγραφο 6.1.

---

* Τον πηγαίο κώδικα των αλγορίθμων μας τον έδωσε ο Stanley R. Oliveira, τον οποίο και ευχαριστούμε πολύ για την βοήθειά του.

Στους φακέλλους που έχουν τα ονόματα των datasets που χρησιμοποιήθηκαν, υπάρχουν όλα τα αποτελέσματα των πειραμάτων. Πιο συγκεκριμένα, τα αρχεία της μορφής:

- <filename>_exec.dat περιέχουν τους χρόνους εκτέλεσης
- <filename>_rules.dat περιέχουν τους κανόνες συσχέτισης
- <filename>_srules.dat περιέχουν τους ευαίσθητους κανόνες συσχέτισης
- <filename>_san_sdb.dat περιέχουν τις καθαρισμένες βάσεις δεδομένων
- <filename>_san_rules.dat περιέχουν τους ευαίσθητους κανόνες συσχέτισης των καθαρισμένων βάσεων δεδομένων
- <filename>_metrics.dat περιέχουν τα αποτελέσματα των μετρικών

Επίσης, σημειώνεται πως όλοι οι ευαίσθητοι κανόνες των βάσεων μπορούν να βρεθούν στον φάκελλο /Apriori/apriori_linux/Srules. Οι διαφορετικού πλήθους ευαίσθητοι κανόνες για την βάση Connect μπορούν να βρεθούν στον φάκελλο /Apriori/apriori_linux/conn_srules.

Ο φάκελλος /Codmine Executables περιέχει τα εκτελέσιμα αρχεία της εφαρμογής CODMINE η οποία τρέχει σε περιβάλλον Windows με εγκατεστημένο το .NET Framework. Η εφαρμογή αυτή, όπως και η ARMiner, παρατίθενται για τη βοήθεια του αναγνώστη που θέλει να εκτελέσει παραδείγματα διατήρησης ιδιωτικότητας σε διαφορετικό περιβάλλον.

Ο φάκελλος /IBM_VC++ περιέχει τον IBM Quest Market-Basket Synthetic DataGenerator, για περιβάλλον Windows. Πιο συγκεκριμένα ο φάκελλος /IBM_VC++/Debug περιέχει και τα εκτελέσιμα (συγκεκριμένα το αρχείο main.exe εκτελεί την εφαρμογή).