ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"ΕΦΑΡΜΟΓΗ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΟΥ ΓΙΑ ΤΗΝ ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ"

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΜΠΑΚΟΜΙΧΑΛΗΣ ΙΩΑΝΝΗΣ

Α.Μ.: 236326

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΣΙΟΥΤΑΣ ΣΠΥΡΟΣ

ΣΥΝΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΣΤΑΜΑΤΙΟΥ ΙΩΑΝΝΗΣ

ΠΑΤΡΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2020

ΠΕΡΙΛΗΨΗ

Στην σημερινή εποχή όλες οι καθημερινές μας δραστηριότητες έχουν μετατραπεί σε ψηφιακές με την χρήση του παγκόσμιου ιστού. Η αλλαγή αυτή έχει επιφέρει τόσο αμέτρητα θετικά αποτελέσματα στον τρόπο διαβίωσης του ανθρώπου όσο και τις αντίστοιχες συνέπειες. Μία από αυτές είναι η παραβίασης της ιδιωτικότητας και των προσωπικών δεδομένων. Συνεπώς, η προστασία των προσωπικών δεδομένων καθώς και η ορθή χρήση τους αποτελούν επιτακτική ανάγκη για τον άνθρωπο στην σημερινή εποχή. Στην παρούσα διπλωματική εργασία υλοποιείται μία εφαρμογή αποτίμησης κινδύνου επικεντρωμένη στον χρήστη για την παραβίαση της ιδιωτικότητας στο διαδίκτυο με στατιστική ανάλυση και παρουσίαση αποτελεσμάτων. Αρχικά, περιγράφονται έννοιες όπως των προσωπικών δεδομένων, της ιδιωτικότητας και των ανώνυμων δεδομένων, έπειτα παρουσιάζεται η εφαρμογή *IB Privacy Advisor*. Στην συνέχεια παρουσιάζεται ο τρόπος με τον οποίο αναπτύχθηκε η εφαρμογή τόσο σε επίπεδο αρχιτεκτονικής όσο και σε λογισμικού, καθώς και ο τρόπος λειτουργίας της. Τέλος, παρουσιάζονται τα συμπεράσματα που προέκυψαν καθώς και οι μελλοντικές επεκτάσεις που μπορούν να υλοποιηθούν στην εφαρμογή.

ΕΥΧΑΡΙΣΤΗΡΙΟ

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Σπύρο Σιούτα και τον συνεπιβλέποντα καθηγητή μου κ. Ιωάννη Σταματίου, για την ευκαιρία που μου έδωσαν να ασχοληθώ με αυτό το ενδιαφέρον θέμα, για την πολύτιμη βοήθεια τους και τις χρήσιμες συμβουλές τους.

Τέλος, ευχαριστώ πολύ την οικογένεια μου και τους φίλους μου που με υποστήριξαν σε όλη την διάρκεια των σπουδών μου.

Περιεχόμενα

Κεφάλαιο 1: Εισαγωγή

Στο Κεφάλαιο αυτό παρουσιάζεται το μείζων πρόβλημα της παραβίασης της ιδιωτικότητας και της υποκλοπής των προσωπικών δεδομένων. Στην συνέχεια παρουσιάζεται ο στόχος της διπλωματικής εργασίας καθώς και η δομή των κεφαλαίων της.

1.1 Περιγραφή Προβλήματος

Η ταχεία ψηφιοποίηση των δραστηριοτήτων της κοινωνίας τα τελευταία χρόνια έχει συμβάλει στην τεράστια αύξηση της ανταλλαγής ψηφιακών πληροφοριών [1]. Συγκεκριμένα, η άνοδος του Web 2.0 μαζί με την χρήση του ίντερνετ από έξυπνες συσκευές (smartphones), προώθησαν τη διαθεσιμότητα τεράστιων ποσοτήτων πληροφορίας που είναι χρήσιμες για την καλύτερη κατανόηση και αντιμετώπιση κρίσιμων κοινωνικών προκλήσεων (π.χ. μεταφορά ή υγεία). Παρά τα οφέλη του, η συλλογή μεγάλων ποσοτήτων δεδομένων παρουσιάζει μεγάλες απειλές στο απόρρητο των ατόμων, όπως, κλοπή ταυτότητας ή φθορά που προκαλείται από διαρροές προσωπικών δεδομένων. Πρόσφατες έρευνες δείχνουν ότι ανησυχίες για το απόρρητο των χρηστών και το αίτημα για να έχουν ρητό έλεγχο των προσωπικών τους δεδομένων έχουν αυξηθεί. Για παράδειγμα, το 81% των Ευρωπαίων πιστεύουν ότι δεν έχουν πλήρη έλεγχο των προσωπικών τους δεδομένων στο Διαδίκτυο ενώ το 69% θα ήθελε να δώσει τη ρητή έγκρισή τους πριν από τη συλλογή και επεξεργασία των προσωπικών δεδομένων τους. Έτσι, με τα διάφορα περιστατικά παραβίασης απορρήτου και τις επαναλαμβανόμενες διαρροές, η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων έχει γίνει ένα επείγον και φλέγων θέμα όχι μόνο για τους χρήστες, αλλά και για τους επαγγελματίες προστασίας προσωπικών δεδομένων .

Η προστασία των ιδιωτικών πληροφοριών είναι μια πολυδιάστατη εργασία που περιλαμβάνει τον σχεδιασμό εργαλείων για την προστασίας της ιδιωτικότητας, την ευαισθητοποίηση του χρήστη και την εφαρμογή υποστηρικτικού νομικού πλαισίου [2].

1.2 Στόχος Διπλωματικής

Με βάση τα παραπάνω στοιχεία, στην παρούσα διπλωματική θα αναπτυχθεί μία εφαρμογή (Application) επικεντρωμένη στον χρήστη (User-centered) για την ανάλυση της παραβίασης της ιδιωτικότητας (Privacy Risk Analysis) και των προσωπικών δεδομένων στο διαδίκτυο, με την χρήση βάσης δεδομένων (Database) και των κατάλληλων μεταβλητών (Attributes) ώστε να υπολογίζεται η πιθανότητα επίθεσης στην συγκεκριμένη μεταβλητή και με αμφότερο σκοπό την δημιουργία αναφοράς (Report), η οποία θα δίνει άμεσα στοιχεία για την πιθανότητα επίθεσης με σκοπό την υποκλοπή προσωπικών δεδομένων.

Πιο συγκεκριμένα στα πλαίσια της διπλωματικής εργασίας ζητήθηκε η υλοποίηση των παρακάτω απαιτήσεων :

- Η ανάπτυξη εφαρμογής (GUI) επικεντρωμένη στον χρήστη (User-centered) για υπολογισμό πιθανότητας επίθεσης για παραβίαση και υποκλοπή προσωπικών δεδομένων με χρήση πιθανότητας Bayes (Rule of Bayes) και μεταβλητών (Attributes).

- Η ανάπτυξη κώδικα για δημιουργία μίας επαρκούς βάσης δεδομένων με τα πεδία όνομα, επίθετο, username, password, διεύθυνση, ταχυδρομικό κώδικα, πόλη διαμονής και χώρα για τους χρήστες.

- Η ανάπτυξη κώδικα για την δημιουργία αυτοματοποιημένης αναφοράς (Report) για τα αντίστοιχα αποτελέσματα της κάθε μεταβλητής σε σχέση με την πιθανότητα επίθεσης για υποκλοπή προσωπικών δεδομένων.

- Η δημιουργία τεκμηρίωσης (documentation), στην οποία φαίνονται όλες οι απαιτήσεις για την εγκατάσταση της εφαρμογής , τα βήματα εγκατάστασης και εκτέλεσης της εφαρμογής και τέλος η λειτουργία της εφαρμογής μέσα από εικόνες (screenshots).

1.3 Δομή Διπλωματικής

Η δομή της διπλωματικής εργασίας, όπως αυτή αποτυπώνεται παρακάτω, χωρίζεται σε πέντε (5) κεφάλαια. Αρχικά, αναλύεται εκτενέστερα το τεχνολογικό υπόβαθρο, περιγράφονται βασικοί όροι, όπως της ιδιωτικότητας και των προσωπικών δεδομένων, και η νομοθεσία ως προς την προστασία των προσωπικών δεδομένων. Επίσης, αναφέρονται οι τεχνολογίες υλοποίησης και γλώσσες προγραμματισμού που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής. Στο τρίτο κεφάλαιο, αναλύεται η εφαρμογή σε επίπεδο αρχιτεκτονικής, οι απαιτήσεις για την εγκατάστασης της, ο τρόπος εγκατάστασης και τα εργαλεία τα οποία παρέχει. Στο τέταρτο κεφάλαιο, παρουσιάζεται η εφαρμογή που αναπτύχθηκε, αναλύοντας τις απαιτήσεις, τον τρόπο λειτουργίας, την χρήση βάσης δεδομένων και την δημιουργία test cases για την ορθή χρήση της εφαρμογής με σκοπό τον ορθό υπολογισμό της πιθανότητας επίθεσης για παραβίαση της ιδιωτικότητας. Στο πέμπτο κεφάλαιο, παρουσιάζεται η λειτουργία της εφαρμογής μέσα από εικόνες (screenshots). Τέλος, στο έκτο κεφάλαιο παρουσιάζονται τα συμπεράσματα ύστερα από την μελέτη της παραβίασης της ιδιωτικότητας και της υποκλοπής προσωπικών δεδομένων και αναφέρονται μελλοντικές επεκτάσεις που μπορούν να γίνουν στην εφαρμογή που αναπτύχθηκε.

Κεφάλαιο 2: Τεχνολογικό Υπόβαθρο

Στο κεφάλαιο αυτό παρουσιάζονται βασικοί όροι όπως της ιδιωτικότητας, των προσωπικών δεδομένων και των ανώνυμων δεδομένων, τα συνήθη προβλήματα που οδηγούν στην παραβίαση της ιδιωτικότητας, οι μέθοδοι προστασίας των προσωπικών δεδομένων, η υπάρχουσα νομοθεσία για την προστασία των προσωπικών δεδομένων (GDPR) καθώς και οι τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίηση της εφαρμογής.

2.1 Ιδιωτικότητα και Προσωπικά Δεδομένα

Με την εξέλιξη της τεχνολογίας και της κοινωνίας, η ιδιωτικότητα ως όρος και αξία εξελίσσεται και μεταλλάσσεται λαμβάνοντας τη μορφή πλέον του σεβασμού των δεδομένων προσωπικού χαρακτήρα. Η σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών, η αποκέντρωση της επεξεργασίας, η διείσδυση της επεξεργασίας και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας αλλάζουν ριζικά το περιβάλλον χρήσης της προσωπικής πληροφορίας, αλλά και τα ζητήματα που εγείρονται σε σχέση με την προστασία της.

2.1.1 Η έννοια της ιδιωτικότητας

Η ιδιωτικότητα ως έννοια από μόνη της είναι ιδιαίτερα ενδιαφέρουσα και μυστηριώδης, ίσως επειδή σχεδόν κανένας δεν συμφωνεί στο τι πραγματικά είναι. Ωστόσο, το δικαίωμα στην ιδιωτικότητα είναι εκείνο που ενέπνευσε πλήθος συζητήσεων και αντιπαραθέσεων σε πολλά επιστημονικά πεδία όπως νομικό, φιλοσοφικό, κοινωνικό, πολιτικό και πιο πρόσφατα τεχνολογικό πεδίο.

Οι ορισμοί ποικίλλουν ανάλογα με το περιεχόμενο, την κουλτούρα και το περιβάλλον. Σε άρθρο του 1890, οι Samuel Warren και Louis Brandeis [3] ορίζουν την ιδιωτικότητα ως «το δικαίωμα του να είσαι μόνος» (the right to be let alone) και τονίζεται η αναγκαιότητα να κατοχυρωθεί συνταγματικά η έννοια της ιδιωτικότητας. Επίσης στο ίδιο άρθρο αναφέρεται πως η σημασία του θέματος της ιδιωτικότητας συνεχώς θα μεγαλώνει καθώς η αξία της είναι πολύ μεγαλύτερη από ότι στο παρελθόν. Μετά από μακροχρόνιες κοινωνικές συζητήσεις το 1965, για πρώτη φορά θεσπίζεται το συνταγματικό δικαίωμα στην ιδιωτικότητα από το ανώτατο δικαστήριο των Η.Π.Α. και έτσι κατοχυρώνεται και συνταγματικά. Χαρακτηριστικά αναφέρουμε τη δήλωση το Lyndon B. Johnson, προέδρου των Η.Π.Α. (1963-1969), πως «κάθε άνθρωπος θα πρέπει να γνωρίζει ότι οι συνομιλίες του, οι συναναστροφές του και η προσωπική του ζωή είναι ιδιωτικά».

Το 1967 ο Alan Westlin ορίζει την ιδιωτικότητα ως το «δικαίωμα των ανθρώπων να επιλέγουν ελεύθερα και χωρίς περιορισμούς το βαθμό έκθεσης του εαυτού τους, τη στάση και τη συμπεριφορά τους απέναντι σε άλλους» [4].

Μια από τις πιο πρόσφατες αναφορές στην ιδιωτικότητα είναι της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα (1948), όπου στο άρθρο 17 αναφέρει πως «κανείς δεν πρέπει να υποβάλλεται σε περιορισμό ή παράνομη επέμβαση στην ιδιωτική του ζωή, την οικογένεια, το σπίτι ή την αλληλογραφία του, ούτε να υπόκειται σε παράνομες προσβολές της τιμής και της υπόληψής του. Επίσης, καθένας έχει το δικαίωμα της έννομης προστασίας από τέτοιου είδους παρεμβάσεις και επιθέσεις».

Ο Rachels το 1975 κάνει λόγο για «την ικανότητα να ελέγχουμε ποιος έχει πρόσβαση σε εμάς» και ο Benn το 1988 θέτει το σεβασμό στην προσωπική ζωή ως συνώνυμο του σεβασμού στην αυτονομία και την αξιοπρέπεια του ατόμου.

Οι κοινωνιολόγοι ορίζουν την έννοια της ιδιωτικότητας ως το δικαίωμα κάποιου να ελέγχει τη συλλογή και τη χρήση των πληροφοριών σχετικά με τον εαυτό του [5].

Εκατό και πλέον χρόνια μετά από το δικαίωμα του ατόμου σε μια ανενόχλητη ιδιωτική ζωή των Αμερικανών δικαστών Warren και Brandeis, και υπό τη καταλυτική επίδραση της τεχνολογικής επανάστασης, ήδη η κλασσική αντίληψη της ιδιωτικότητας έχει σημαντικά εμπλουτιστεί με επιμέρους δικαιώματα, όπως το δικαίωμα στην ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο, η ελαχιστοποίηση των παρεμβάσεων, η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς, της –υπό στενή εννοία- ιδιωτικότητας, της ανωνυμίας και της απόσυρσης.

Γενικά, η ατομική ιδιωτικότητα αποτελεί ένα κοινωνικό και πολιτισμικό ζήτημα. Ωστόσο , με την πανταχού παρουσία των υπολογιστών και την εμφάνιση του διαδικτύου, η ιδιωτικότητα εξελίχθηκε σε ψηφιακό πρόβλημα. Πιο συγκεκριμένα, η επανάσταση του διαδικτύου άλλαξε άρδην τον τρόπο που αντιλαμβανόμαστε την ιδιωτικότητα οδηγώντας στον όρο internet privacy ήτοι ασφάλεια του διαδικτύου.

Ο συγκεκριμένος όρος αναφέρεται στο δικαίωμα των χρηστών του διαδικτύου να αποκρύπτουν προσωπικές πληροφορίες και να απολαμβάνουν ένα βαθμό ελέγχου στα δεδομένα που μοιράζονται με άλλους χρήστες του διαδικτύου.

2.1.2 Η έννοια των προσωπικών δεδομένων

Τα προσωπικά δεδομένα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα [6].

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του Προστασίας Προσωπικών Δεδομένων.

Η Νομοθεσία για την Προστασία των Προσωπικών Δεδομένων (GDPR) προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά).

Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει η Νομοθεσία για την Προστασία των Προσωπικών Δεδομένων (GDPR) .

Παραδείγματα δεδομένων προσωπικού χαρακτήρα:

- Όνομα και επώνυμο
- Διεύθυνση κατοικίας
- Ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com
- Αναγνωριστικός αριθμός πιστωτικής κάρτας
- Δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- Διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
- Αναγνωριστικό cookie.
- Δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

Παραδείγματα δεδομένων που δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα:

- Αριθμός μητρώου εταιρίας
- Ηλεκτρονική διεύθυνση του τύπου πληροφορίες@εταιρεία.com
- Ανώνυμα δεδομένα

2.2 Παραβίαση Ιδιωτικότητας και Υποκλοπή Προσωπικών Δεδομένων

Γενικά, με τον όρο παραβίαση ιδιωτικότητας εννοείται η απουσία ασφάλειας σε σχέση με τα προσωπικά δεδομένα ενός ατόμου και έχει ως αποτέλεσμα την παραβίαση του απορρήτου, της διαθεσιμότητας ή της ακεραιότητας του.

2.2.1 Λόγοι Παραβίασης Ιδιωτικότητας

Η ραγδαία αύξηση των χρηστών του διαδικτύου, είχε ως αποτέλεσμα να αποδειχθεί πηγή πολύτιμων πληροφοριών για τους κυβερνοεγκληματίες.

Οι επιθέσεις απέναντι στους χρήστες του διαδικτύου εκμεταλλεύονται τις αδυναμίες του συστήματος του χρήστη, οι οποίες μπορεί να είναι σχεδιαστικές, λειτουργικές αλλά και ανθρώπινες προκειμένου να αντλήσουν τις προσδοκώμενες πληροφορίες. Τα αποτελέσματα των ενεργειών αυτών έχουν αναδείξει την ασφάλεια των πληροφοριών και την προστασία της ιδιωτικότητας στο διαδίκτυο σε θέματα εξαιρετικής σημασίας καθώς αφορούν τομείς όπως η παραδοσιακή πληροφοριακή ασφάλεια, η αρχιτεκτονική των υπολογιστών, ο σχεδιασμός των συστημάτων, η μηχανική λογισμικού, η τεχνολογία διαδικτύου, τα μαθηματικά, οι νόμοι.

Οι λόγοι των επιθέσεων αυτών ποικίλλουν. Πιο συγκεκριμένα η παραβίαση της ιδιωτικότητας και του απορρήτου της επικοινωνίας των χρηστών οφείλεται στους παρακάτω λόγους.

1) Αλλοίωση δεδομένων (Data Distortion)

Σύμφωνα με τις Ευρωπαϊκές Οδηγίες, τα δεδομένα ενός ατόμου πρέπει να είναι ακριβή και ενημερωμένα, όσο αυτό είναι εφικτό, ενώ παράλληλα πρέπει να παρέχεται στα άτομα το δικαίωμα να επεμβαίνουν στα στοιχεία αυτά και να τα διορθώνουν ή ακόμα και να τα μπλοκάρουν σε περίπτωση που αυτά δεν ανταποκρίνονται στην πραγματικότητα. Και αυτό διότι, η αλλοίωση δεδομένων μπορεί να οδηγήσει σε στιγματισμό και να επιφέρει σημαντικό πλήγμα στη φήμη ενός ανθρώπου και η φήμη είναι το μέσο με το οποίο αλληλοεπιδρούμε με τους άλλους σε μια κοινωνία [7].

2) Συλλογή Δεδομένων (Data Aggregation)

Η συλλογή του όγκου των πληροφοριών από διαφορετικές πηγές και η εξαγωγή συμπερασμάτων για ένα πρόσωπο, αποτελεί μια από τις μεγαλύτερες προκλήσεις για την ιδιωτικότητα. Η ομαδοποίηση δεδομένων αναφέρεται στην τάση για συσσώρευση, διατήρηση και χρήση πληροφοριών και για διάφορους λόγους, όπως η αρχειοθέτηση και η ανάλυση. Ωστόσο, από τη συσχέτιση αυτή των δεδομένων ενδέχεται να προκύψουν στοιχεία για τα άτομα που δεν ήταν γνωστά. Οι χρήστες δίνουν σε διάφορους ιστότοπους μερικά από τα στοιχεία τους και πιστεύουν πως έτσι προστατεύονται. Όταν όμως τα στοιχεία αυτά συγχωνευτούν από κοινού, τότε προκύπτουν πολύ περισσότερες πληροφορίες για τη ζωή τους χωρίς να το γνωρίζουν.

3) Αποκλεισμός των χρηστών από τη δυνατότητα πρόσβασης στα προσωπικά τους δεδομένα (Exclusion)

Το πρόβλημα του αποκλεισμού δημιουργείται όταν στους χρήστες δεν παρέχεται η δυνατότητα πρόσβασης, διόρθωσης και ελέγχου των προσωπικών τους δεδομένων, με αποτέλεσμα οι χρήστες να αισθάνονται ανασφαλείς και ανενημέρωτοι αναφορικά με τη χρήση των δεδομένων τους.

4) Χρήση των προσωπικών δεδομένων των χρηστών για σκοπούς άλλους για τους οποίους συλλέχθηκαν (Secondary Use)

Η δευτερογενής χρήση είναι μια μορφή όπου στοιχεία που έχουν συλλεχθεί για ένα σκοπό, τελικά χρησιμοποιούνται για κάποιο άλλο χωρίς τη συγκατάθεση του εμπλεκόμενου ατόμου. Ήδη από το 1980, χρονιά που ο ΟΟΣΑ εξέδωσε τις κατευθυντήριες αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές των προσωπικών δεδομένων, γίνεται αναφορά στη αρχή του προσδιορισμένου σκοπού (Purpose specification principle), σύμφωνα με την οποία θα πρέπει να προσδιορίζονται επακριβώς οι σκοποί για τους οποίους συλλέγονται τα προσωπικά δεδομένα και η χρήση τους να συνάδει με τους σκοπούς αυτούς, ενώ κάθε αλλαγή στους σκοπούς θα πρέπει να αναφέρεται. Ο λόγος για τον οποίο υπάρχει τόσο μεγάλο ενδιαφέρον για τη μη εξουσιοδοτημένη χρήση των δεδομένων από τρίτους, είναι γιατί δημιουργεί αισθήματα φόβου στο χρήστη για τη μελλοντική τους χρήση καθώς δεν μπορεί να γνωρίζει τις επιπτώσεις που θα έχει στη ζωή του.

5) Παραβίαση Απορρήτου (Breach of confidentiality)

Η παραβίαση απορρήτου παραβιάζει την εμπιστοσύνη σε μια συγκεκριμένη σχέση. Είναι η αναίρεση μιας υπόσχεσης που έχει δοθεί για τη διατήρηση των προσωπικών πληροφοριών ενός ατόμου εμπιστευτικά. Η βασική διαφορά μεταξύ της αποκάλυψης πληροφοριών και της παραβίασης του απορρήτου έγκειται στο γεγονός πως η πιο σημαντική πτυχή της δεύτερης είναι η διατάραξη της σχέσης εμπιστοσύνης που έχει αναπτυχθεί και το αίσθημα προδοσίας που αισθάνεται το άτομο.

6) Αποκάλυψη κοινωνικών συνδέσεων

Η αποκάλυψη κοινωνικών συνδέσεων συμβαίνει όταν ένας αντίπαλος είναι σε θέση να μάθει την ύπαρξη μιας ευαίσθητης συσχέτισης μεταξύ δύο χρηστών, μια σχέση που οι χρήστες θα ήθελαν να παραμείνει κρυφή από το κοινό.
Παραδείγματα ευαίσθητων σχέσεων μπορούν να βρεθούν σε κοινωνικά δίκτυα, σε δεδομένα επικοινωνία και άλλα. Σε κοινωνικό δίκτυο δεδομένων, βάσει των σχέσεων φιλίας ενός ατόμου και των προτιμήσεων των φίλων του, μπορεί να είναι δυνατό να εξαχθούν συμπεράσματα για τις προσωπικές προτιμήσεις του εν λόγω προσώπου. Σε ένα τηλεπικοινωνιακό δίκτυο, η κλήση ενός άγνωστου ατόμου σε ένα γνωστό οργανισμό, μπορεί να θέσει σε κίνδυνο την ταυτότητα του αγνώστου, μέσω της άντλησης πληροφοριών

2.2.2 Μέθοδοι Υποκλοπής Προσωπικών Δεδομένων

Η γενικότερη κατηγορία πάνω στην οποία στηρίζεται η υποκλοπή προσωπικών δεδομένων είναι το κακόβουλο λογισμικό. Ως κακόβουλο λογισμικό χαρακτηρίζεται εκείνο το λογισμικό το οποίο έχει πρόθεση να βλάψει ένα υπολογιστικό σύστημα, με σκοπό την εκπλήρωση κάποιας κακόβουλης ενέργειας που θέλει να πετύχει ο προγραμματιστής της, όπως πρόσβαση σε ευαίσθητα προσωπικά δεδομένα (λίστα επαφών, κωδικούς πρόσβασης, φωτογραφίες, τραπεζικοί λογαριασμοί).Τα σημαντικότερα είδη κακόβουλων λογισμικών αναλύονται παρακάτω.

1) Ιός (Virus)

Είναι κακόβουλο λογισμικό το οποίο έχει τη δυνατότητα να εξαπλώνεται εύκολα σε χρήσιμα προγράμματα ενός ξένου υπολογιστή με αποτέλεσμα να βλάψει χρήσιμα αρχεία ενός χρήστη. Η μετάδοσή του σε άλλους υπολογιστές μπορεί να γίνει πολύ εύκολα με τη βοήθεια κάποιας εξωτερικής συσκευής όπως μια φορητή μνήμη USB ή ένας εξωτερικός σκληρός δίσκος. Ένα στοιχείο που διαφοροποιεί τους ιούς από τα άλλα προγράμματα είναι ότι μπορεί να μεταδοθεί οπουδήποτε έχει τη δυνατότητα. Τέλος οι επιπτώσεις που μπορεί να έχει ένας ιός είναι από το να διαγράψει κάποια δεδομένα έως και να οδηγήσει στην κατάρρευση ολόκληρου του συστήματος.

2) Δούρειος Ίππος (Trojan Horse)

Είναι κακόβουλο λογισμικό που χρησιμοποιεί το στοιχείο της παραπλάνησης. Λογισμικό αυτού του είδους παριστάνει ότι είναι χρήσιμο για τον υπολογιστή αλλά στην πραγματικότητα μέσα από αυτό καταφέρνουν να κλέψουν σημαντικά αρχεία ή να αποκτήσουν τον έλεγχο του συστήματος. Τις περισσότερες φορές το συγκεκριμένο λογισμικό δεν έχει στόχο τη μόλυνση του υπολογιστή, δηλαδή δεν αναπαράγεται, και για αυτό τα προγράμματα αυτά δεν χαρακτηρίζονται και επίσημα ως ιοί. [8]

3) Σκουλήκι (Warm)

Είναι κακόβουλο λογισμικό το οποίο μπορεί να μεταδοθεί άμεσα με τη χρήση κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος e-mail. Η ικανότητά

του να πολλαπλασιάζεται αυτόματα στο σύστημα στο οποίο βρίσκεται του δίνει τη δυνατότητα να αποστέλλει προσωπικά δεδομένα ή κωδικούς πρόσβασης, ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου. Τέλος, ένα άλλο αρνητικό χαρακτηριστικό είναι ότι επιβαρύνουν το δίκτυο, φορτώνοντάς το με άχρηστη δραστηριότητα.

4) Κερκόπορτα (Backdoor ή Trapdoor)

Η κερκόπορτα είναι η πιο επικίνδυνη κατηγορία δούρειων ίππων επειδή η λειτουργία της θυμίζει κανονικά προγράμματα απομακρυσμένης διαχείρισης. Οι κερκόπορτες εγκαθίστανται εν αγνοία του χρήστη και παρέχουν στον εισβολέα τη δυνατότητα απομακρυσμένης διαχείρισης του υπολογιστή. Έτσι, αυτή η κερκόπορτα είναι μια κρυφή λειτουργία μιας εφαρμογής η οποία έχει προγραμματιστεί με στόχο να εκμεταλλεύεται το σύστημα που θέλει και να αποσπά τις πληροφορίες που θέλει.

5) Κακόβουλοι Πράκτορες (Bot- Zombie)

Το bot είναι ένα είδος κακόβουλου λογισμικού που επιτρέπει σε έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο στον πληγέντα υπολογιστή. Οι υπολογιστές που έχουν μολυνθεί από ένα bot συνήθως αναφέρονται ως zombie. Ο επιτιθέμενος καθίσταται αόρατος με στόχο τον πλήρη έλεγχο του υπολογιστή [9].

Πρόκειται για κακόβουλο λογισμικό που προσβάλλει τους υπολογιστές καθιστώντας τους μέλη ενός δικτύου (botnet), το οποίο ελέγχεται εξ' αποστάσεως από τρίτους, με σκοπό τη πραγματοποίηση επιθέσεων κατά τις οποίες ένας αριθμός μολυσμένων υπολογιστών προσπαθεί να συνδεθεί στον υπολογιστή - στόχο μέσω δικτύου. Ο όρος bot προέρχεται από την τσεχικής προέλευσης λέξη «robota» και χρησιμοποιείται

6) Adware

Πρόκειται για λογισμικό υποστήριξης διαφημίσεων καθώς εμφανίζουν διαφημιστικά πλαίσια στο περιβάλλον άλλων προγραμμάτων και ανακατευθύνουν ερωτήματα αναζήτησης σε διαφημιστικούς δικτυακούς τόπους. Επίσης, μεταφέρουν και πληροφορίες με την άδεια του χρήστη.

Η εκτέλεση αυτού του λογισμικού μπορεί να γίνεται νόμιμα, στα πλαίσια μιας εφαρμογής που το ορίζει ρητώς στους όρους χρήσης της, ή με τρόπο μη φανερό. Στη δεύτερη περίπτωση τα λογισμικά τύπου adware θεωρούνται κακόβουλο λογισμικό. Το λογισμικό adware συνήθως συνεργάζεται με λογισμικό spyware.

Οι παρενέργειες ενός λογισμικού adware ποικίλλουν: εμφάνιση ανεπιθύμητων μηνυμάτων, αλλαγή αρχικής σελίδας του browser, αναδρομολόγηση σε λανθασμένο (πλαστό) δικτυακό τόπο (web spoofing).

2.3 Τεχνολογίες Διασφάλισης της Ιδιωτικότητας και Προστασία Προσωπικών Δεδομένων

Οι τεχνολογίες διασφάλισης ιδιωτικότητας ορίζονται ως τεχνικές και λειτουργικά πρότυπα που στοχεύουν στην προστασία της προσωπικής ταυτότητας και των προσωπικών δεδομένων που αποκαλύπτονται κατά τη χρήση δικτύων ηλεκτρονικών υπολογιστών

2.3.1 Απαιτήσεις Ιδιωτικότητας

Στη σημερινή ψηφιακή κοινωνία, οι νόμοι και οι κανονισμοί δεν επαρκούν για να καλύψουν την ιδιωτικότητα. Τα πληροφοριακά συστήματα που συλλέγουν δεδομένα θα πρέπει να αποτρέπουν την παραβίαση της ιδιωτικότητας και για το λόγο αυτό θα πρέπει να λαμβάνεται υπόψη σαν μια βασική παράμετρος που θα πρέπει να υλοποιηθεί.

Οι υπεύθυνοι για την προστασία δεδομένων απαιτούν πλέον από τους αναλυτές και προγραμματιστές πληροφοριακών συστημάτων να συμπεριλαμβάνουν την ιδιωτικότητα ως τεχνική απαίτηση που πρέπει να λαμβάνεται υπόψη στο υπο-ανάπτυξη σύστημα και πιο συγκεκριμένα θα πρέπει να λαμβάνεται υπόψη από τη φάση της σχεδίασης του συστήματος αποτελώντας ξεχωριστό κριτήριο που πρέπει να υλοποιηθεί.

Για τη μετατροπή της ιδιωτικότητας από μια γενική έννοια σε τεχνική απαίτηση, θα πρέπει να ικανοποιούνται κάποιες απαιτήσεις οι οποίες αναλύονται παρακάτω.

1)Αυθεντικοποίηση (Authentication)

Η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα του χρήστη. Σε ιδιωτικά και δημόσια δίκτυα, η αυθεντικοποίηση υλοποιείται συνήθως με τη χρήση κωδικών πρόσβασης. Αποτελεί κυρίως απαίτηση ασφάλειας παρά ιδιωτικότητας, ωστόσο έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας

2)Εξουσιοδότηση (Authorization)

Η διαδικασία μέσω της οποίας ο χρήστης αποκτά δικαιώματα-πρόσβαση σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος. Αν σε ένα σύστημα υπάρχουν πολλοί χρήστες, τότε ο διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα από αυτούς με τα αντίστοιχα δικαιώματα, ανάλογα με το ρόλο τους και τις υποχρεώσεις τους στο σύστημα.

3) Αναγνώριση (Identification)

Η διαδικασία μέσω της οποίας ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.

4) Ανωνυμία (Anonymity)

Η διαδικασία μέσω της οποίας διασφαλίζεται ότι ένας χρήστης μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με έναν άλλο χρήστη, χωρίς να αποκαλύψει την ταυτότητά του. Σύμφωνα με τους Pfitzmann και Hansen (2007), ανωνυμία μιας οντότητας σημαίνει ότι αυτή δεν είναι αναγνωρίσιμη μέσα σε ένα σύνολο οντοτήτων. Το σύνολο αυτό περιλαμβάνει όλες τις οντότητες που μετέχουν σε μια επικοινωνία και που πιθανόν θα μπορούσαν να αναγνωρισθούν από διάφορους επιτιθέμενους. [10].

5) Ψευδωνυμία (Pseydonymity)

Η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση του χρήστη από μη εξουσιοδοτημένους τρίτους χρήστες. Η Fischer-Hubner (2001) ορίζει τη ψευδωνυμία ως την απαίτηση που διασφαλίζει την απόκρυψη της ταυτότητας του χρήστη όταν αυτός ενεργεί στα πλαίσια μίας επικοινωνίας χρησιμοποιώντας ένα ή περισσότερα ψευδώνυμα. Η ψευδωνυμία υλοποιείται όταν δεν μπορεί να υλοποιηθεί η ανωνυμία.

6) Μη συνδεσιμότητα (Unlinkability)

Η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα του χρήστη από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, οδηγώντας έτσι στην αποκάλυψη της ταυτότητάς του χρήστη. Στην ουσία, μη συνδεσιμότητα σημαίνει πως ο επιτιθέμενος δεν είναι σε θέση να διακρίνει αν τα στοιχεία που τον ενδιαφέρουν μέσα σε ένα σύστημα (χρήστες, μηνύματα που εστάλησαν), σχετίζονται μεταξύ τους ή όχι.

7) Μη παρατηρησιμότητα (Unobservability)

Η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα του χρήστη από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν ίχνη του πρώτου. Σύμφωνα με τους Pfitzmann και Hansen (2007), μία οντότητα (π.χ. χρήστης, μήνυμα, ενέργεια) είναι μη-παρατηρήσιμη σε ένα σύνολο οντοτήτων όταν: α) ο επιτιθέμενος δεν μπορεί να εντοπίσει την οντότητα αυτή και β) ο κάτοχος της οντότητας αυτής παραμένει ανώνυμος σε σχέση με τους άλλους κατόχους των υπόλοιπων οντοτήτων

2.3.2 Τρόποι Προστασίας της Ιδιωτικότητας και των Προσωπικών Δεδομένων

Η προστασία των προσωπικών δεδομένων είναι μια εξαιρετικά πολύπλοκη διαδικασία στην οποία, εκτός από τον ίδιο το χρήστη, εμπλέκονται αρκετοί παράγοντες. Οι τεχνικές ρύθμισης της ιδιωτικότητας στο διαδίκτυο (Privacy Enhancing Technologies) αποτελούν ένα ευρύ φάσμα τεχνικών μέσων εξαλείφοντας ή εμποδίζοντας την περιττή ή/και ανεπιθύμητη επεξεργασία προσωπικών δεδομένων χωρίς να υπάρξει απώλεια της λειτουργικότητας του συστήματος πληροφοριών και για αυτό το λόγο έχουν αποκτήσει σημαντική δυναμική στον ακαδημαϊκό χώρο και τη βιομηχανία. Οι τεχνολογίες αυτές πολλές φορές θεωρούνται λανθασμένα ως υποκατάστατα άλλων μέσων προστασίας των προσωπικών δεδομένων (όπως η νομοθεσία). Στην πραγματικότητα, όμως, δρουν συμπληρωματικά με τους υφιστάμενους νόμους ώστε να εξασφαλίζεται η όσο το δυνατόν μεγαλύτερη ασφάλεια δεδομένων και είναι οι παρακάτω.

1)Πολιτικές Ιδιωτικότητας των Ιστιοτόπων

Τα μέτρα πολιτικής τα οποία θα πρέπει να λάβουν οι οργανισμοί και οι υπηρεσίες που συλλέγουν προσωπικές πληροφορίες στο διαδίκτυο, είναι αναμφισβήτητα το πιο σημαντικό εργαλείο για την προστασία της ιδιωτικής ζωής. Οι πολιτικές ιδιωτικότητας που αναγράφουν οι ιστότοποι στις αρχικές τους σελίδες, αποτελούν στην ουσία ένα είδος υπόσχεσης της διαδικτυακής εταιρείας να επεξεργαστεί τα ιδιωτικά δεδομένα των χρηστών της με ένα συγκεκριμένο τρόπο. Περιλαμβάνουν προτάσεις που αναφέρονται στον τρόπο συλλογής των ιδιωτικών δεδομένων, στη μη χρησιμοποίηση των δεδομένων αυτών για άλλους σκοπούς εκτός της παρούσας συναλλαγής και στη μη παροχή των δεδομένων αυτών προς τρίτα μη εξουσιοδοτημένα μέρη.

Σημαντικό είναι επίσης το γεγονός πως οι συγκεκριμένες πολιτικές αφορούν κυρίως τις συμμετέχουσες οντότητες που επεξεργάζονται τα δεδομένα προκειμένου να παρέχουν εξατομικευμένες υπηρεσίες στο χρήστη. Εντούτοις, δεν επαρκούν ενάντια σε μια τρίτη, κακόβουλη οντότητα η οποία επιθυμεί να υποκλέψει τα δεδομένα αυτά.

Παράλληλα, ο καθορισμός μιας τέτοιας πολιτικής βρίσκεται στην ευχέρεια του κάθε φορέα παροχής υπηρεσιών, με αποτέλεσμα να μην υπάρχει μια κοινή πολιτική προστασίας της ιδιωτικότητας. Τέλος, δεδομένου ότι οι εφαρμογές αυτές είναι σχετικά νέες, είναι αμφισβητήσιμο το πόσο αποτελεσματικά είναι αυτά τα μέτρα για την προστασία των χρηστών. Για το λόγο αυτό, δεν επαρκεί να ορίζονται μόνο οι πολιτικές ιδιωτικότητας αλλά θα πρέπει να λαμβάνονται και άλλα μέτρα προστασίας των δεδομένων.

2) Κρυπτογραφία

Η κρυπτογραφία (Encryption) είναι μια από τις βασικότερες τεχνικές προκειμένου να επιτευχθεί η αυθεντικοποίηση του χρήστη καθώς και η προστασία των δεδομένων από πιθανή κακόβουλη χρήση. Πρόκειται για μια μέθοδο παραλλαγής του απλού κειμένου (plaintext) σε μη αναγνώσιμη μορφή χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης με αποτέλεσμα τη δημιουργία του cipher text. Με αυτό τον τρόπο, οι πληροφορίες μετατρέπονται από έναν αλγόριθμο και γίνονται δυσανάγνωστες. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά [11].

Στο plaintext τα δεδομένα είναι ευανάγνωστα και κατανοητά. Στο cipher text τα δεδομένα προκύπτουν αν στο plaintext εφαρμοστεί ένας αλγόριθμος κρυπτογράφησης. Κλειδί (key) ονομάζεται ένα κομμάτι πληροφορίας το οποίο υπολογίζει την έξοδο ενός αλγορίθμου και καθορίζει την αλλαγή από το plaintext στο cipher text.

Στόχος, επομένως, της κρυπτογραφίας είναι να επικοινωνούν δύο άνθρωποι από ένα μη ασφαλές κανάλι χωρίς να υποκλαπεί το μήνυμά τους. Έτσι, ένα κρυπτοσύστημα αποτελείται από τις εξής πέντε παραμέτρους:

1. Τα plaintexts
2. Τα cipher texts
3. Τα κλειδιά
4. Την κρυπτογραφική μετατροπή ή κρυπτογραφική συνάρτηση
5. Την αντίθετη συνάρτηση ή αποκρυπτογραφική μετατροπή

3)Ψηφιακές υπογραφές

Ο σκοπός της τεχνικής των ψηφιακών υπογραφών είναι να συνδυάσει μοναδικά την πληροφορία με την ταυτότητα του κατόχου της. Πρόκειται για ένα εργαλείο που παρέχει ακεραιότητα των δεδομένων και πιστοποίηση ταυτότητας. Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων και την ταυτοποίηση ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία το αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας συνάρτησης κατακερματισμού και του ιδιωτικού κλειδιού του αποστολέα.

Η σωστή εφαρμογή της ψηφιακής υπογραφής σε ένα κρυπτογραφημένο σύστημα διασφαλίζει θεμελιώδεις απαιτήσεις ασφαλείας όπως την αυθεντικότητα των δεδομένων και της πηγής (data origin authentication, data source authentication), την ακεραιότητα της πληροφορίας (data integrity) την εξουσιοδότηση του υπογράφοντα (authorization) και την αποφυγή άρνησης αποστολής της από αυτόν (non-repudiation). Η απαίτηση για non-repudiation προσθέτει ένα επιπλέον επίπεδο ασφαλείας σε ένα κρυπτογραφημένο σύστημα καθώς, εάν ο δημιουργός μιας υπογραφής την αποστείλει και στη συνέχεια το αρνηθεί, αυτό σημαίνει ότι ψεύδεται διότι η υπογραφή θα επικυρώνεται με τη χρήση του δημοσίου κλειδιού.

4) **Ασφάλεια Περιμέτρου**

Ως Περίμετρος Δικτύου ορίζονται όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα (διαδίκτυο, δίκτυα άλλων υποκαταστημάτων του παρόχου, δίκτυα συνεργατών του, ασύρματα δίκτυα, κλπ). Ο πρωταρχικός σκοπός της πολιτικής ασφαλείας περιμέτρου είναι να προστατεύσει τους διάφορους δικτυακούς πόρους του παρόχου διαδικτύου από εισβολείς, δηλαδή να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του παρόχου, καθώς και τη διακοπή της ομαλής παροχής των υπηρεσιών του. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΕΑ) υποχρεώνει κάθε πάροχο διαδικτύου, συνεπώς έμμεσα και κάθε οργανισμό ηλεκτρονικού εμπορίου, να χρησιμοποιεί συστήματα firewall για την προστασία των συνδέσεων του δικτύου του με το διαδίκτυο και επιπλέον τον υποχρεώνει να χρησιμοποιεί συστήματα ανίχνευσης εισβολών για την ενίσχυση της προστασίας του δικτύου [80].

Ένα σύστημα firewall (τοίχος προστασίας) καλείται να λειτουργήσει ως μηχανισμός «περιμετρικής άμυνας», ο οποίος δρα συμπληρωματικά με τους υπόλοιπους μηχανισμούς ασφάλειας. Σκοπός του είναι ο έλεγχος και η καταγραφή όλων των προσπαθειών προσπέλασης οι οποίες κατευθύνονται προς το προστατευμένο σύστημα, με το να επιτρέπει, να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του. Η κύρια λειτουργία του είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ το εταιρικό δίκτυο ή το δίκτυο ενός σπιτιού διαθέτει το μέγιστο βαθμό εμπιστοσύνης.

2.4 Ανώνυμα Δεδομένα

Τα Ανώνυμα Δεδομένα είναι μία τεχνική που χρησιμοποιείται από οργανισμούς, οι οποίοι χρησιμοποιούν ευαίσθητα προσωπικά δεδομένα, για την εξαγωγή συμπερασμάτων και αποτελεσμάτων από έρευνες που έχουν προηγηθεί. Με αυτή την τεχνική, οι οργανισμοί αυτοί ανωνυμοποιούν τα δεδομένα από τις βάσεις που χρησιμοποιούν ώστε να μην μπορούν να υποκλαπούν και να ταυτοποιηθούν τα άτομα στα οποία ανήκουν.

Βασική ιδέα του κλάδου της ανωνυμοποίησης δεδομένων είναι ο μετασχηματισμός των αρχικών αυτών δεδομένων σε μία μορφή που αντιμετωπίζει τους κινδύνους περιορίζοντας την απώλεια πληροφορίας. Οι εν λόγω κίνδυνοι αφορούν τρεις παραμέτρους. Πρώτον, την αποκάλυψη συμμετοχής, όταν και μόνο όταν η συμμετοχή στα δημοσιευμένα δεδομένα είναι ευαίσθητη πληροφορία. Δεύτερον, την αναγνώριση, όταν εντοπίζουμε μια εγγραφή που αναφέρεται σε ένα πρόσωπο. Και τρίτον, τη συσχέτιση, όταν συσχετίζουμε μια ευαίσθητη τιμή με ένα πρόσωπο[12].

2.4.1 Linking Attacks και *k*-Anonymity

Η πρώτη τεχνική προστασίας που προτάθηκε για την ανωνυμοποίηση δεδομένων ήταν αυτή της *k*-Anonymity, η οποία σχεδιάστηκε για την προστασία από μία κατηγορία επιθέσεων που χαρακτηρίζονται ως Linking Attacks. Μια βάση δεδομένων ονομάζεται *k*-ανώνυμη εάν δεν υπάρχει καμία ερώτηση που να μπορεί να εξάγει λιγότερες από *k* εγγραφές από αυτή.
Η τιμή του *k* καθορίζει την αναλογία μεταξύ της απώλειας πληροφορίας και ισχύος της ανωνυμίας των ανωνυμοποιημένων δεδομένων[13].

Στόχος, λοιπόν, της προστασίας ιδιωτικότητας είναι να μειωθεί η πιθανότητα να προσδιοριστεί μοναδικά μια συγκεκριμένη οντότητα, ακόμα και με τη διασταύρωση δημοσιευμένων εγγράφων που μπορεί να είναι ανωνυμοποιημένα. Για να γίνει αυτό, πρέπει ουσιαστικά να υπάρχει μία μέγιστη πιθανότητα το πολύ *k*, ένας επιτιθέμενος πρέπει να μπορεί να ανακαλύψει με κάποια σύνδεση πινάκων, δηλαδή σε ποιο άτομο ανήκει μια εγγραφή ή ένα σύνολο εγγραφών.

Με τη μέθοδο της *k*-ανωνυμίας εξασφαλίζεται ότι, η πιθανότητα ανακάλυψης της ταυτότητας μιας εγγραφής είναι το πολύ $1/k$. Επειδή είναι σπάνια τα σύνολα δεδομένων που συλλέγονται να ικανοποιούν την *k*-ανωνυμία στην αρχική τους μορφή, ο τομέας της προστασίας της ιδιωτικότητας έχει αναπτύξει τεχνικές και αλγορίθμους ώστε να τροποποιούνται τα δεδομένα προς μία μορφή τέτοια ώστε να ικανοποιείται η *k*-ανωνυμία. Συνήθως, από τις διαδικασίες αυτές προκύπτει μια νέα έκδοση του πίνακα δεδομένων.

Οι μετασχηματισμοί δεδομένων που χρησιμοποιούνται κατά την ανωνυμοποίηση με την τεχνική της *k*-ανωνυμίας είναι οι κάτωθι:

- **Η μέθοδος της Γενίκευσης (Generalization)**

Η μέθοδος της γενίκευσης συνιστά μια πολύ χρήσιμη τεχνική στο χώρο της προστασίας της ιδιωτικότητας. Με τη χρήση της επιτυγχάνεται η αντικατάσταση της αρχικής τιμής ενός πεδίου με μια άλλη τιμή πιο γενική. Αυτό έχει ως αποτέλεσμα να διατηρείται μέρος της πληροφορίας που περιέχει η αρχική τιμή, χωρίς να αλλοιώνεται πλήρως. Με την σειρά της, αυτή η γενικευμένη τιμή μπορεί να γενικευτεί ξανά σε μια πιο γενικευμένη τιμή διατηρώντας πάλι την

ίδια σημασιολογία με την αρχική τιμή του πεδίου. Για τη γενίκευση ακολουθείται ένα δέντρο ιεραρχίας όπου τα φύλλα απεικονίζονται στην τιμή του γονέα, αυτή στου δικού του γονέα πηγαίνοντας μέχρι τη ρίζα του δέντρου που σημασιολογικά αντιστοιχεί σε όλες τις τιμές.

- **Η μέθοδος της Απόκρυψης (Suppression)**

Σε αυτήν την περίπτωση αφαιρούνται δεδομένα από το σύνολο εγγραφών προκειμένου να ελαχιστοποιηθεί το επίπεδο γενίκευσης και να μειωθεί η απώλεια πληροφορίας στα δεδομένα.

2.4.2 Inference Attack

Είναι πολύ σημαντικό να αναφερθεί ότι παρά την χρήση ανώνυμων δεδομένων μπορεί να υπάρχει παραβίαση της ιδιωτικότητας μέσω του συνδυασμού τους. Μία τέτοια τεχνική εξόρυξης δεδομένων είναι το Inference Attack, το οποίο εκτελείται αναλύοντας ανώνυμα δεδομένα με σκοπό να αποκτήσει ο επιτιθέμενος παράνομα γνώσεις σχετικά με μία βάση δεδομένων ή έναν άνθρωπο[14]. Οι ευαίσθητες πληροφορίες ενός ανθρώπου μπορεί να θεωρηθεί ότι έχουν υποστεί διαρροή, εφόσον ο επιτιθέμενος μπορεί να συμπεράνει με μεγάλη βεβαιότητα την πραγματική τιμή(value) των προσωπικών του δεδομένων καταλήγοντας σε αυτά με τον συνδυασμό ανώνυμων δεδομένων. Ουσιαστικά, μία επίθεση ανήκει στην κατηγορία Inference Attack όταν ένας χρήστης μπορεί να συμπεράνει από ασήμαντες πληροφορίες πιο σημαντικές και ευαίσθητες πληροφορίες για έναν άνθρωπο μέσω βάσης δεδομένων, χωρίς όμως να έχει άμεσα πρόσβαση σε αυτή[14].

2.5 Νομοθεσία για Προστασία Προσωπικών Δεδομένων

Γενικά, ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Ε.Ε.) προβλέπει ότι όλοι οι πολίτες της Ε.Ε. έχουν το δικαίωμα προστασίας των προσωπικών δεδομένων τους. Είναι πολύ σημαντικό να αναφερθεί ότι πάνω από το 90% των Ευρωπαίων πολιτών δήλωσε τον Μάιο του 2016 την επιθυμία του να ισχύουν τα ίδια δικαιώματα προστασίας των προσωπικών δεδομένων σε όλη την Ε.Ε. , ανεξάρτητα από το που πραγματοποιείται η επεξεργασία τους. [15]

2.5.1 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Ο Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο κανονισμός αυτός αποτελεί ένα ουσιαστικό βήμα για την ενίσχυση των θεμελιωδών δικαιωμάτων των πολιτών στην ψηφιακή εποχή, αλλά και για τη διευκόλυνση των επιχειρήσεων με την απλούστευση των κανόνων για τις επιχειρήσεις στην ενιαία ψηφιακή αγορά. Με ενιαία νομοθετική ρύθμιση θα ξεπεραστεί επίσης ο σημερινός κατακερματισμός και ο δαπανηρός διοικητικός φόρτος. Ο κανονισμός τέθηκε σε ισχύ στις 24 Μαΐου 2016 και θα αρχίσει να εφαρμόζεται από τις 25 Μαΐου 2018 [16].

Όσον αφορά την αστυνομία εκδόθηκε η Οδηγία (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η οδηγία αυτή προστατεύει το θεμελιώδες δικαίωμα των πολιτών για την προστασία των δεδομένων, όταν αυτά χρησιμοποιούνται από αρχές επιβολής του ποινικού δικαίου. Ειδικότερα, θα διασφαλίσει την κατάλληλη προστασία των προσωπικών δεδομένων θυμάτων, μαρτύρων και υπόπτων εγκληματικών πράξεων και θα διευκολύνει τη διασυνοριακή συνεργασία για την καταπολέμηση του εγκλήματος και της τρομοκρατίας. Η οδηγία τέθηκε σε ισχύ στις 5 Μαΐου 2016 και τα κράτη μέλη της ΕΕ οφείλουν να τη μεταφέρουν στο εθνικό τους δίκαιο έως τις 6 Μαΐου 2018.

Επιπλέον, αξίζει να σημειωθεί ότι οι χώρες της Ευρωπαϊκής Ένωσης έχουν συγκροτήσει εθνικούς φορείς για την προστασία των προσωπικών δεδομένων σύμφωνα με το άρθρο 8 παράγραφος 3 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

2.5.2 Προστασία Δεδομένων στα Όργανα και στους Οργανισμούς της Ευρωπαϊκής Ένωσης

Ο κανονισμός 45/2001 καθορίζει τους κανόνες που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της ΕΕ. Στις 10 Ιανουαρίου 2017, η Επιτροπή υπέβαλε πρόταση τροποποίησης των κανόνων αυτών ώστε να είναι σύμφωνοι με τον γενικό κανονισμό για την προστασία δεδομένων (ΓΚΠΔ). Με τον κανονισμό για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τα όργανα της ΕΕ θεσπίστηκε ο Ευρωπαίος επόπτης προστασίας δεδομένων (ΕΕΠΔ). Ο ΕΕΠΔ είναι ένα ανεξάρτητο όργανο της ΕΕ αρμόδιο για τον έλεγχο της εφαρμογής των κανόνων περί προστασίας δεδομένων εντός των ευρωπαϊκών θεσμικών οργάνων καθώς και για τη διερεύνηση καταγγελιών. Επιπλέον, η Ευρωπαϊκή Επιτροπή έχει ορίσει έναν υπεύθυνο προστασίας δεδομένων, αρμόδιο για την παρακολούθηση και την εφαρμογή των κανόνων προστασίας των δεδομένων στην Ευρωπαϊκή Επιτροπή. Ο υπεύθυνος προστασίας δεδομένων διασφαλίζει ανεξάρτητα την εσωτερική εφαρμογή των κανόνων προστασίας των δεδομένων σε συνεργασία με τον Ευρωπαίο επόπτη προστασίας δεδομένων[15].

2.5.3 Επικρατούσα Νομοθεσία στην Ελλάδα

Νόμος 4624/2019 : Αφορά την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τα μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 καθώς και άλλες διατάξεις[17].

Προεδρικό Διάταγμα 75/2020 - ΦΕΚ 173/Α/10-9-2020: Αφορά την χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους Με το παρόν διάταγμα θεσπίζονται οι ειδικότεροι κανόνες για την εγκατάσταση και λειτουργία, σε

δημόσιους χώρους, συστημάτων λήψης ή καταγραφής ήχου ή εικόνας (εφεξής συστήματα επιτήρησης), στο μέτρο που διενεργείται επεξεργασία δεδομένων προσωπικού χαρακτήρα, κατά τρόπο ώστε να επιτυγχάνονται αποτελεσματικά οι σκοποί που προβλέπονται στο άρθρο 14 του ν. 3917/2011 (Α' 22), με ταυτόχρονη διασφάλιση των δικαιωμάτων των προσώπων που θίγονται από τη χρήση των συστημάτων αυτών.

Νόμος 3917/201: Αφορά την διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις. Οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών υποχρεούνται να διατηρούν τα δεδομένα του άρθρου 5 που παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς, προκειμένου τα δεδομένα αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, όπως αυτά ορίζονται στο άρθρο 4 του νόμου 2225/1994 (ΦΕΚ 121 Α').

Νόμος 3471/2006-ΦΕΚ 133/Α/28-6-2006: Αφορά την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και σκοπός των διατάξεων των άρθρων 1 έως 17 του παρόντος νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

2.6 Τεχνολογίες Υλοποίησης

Στο κεφάλαιο αυτό αναλύονται όλες οι τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίηση της εφαρμογής.

2.6.1 Java (Programming Language)

Η Java είναι μία αντικειμενοστραφής γλώσσα προγραμματισμού που σχεδιάστηκε από την εταιρία πληροφορικής Sun Microsystems και δημοσιεύτηκε στον κόσμο της πληροφορικής τον Μάρτιο του 1995. Είναι ίσως η πιο δημοφιλής γλώσσα προγραμματισμού χάρη στην ανεξαρτησία της απέναντι στο λειτουργικό σύστημα της πλατφόρμας. Με άλλα λόγια, τα προγράμματα σε γλώσσα Java τρέχουν ακριβώς το ίδιο σε Windows, Linux, Unix και Mac χωρίς να χρειαστεί να ξαναγίνει μεταγλώττιση (compiling) ή να αλλάξει ο πηγαίος κώδικας για κάθε διαφορετικό λειτουργικό σύστημα[18].

Η Java ως αντικειμενοστραφής γλώσσα βασίζεται στην χρήση αντικειμένων. Τα αντικείμενα είναι συλλογές πεδίων πληροφορίας και μεθόδων επεξεργασίας και προβολής πληροφορίας. Τα διάφορα αντικείμενα ανήκουν σε κλάσεις, οι οποίες δηλώνουν τον τύπο ομοειδών αντικειμένων. Κάθε μέλος μίας κλάσης, είτε πεδίο είτε μέθοδος, προσδιορίζεται από έναν μετατροπέα ορατότητας. Υπάρχουν τέσσερεις μετατροπείς ορατότητας: private, package-private (με κενό μετατροπέα), protect και public. Τα private μέλη είναι ορατά μόνο από την ίδια κλάση, τα package-private είναι ορατά από κλάσεις του ίδιου πακέτου, τα protected από κλάσεις του ίδιου πακέτου και από κλάσεις εκτός πακέτου που επεκτείνουν (extends) αυτήν την τάξη. Τα public μέλη είναι ορατά από όλες τις κλάσεις της εφαρμογής.

Τέλος, η Java χρησιμοποιείται για ανάπτυξη εφαρμογών κινητού τηλεφώνου (Mobile Applications), εφαρμογών Η/Υ (Desktop Applications), εφαρμογών ιστού (Web Applications), παιχνιδιών (Gaming), εφαρμογών με διεπαφή χρήστη (GUI Applications) και ιστοσελίδων (Websites)[19].

2.6.2 SQL (Programming Language for Databases)

Η SQL (Structured Query Language) είναι μία γλώσσα προγραμματισμού για βάσεις δεδομένων. Σχεδιάστηκε για διαχείριση δεδομένων σε ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων και αρχικά βασίστηκε στην σχεσιακή άλγεβρα. Αναπτύχθηκε στην IBM από τους Andrew Richardson Donald C. Messerly και Raymond F. Boyce, στις αρχές της δεκαετίας του 1970[20].

Η SQL ως γλώσσα περιλαμβάνει δυνατότητες ανάκτησης και ενημέρωσης δεδομένων, δημιουργίας και τροποποίησης σχεσιακών πινάκων, αλλά και ελέγχου πρόσβασης στα δεδομένα.

Η γλώσσα SQL υποδιαιρείται σε διάφορα γλωσσικά στοιχεία, που περιλαμβάνουν Clauses, οι οποίες είναι σε μερικές περιπτώσεις προαιρετικές, αλλά απαραίτητα συστατικά των δηλώσεων και ερωτήσεων, Expressions που μπορούν να παραγάγουν είτε τις κλιμακωτές τιμές είτε πίνακες που αποτελούνται από στήλες και σειρές στοιχείων, Predicates που διευκρινίζουν τους όρους που μπορούν να αξιολογηθούν σαν σωστό ή λάθος, Queries που ανακτούν τα στοιχεία βασισμένες σε ειδικά κριτήρια και Statements που μπορούν να έχουν μια επίδραση στα σχήματα και τα στοιχεία, ή που μπορούν να ελέγξουν τη ροή του προγράμματος και τις συνδέσεις από άλλα προγράμματα[21].

2.6.3 Apache Netbeans (Programming Environment for Java GUI Applications)

Το Apache Netbeans είναι ένα προγραμματιστικό περιβάλλον για σχεδιασμό εφαρμογών με διεπαφή χρήστη (GUI) με κύρια χρήση της γλώσσας προγραμματισμού Java[22]. Εκτός από Java editor, το Apache Netbeans περιέχει μία τεράστια ποικιλία από εργαλεία (tools), πρότυπα (templates) και επεκτάσεις (plugins) για συνδυασμό τεχνολογιών καθώς και αύξηση της λειτουργικότητας των εφαρμογών του που είναι υπό ανάπτυξη[23].

2.6.4 Xampp (Open Source Package for Databases)

Το Xampp είναι ένα πακέτο ανοιχτού κώδικα που χρησιμοποιείται για την αποθήκευση και την λειτουργικότητα μία βάσης δεδομένων που είναι συνδεδεμένη με μία εφαρμογή ή ιστοσελίδα στον τοπικό server του υπολογιστή (localhost server), έτσι δίνεται η δυνατότητα στον χρήστη να αναπτύξει και να υλοποιήσει μία εφαρμογή ή ιστοσελίδα βλέποντας την κανονικής της λειτουργία όπως θα ήταν σε έναν πραγματικό server[24][25].

2.6.5 Jasper Report (Plugin)

Το Jasper Report είναι ένα δυναμικό open source εργαλείο για δημιουργία αναφοράς. Μέσω αυτού έχουμε την δυνατότητα να δημιουργούμε αυτοματοποιημένη αναφορά με την χρήση ή μη βάσης δεδομένων με απώτερο σκοπό την εμφάνιση της στην οθόνη μας έχοντας επιλογές εκτύπωσης ή αποθήκευσης σε πληθώρα τύπων αρχείου (Pdf, Html, Xls, Rtf, Odt, Csv, Txt, Xml). Κυρίως χρησιμοποιείται από την γλώσσα προγραμματισμού Java και τα αντίστοιχα περιβάλλοντα της με σκοπό να γενικεύσει το δυναμικό περιεχόμενο[26].

Κεφάλαιο 3: IB Privacy Advisor App

Στο κεφάλαιο αυτό θα αναλυθεί η εφαρμογή που αναπτύχθηκε τόσο στην φάση των απαιτήσεων της όσο και στην φάση της ανάλυσης της σε επίπεδο αρχιτεκτονικής και λογισμικού.

3.1 Απαιτήσεις και Εγκατάσταση

Οι απαιτήσεις του IB Privacy Advisor App έτσι ώστε να εγκατασταθεί σε Windows και να είναι ικανό να τρέξει είναι οι εξής:

- Java JDK 8+
- Apache Netbeans IDE 11+ or Java Netbeans IDE 8+
- Xampp v3.2.4+
- mysql-connector-java-8.0.18 +
- jasperreports-fonts-6.14.0
- iReport-5.6.0-plugin

3.2 Ανάλυση Εφαρμογής

Η IB Privacy Advisor App είναι μία εφαρμογή GUI επικεντρωμένη στον χρήστη (user-focused), υλοποιημένη σε γλώσσα προγραμματισμού Java με χρήση βάσης δεδομένων σε γλώσσα SQL. Δίνει την δυνατότητα στον χρήστη να κατανοήσει πόσο σημαντικά είναι τα προσωπικά δεδομένα και η ορθή χρήση τους. Πιο συγκεκριμένα, αναλύει μία βάση δεδομένων και δίνει την δυνατότητα στο χρήστη μέσω πιθανο-στατιστικών τεχνολογιών και την εφαρμογή του νόμου του Bayes (Rule of Bayes) να κατανοήσει την πιθανότητα για επίθεση και υποκλοπή προσωπικών δεδομένων. Ειδικότερα, χρησιμοποιούνται έξι μεταβλητές (attributes), οι οποίες αντιστοιχούν σε έξι προσωπικά δεδομένα ,πάνω στις οποίες ο χρήστης έχει την δυνατότητα να ενημερωθεί για την πιθανότητα επίθεσης. Υπάρχουν τρία στάδια για το ποσοστό της πιθανότητας επίθεσης, το μικρό, το μεσαίο και το μεγάλο. Αν το ποσοστό της εκάστοτε μεταβλητής του χρήστη ανήκει στο μεγάλο στάδιο, ο χρήστης έχει την δυνατότητα να επιλέξει αν επιθυμεί να δώσει ή όχι το συγκεκριμένο προσωπικό δεδομένο του. Τέλος, ο χρήστης έχει την δυνατότητα να κατεβάσει ή να εκτυπώσει αναφορά με τα αντίστοιχα αποτελέσματα της κάθε μεταβλητής.

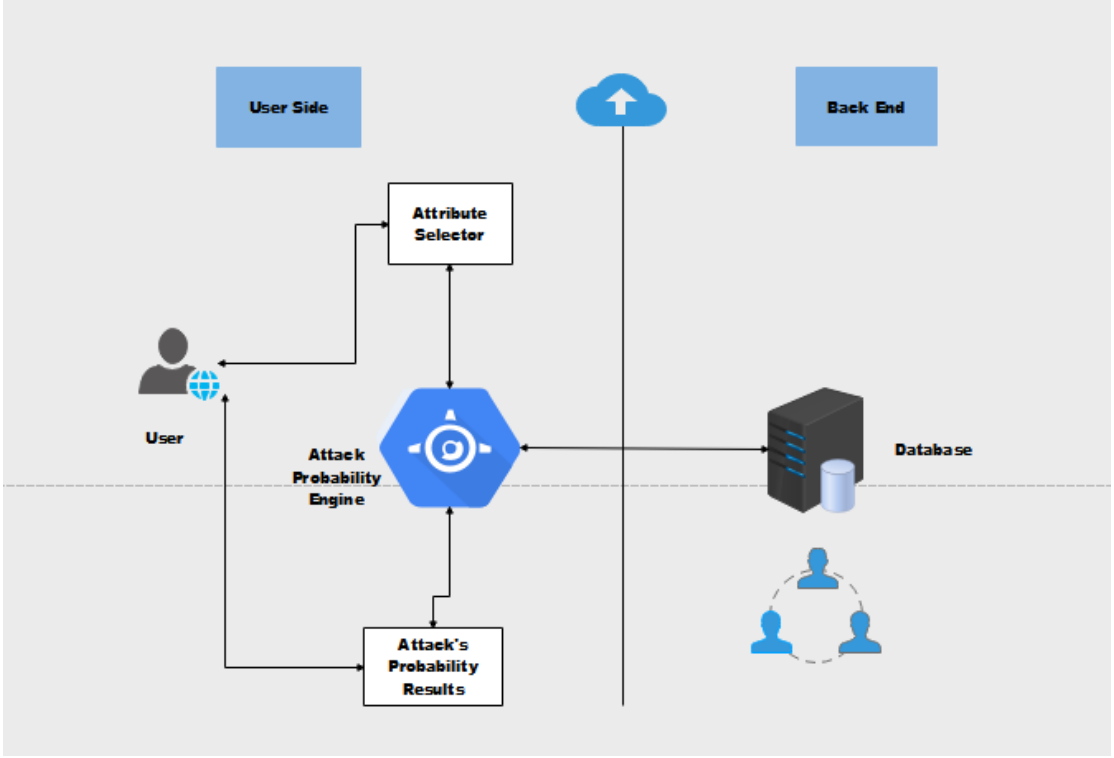
3.2.1 Αρχιτεκτονική

Η αρχιτεκτονική του IB Privacy Advisor App αποτελείται από τρία κύρια περιεχόμενα και αυτά παρουσιάζονται παρακάτω:

- **Επιλογή Μεταβλητής (Attribute Selector):** Ο χρήστης επιλέγει μία από τις έξι μεταβλητές του συστήματος, οι οποίες αντιστοιχούν σε προσωπικά δεδομένα των χρηστών, ώστε να αλληλεπιδράσει με το σύστημα και έπειτα να οδηγηθεί στην πιθανότητα επίθεσης της συγκεκριμένης μεταβλητής.

- **Μηχανισμός Πιθανότητας Επίθεσης (Attack Probability Engine):** Ο μηχανισμός Πιθανότητα επίθεσης είναι το πιο σημαντικό κομμάτι της εφαρμογής. Εδώ, αφού έχει προηγηθεί η επιλογή μεταβλητής από τον χρήστη, η εφαρμογή υπολογίζει την πιθανότητα επίθεσης στην συγκεκριμένη μεταβλητή μέσω των τιμών που είναι αποθηκευμένες στην βάση δεδομένων και της πιθανότητα Bayes και δίνετε η δυνατότητα στον χρήστη να επιλέξει αν επιθυμεί ή όχι να δώσει το συγκεκριμένο προσωπικό δεδομένο, εφόσον η πιθανότητα επίθεσης της μεταβλητής ανήκει στο μεγάλο στάδιο. Έπειτα ο χρήστης οδηγείται στα αποτελέσματα της πιθανότητας επίθεσης.

- **Αποτελέσματα Πιθανότητας Επίθεσης (Attack's Probability Results):** Στα αποτελέσματα Πιθανότητας Επίθεσης ο χρήστης έχει την δυνατότητα να δει όλα τα αποτελέσματα που προκύπτουν από τον υπολογισμό της πιθανότητας επίθεσης καθώς και να εκτυπώσει ή να κατεβάσει την αντίστοιχη αναφορά.



Εικόνα 3.2.1.1 Αρχιτεκτονική IB Privacy Advisor App

3.2.2 Επιλογή Μεταβλητής (Attribute Selector)

Όπως αναφέρθηκε και παραπάνω, η επιλογή μεταβλητής είναι η πρώτη και πιο βασική διαδικασία που πρέπει να υλοποιήσει ο χρήστης πριν οδηγηθεί στον μηχανισμό Πιθανότητας Επίθεσης. Πιο συγκεκριμένα, ο χρήστης έχει να επιλέξει ανάμεσα από έξι μεταβλητές οι οποίες είναι όνομα, επώνυμο, διεύθυνση, ταχυδρομικό κώδικα, πόλη και χώρα. Αφού υπολογιστεί η πιθανότητα επίθεσης γίνεται η ομαδοποίηση της σε μία από τις τρεις κατηγορίες σχετικά με το ποσοστό για πιθανότητα επίθεσης στην συγκεκριμένη μεταβλητή. Οι 3 κατηγορίες,οι οποίες παρουσιάζονται παρακάτω είναι:

- **Μικρό Ρίσκο (Negligible Risk)**: Η πιθανότητα επίθεσης κυμαίνεται από 0% έως 33%.
- **Μεσαίο Ρίσκο (Significant Risk)**: Η πιθανότητα επίθεσης κυμαίνεται από 33% έως 66%.
- **Μεγάλο Ρίσκο (High Risk**): Η πιθανότητα επίθεσης κυμαίνεται από 66% έως 100%.

Attack Probability score	**Interpretation**
0% < AP < 33%	Negligible Risk
33% ≤ AP < 66%	Significant Risk
66% ≤ AP < 100%	High Risk

Εικόνα 3.2.2.1 Πίνακας κατηγοριών ανάλογα με την πιθανότητα επίθεσης σε μία μεταβλητή.

Είναι σημαντικό να σημειωθεί ότι αν η πιθανότητα επίθεσης ανήκει στην κατηγορία Μεγάλο Ρίσκο (High Risk), ο χρήστης έχει την δυνατότητα να επιλέξει αν επιθυμεί η όχι να δώσει το αντίστοιχο προσωπικό του δεδομένο στο σύστημα.

3.2.3 Πιθανότητα Bayes (Νόμος του Bayes)

Ο Νόμος του Bayes (Rule of Bayes) είναι ένα θεώρημα με εφαρμογή πάνω στην θεωρία πιθανοτήτων και στην στατιστική, το οποίο συσχετίζει την τρέχουσα πιθανότητα με την αρχική πιθανότητα. Επιπλέον, είναι ένα σημαντικό θεώρημα για την κατανόηση του μαθηματικού χειρισμού της υπό-συνθήκης πιθανότητας.

Το θεώρημα Bayes πήρε το όνομα του έτσι από τον βρετανό κληρικό Thomas Bayes (1701–1761), ο οποίος πρώτος έδειξε τον τρόπο που χρησιμοποιούνται τα νέα στοιχεία για την ανανέωση των εκάστοτε πεποιθήσεων. Αυτό αναπτύχθηκε περαιτέρω από τον Pierre-Simon Laplace, ο οποίος πρώτος δημοσίευσε τη μοντέρνα διατύπωση το 1812 στο βιβλίο του “Théorie analytique des probabilités”. Ο Harold Jeffreys έθεσε τον αλγόριθμο του Bayes και την διατύπωση του Laplace σε αξιωματική βάση. Ο Jeffreys έγραψε πως το θεώρημα Bayes "είναι στη θεωρία πιθανοτήτων όπως αντίστοιχα το Πυθαγόρειο θεώρημα στη Γεωμετρία "[27].

Το θεώρημα Bayes ορίστηκε μαθηματικά ως η ακόλουθη συνάρτηση:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

,όπου Α και Β είναι γεγονότα.

Η P(A) και η P(B) είναι οι πιθανότητες των Α και Β αντίστοιχα και είναι ανεξάρτητες μεταξύ τους. Η P(A|B) είναι η υπό-συνθήκη πιθανότητα, δηλαδή η πιθανότητα του Α δεδομένου του Β να είναι αληθής και τέλος η P(B|A) είναι η πιθανότητα του Α δεδομένου του Β να είναι αληθής.

Στο δικό μας πρόβλημα, η πιθανότητα επίθεσης σε μία μεταβλητή (*AP*) ορίζεται ως εξής στηριζόμενη στην πιθανότητα Bayes:

$$AP = \frac{sum - sva}{sum}$$

,όπου *AP* η πιθανότητα επίθεσης στην αντίστοιχη μεταβλητή, *sum* το πλήθος τον χρηστών της βάσης δεδομένων της εφαρμογής και *sva* το πλήθος τον χρηστών με την ίδια τιμή στην ίδια μεταβλητή.

3.2.4 Εμφάνιση Αποτελεσμάτων (Results)

Έπειτα από τον υπολογισμό της πιθανότητας επίθεσης σε μία μεταβλητή ο χρήστης έχει την δυνατότητα να δει στην οθόνη του τα αντίστοιχα αποτελέσματα. Τα αποτελέσματα περιέχουν τα παρακάτω στοιχεία:

- Τον αριθμό των χρηστών της βάσης δεδομένων της εφαρμογής.

- Την τιμή της συγκεκριμένης μεταβλητής.
- Τον αριθμό των χρηστών με την ίδια τιμή στην ίδια μεταβλητή.
- Την πιθανότητα επίθεσης στην συγκεκριμένη μεταβλητή (σε ποσοστό τις %).

Τέλος, δίνεται η δυνατότητα στον χρήστη να εκτυπώσει ή να κατεβάσει την αναφορά της συγκεκριμένης μεταβλητής με τα αντίστοιχα αποτελέσματα.

3.2.5 Αναφορά (Report)

Όπως αναφέρθηκε και παραπάνω, έπειτα από την εμφάνιση των αποτελεσμάτων ο χρήστης έχει την δυνατότητα να εκτυπώσει ή να κατεβάσει την αναφορά της συγκεκριμένης μεταβλητής με τα αντίστοιχα αποτελέσματα. Εκτός από τα αποτελέσματα που εμφανίζονται στον χρήστη στην σελίδα Αποτελεσμάτων, στην αναφορά εμφανίζονται τα στοιχεία του χρήστη που είναι αποθηκευμένα στην βάση δεδομένων της εφαρμογής και παρουσιάζονται παρακάτω:

- Ο αριθμός χρήστη (id)
- Το όνομα (name)
- Το επώνυμο (surname)
- Το όνομα χρήστη (username)
- Ο κωδικός (password)
- Η διεύθυνση (address)
- Ο ταχυδρομικός κώδικας (postal code)
- Η πόλη (city)
- Η χώρα (country)

Τέλος, όσον αφορά την αποθήκευση της αναφοράς ο χρήστης μπορεί να επιλέξει ανάμεσα σε ένα πλήθος τύπου αρχείων, οι οποίοι αναφέρονται παρακάτω:

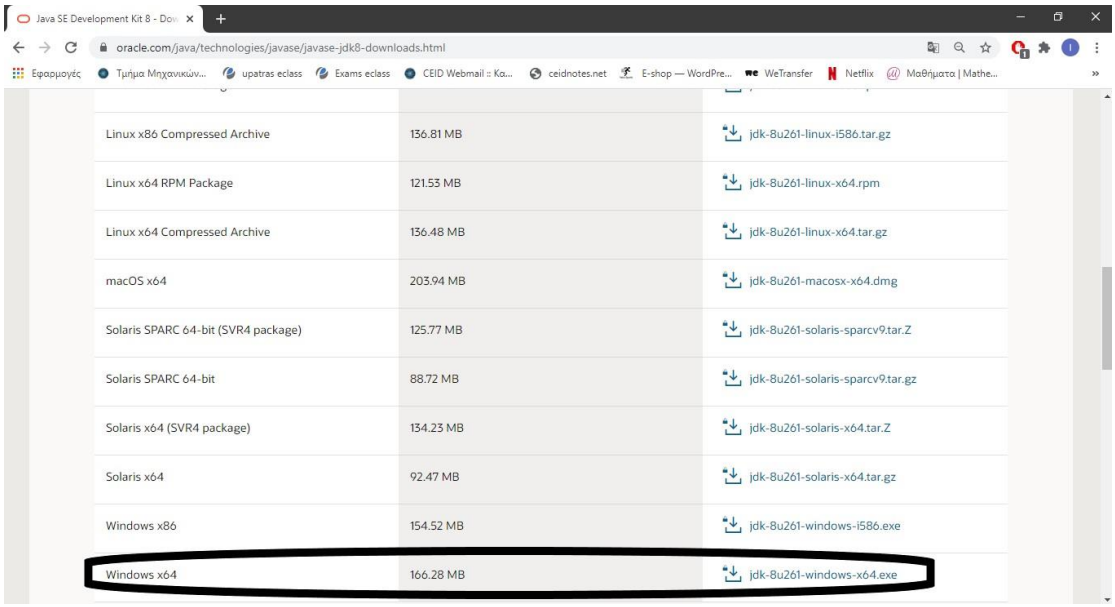
- JasperReports
- PDF
- RTF
- ODT
- DOCX
- HTML
- Single sheet XLS
- Multiple sheet XLS

Κεφάλαιο 4: Υλοποίηση IB Privacy Advisor App

Στο κεφάλαιο αυτό αναφέρονται οι οδηγίες και παρουσιάζονται κατάλληλα screenshots για την επιτυχή εγκατάσταση της εφαρμογής, παρουσιάζεται το UML διάγραμμα των κλάσεων της εφαρμογής, οι απαραίτητες ενέργειες για την σωστή εγκατάσταση της εφαρμογής στο Apache Netbeans IDE, ο κώδικας της βάσης δεδομένων, οι αντίστοιχες ρυθμίσεις για τον τοπικό server (localhost server), το format της αυτοματοποιημένης αναφοράς (i-Report) καθώς και οι βιβλιοθήκες της και τέλος sample tests της εφαρμογής.

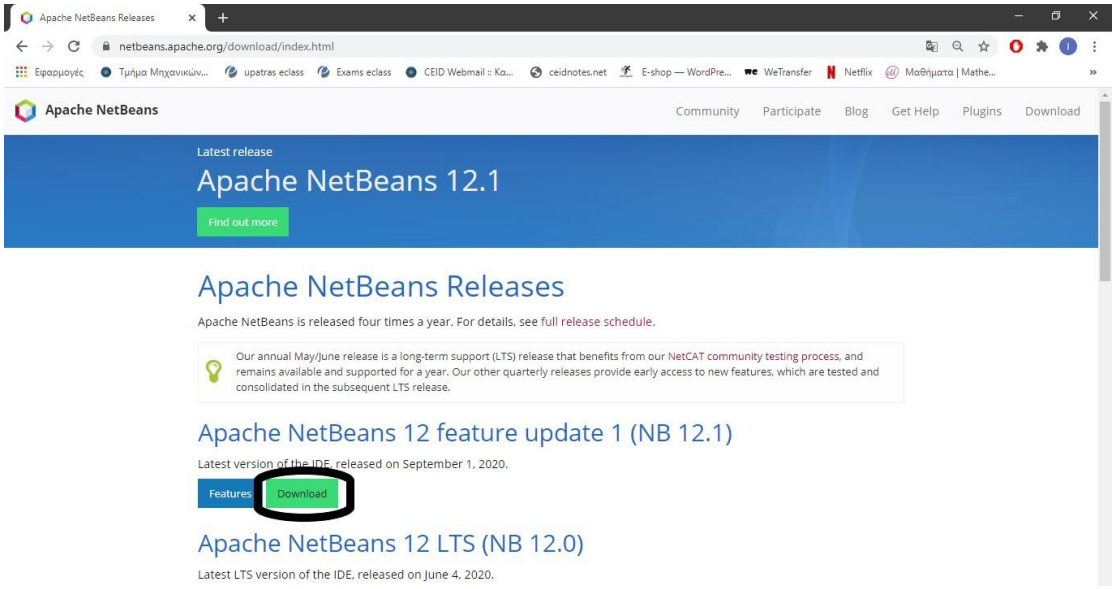
4.1 Εγκατάσταση

Αρχικά για την επιτυχημένη εγκατάσταση της εφαρμογής χρειάζεται να κατεβάσουμε το Java Development Kit (Java JDK 8+).



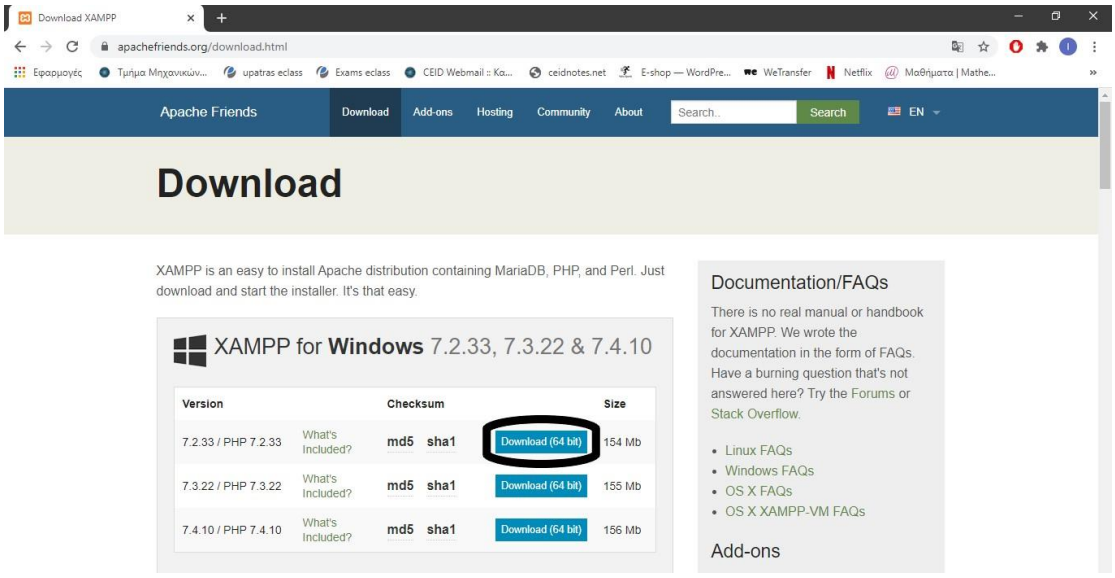
Εικόνα 4.1.1 Java Development Kit 8+

Δεύτερων, κατεβάζουμε το Apache Netbeans IDE (Apache Netbeans IDE 11+).



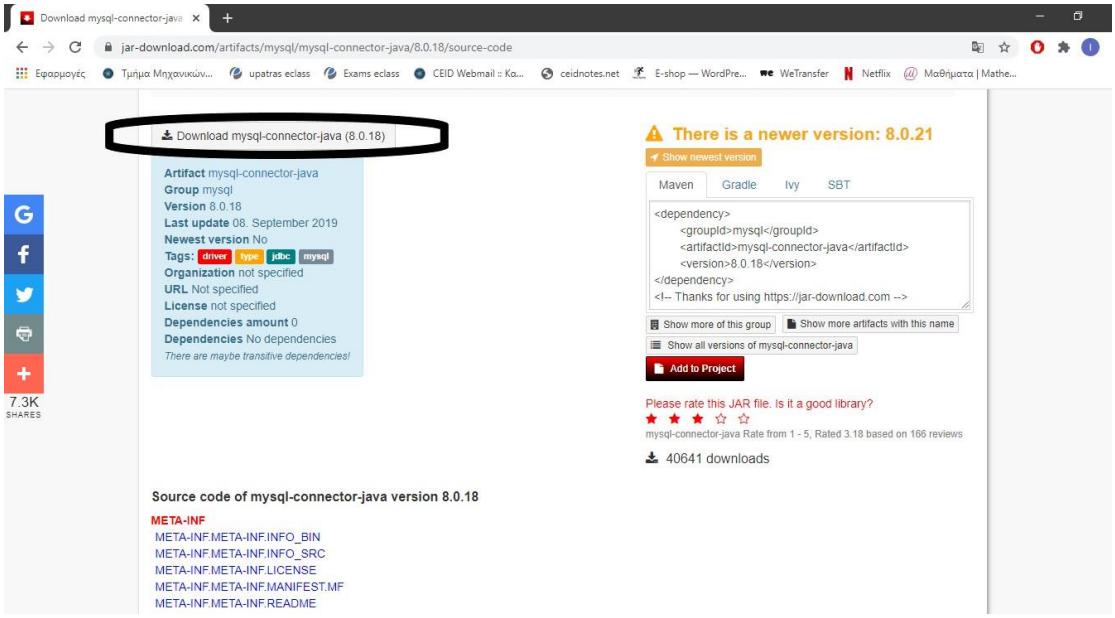
Εικόνα 4.1.2 Apache Netbeans IDE

Τρίτων, κατεβάζουμε το Xampp (xampp v3.2.4+).



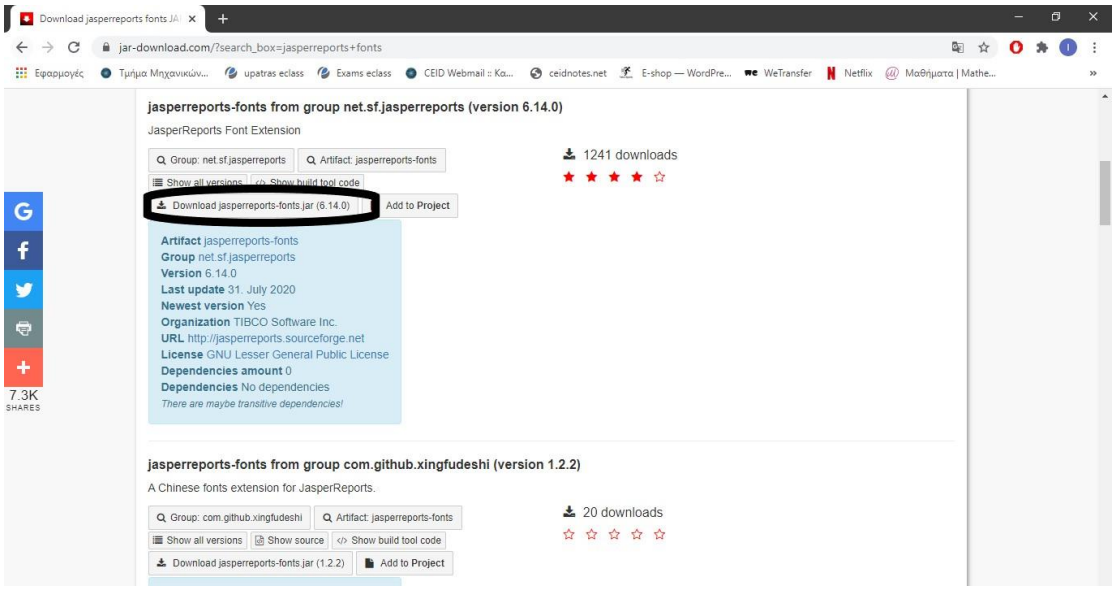
Εικόνα 4.1.3 Xampp

Τέταρτων, κατεβάζουμε το [mysql-connector- java] (mysql-connector- java-8.0.18 +)



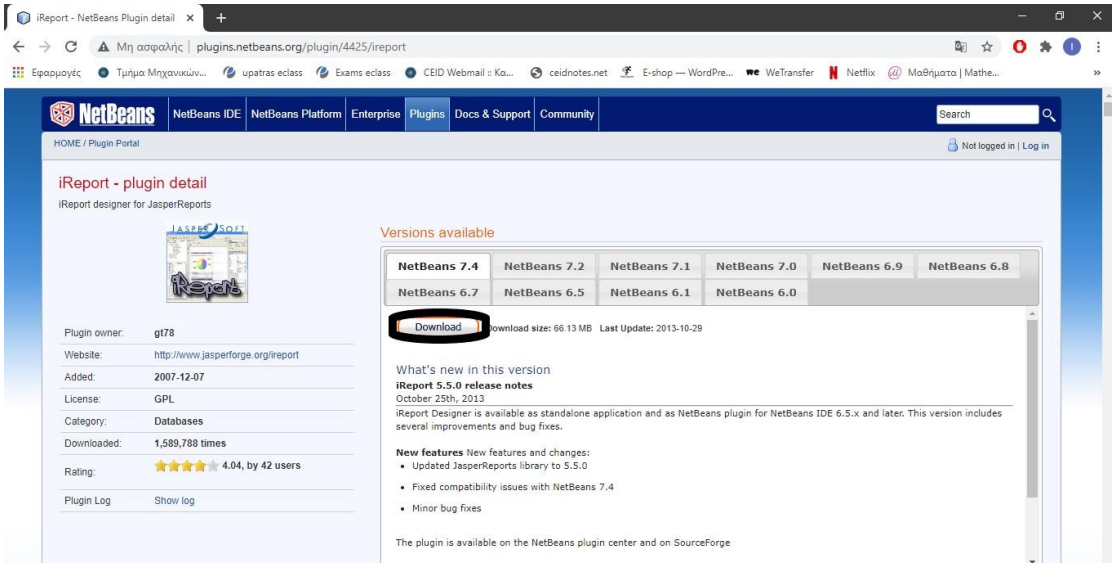
Εικόνα 4.1.4 mysql-connector- java

Πέμπτων, κατεβάζουμε το [JasperReportsLibrary] (jasperreports-fonts-6.14.0)



Εικόνα 4.1.5 JasperReportsLibrary

Τέλος, κατεβάζουμε το iReport Plugin (iReport-5.6.0-plugin)



Εικόνα 4.1.6 iReport Plugin

4.2 UML Διάγραμμα

Το UML διάγραμμα είναι ένα διάγραμμα που χρησιμοποιείται στις αντικειμενοστραφείς γλώσσες προγραμματισμού, κυρίως από την Java, και δείχνει της συσχετίσεις μεταξύ των κλάσεων καθώς και τις μεταβλητές και τις μεθόδους κάθε κλάσης.

Για την υλοποίηση της εφαρμογής δημιουργήθηκαν οχτώ(8) κλάσεις, οι οποίες παρουσιάζονται παρακάτω.

- HomePage(): Στην παρούσα κλάση παρουσιάζεται η αρχική σελίδα της εφαρμογής.

- DatabasePage(): Στην παρούσα κλάση παρουσιάζεται η σελίδα για την προσθήκη της βάσης δεδομένων της εφαρμογής, ο χρήστης προσθέτει το όνομα της βάσης δεδομένων που έχει προσθέσει μέσω xampp στο localhost.

- LoginPage(): Στην παρούσα κλάση παρουσιάζεται η σελίδα σύνδεσης της εφαρμογής, ο χρήστης συνδέεται στο σύστημα της εφαρμογής μέσω username και password.

- SignUpPage(): Στην παρούσα κλάση παρουσιάζεται η σελίδα δημιουργίας λογαριασμού, ο χρήστης δημιουργεί λογαριασμό στο σύστημα της εφαρμογής εφόσον δεν έχει και ανακατευθύνεται στην σελίδα σύνδεσης της εφαρμογής.

- UserPage(): Στην παρούσα κλάση παρουσιάζεται η σελίδα χρήστη, ο χρήστης επιλέγει την μεταβλητή, στην οποία θέλει να μάθει την πιθανότητα επίθεσης σε αυτή και γίνεται εμφάνιση της πιθανότητας καθώς και σε ποια κατηγορία ρίσκου ανήκει, δηλαδή μικρό, μεσαίο ή μεγάλο ρίσκο.

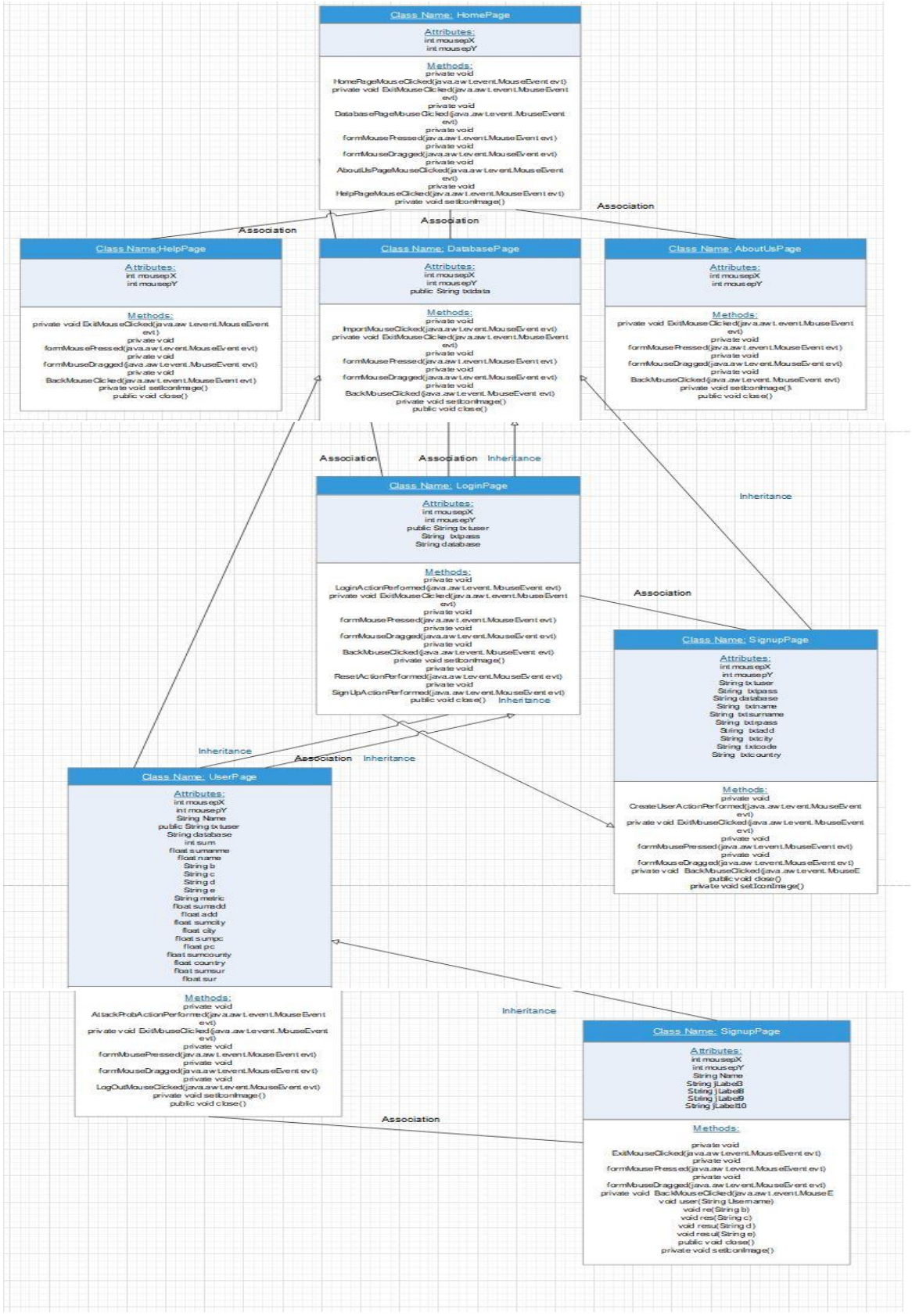
- ResultPage(): Στην παρούσα κλάση παρουσιάζεται η σελίδα αποτελεσμάτων, στην οθόνη εμφανίζονται όλα τα απαραίτητα στοιχεία από την πιθανότητα επίθεσης στην μεταβλητή που έχει επιλέξει ο χρήστης. Επίσης, δίνεται η δυνατότητα στον χρήστη να εκτυπώσει ή να κατεβάσει την αναφορά με όλα τα αποτελέσματα καθώς και τα στοιχεία του από τον υπολογισμό της πιθανότητας επίθεσης πάνω στην αντίστοιχη μεταβλητή.

- HelpPage(): Στην παρούσα κλάση παρουσιάζεται η σελίδα βοήθειας, εδώ παρουσιάζονται όλες οι απαραίτητες οδηγίες στον χρήστη για την επιτυχή χρήση της εφαρμογής.

- AboutUsPage(): Στην παρούσα κλάση παρουσιάζεται η σελίδα σχετικά με εμάς, εδώ παρουσιάζονται όλες οι απαραίτητες πληροφορίες για την λειτουργικότητα καθώς και τον σκοπό της εφαρμογής που δημιουργήθηκε.

Επιπλέον, είναι σημαντικό να αναφερθεί η χρήση του αρχείου *report1.jrxml*, στο οποίο έγινε η σχεδίαση της αναφοράς με χρήση στατικών και δυναμικών μεταβλητών καθώς χρησιμοποιείται και η βάση δεδομένων για την χρήση των προσωπικών δεδομένων του χρήστη.

Τέλος, παρουσιάζεται παρακάτω με μορφή εικόνας το UML διάγραμμα των κλάσεων της εφαρμογής, το οποίο κατασκευάστηκε μέσω του λογισμικού EdrawMax.



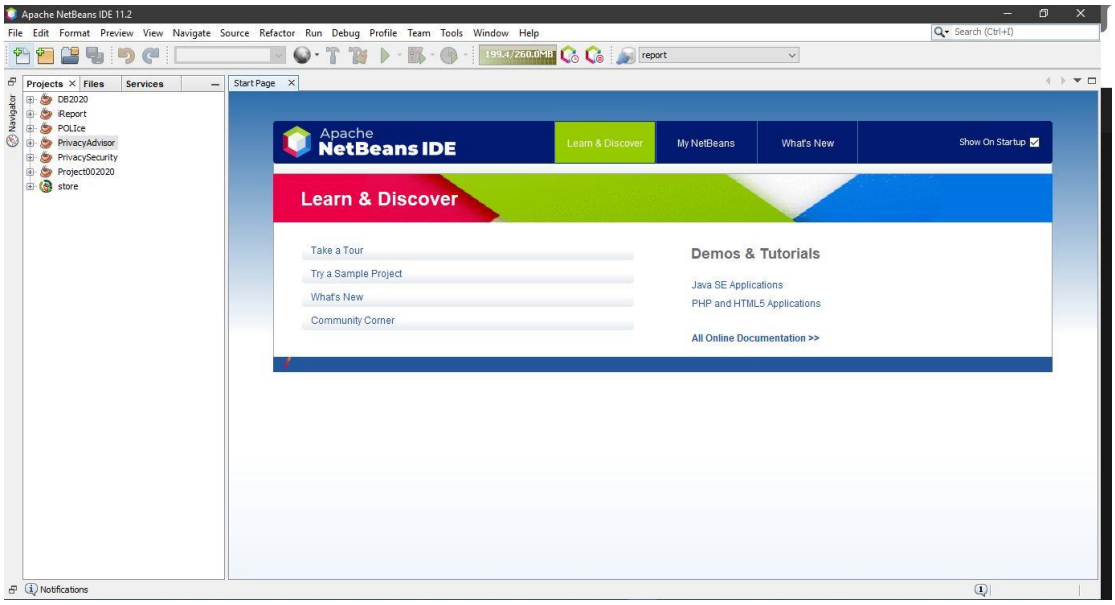
Εικόνα 4.2.1 UML διάγραμμα της εφαρμογής IB Privacy Advisor App.

4.3 Apache Netbeans IDE

Όπως παρουσιάστηκε και παραπάνω το Apache Netbeans IDE είναι ένα προγραμματιστικό περιβάλλον που χρησιμοποιείται από την γλώσσα προγραμματισμού Java για την ανάπτυξη εφαρμογών διεπαφών χρήστη (GUI).

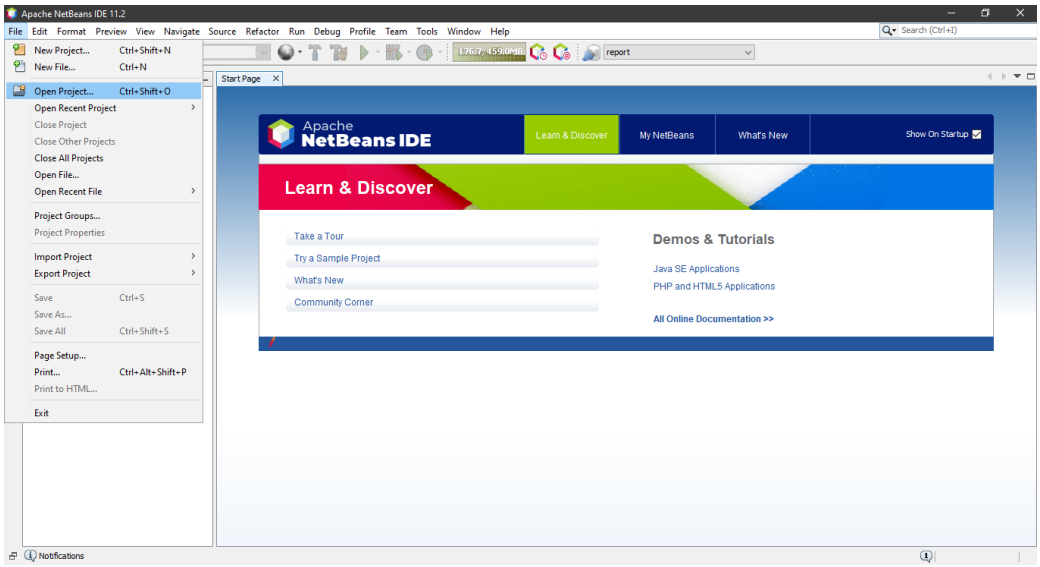
Στο παρόν υπο-κεφάλαιο, θα παρουσιαστούν τα απαραίτητα βήματα ώστε να γίνει ορθή χρήση της για την επιτυχή εκτέλεση της εφαρμογής.

Αρχικά, έχοντας κατεβάσει το Apache Netbeans IDE βρισκόμαστε στην αρχική σελίδα της εφαρμογής.



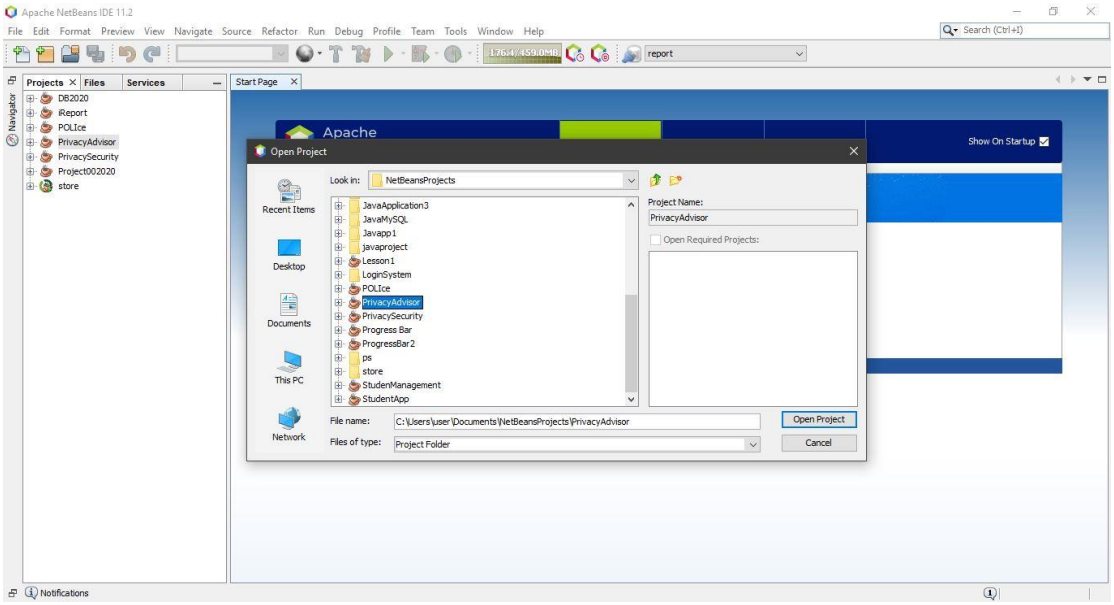
Εικόνα 4.3.1 Αρχική Σελίδα Netbeans

Στην συνέχεια επιλέγουμε από την γραμμή εργαλείων την επιλογή *File* και έπειτα την επιλογή *Open Project.*



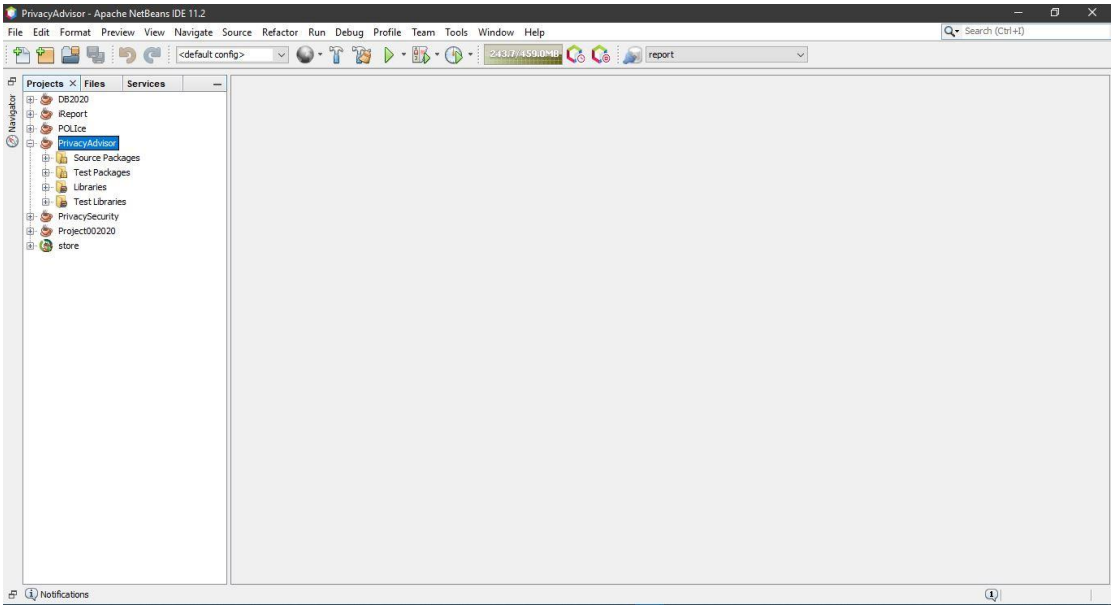
Εικόνα 4.3.2 Netbeans Open Project

Έπειτα, μεταφερόμαστε στον default φάκελο που αποθηκεύονται τα Netbeans Projects (C:\Users\user\Documents\NetBeansProjects) και επιλέγουμε το project που θέλουμε να τρέξουμε. Είναι σημαντικό να αναφερθεί ότι για να τρέξει το Apache Netbeans IDE κάποιο project πρέπει αποκλειστικά να βρίσκεται στο παραπάνω Directory.



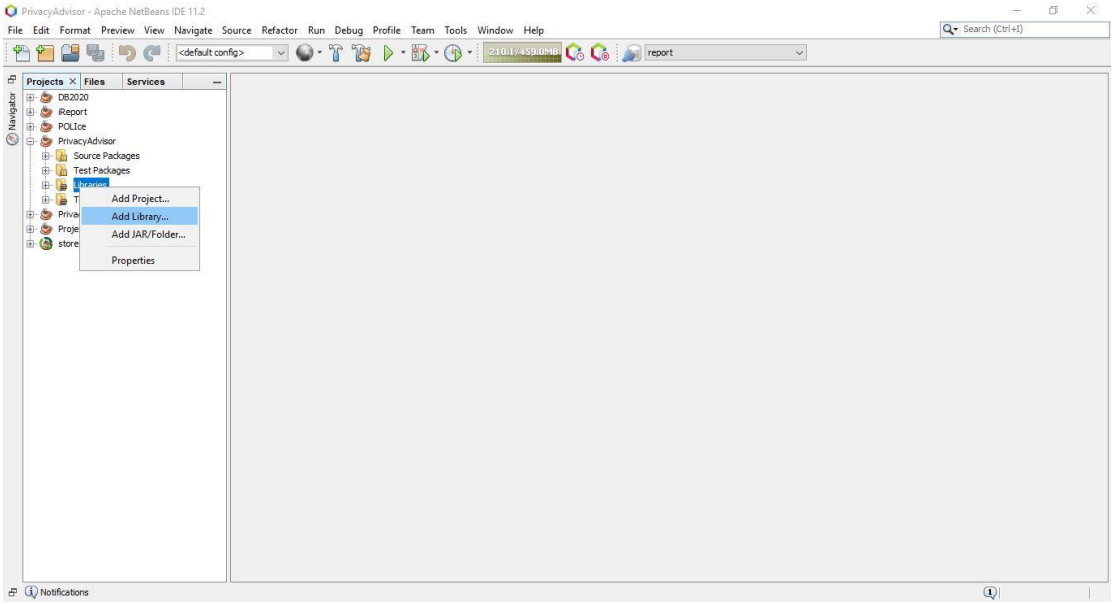
Εικόνα 4.3.3 Επιλογή project από το directory του Apache Netbeans IDE.

Μετά, παρουσιάζονται τα περιεχόμενα της εφαρμογής που κάναμε import στο Apache Netbeans IDE.

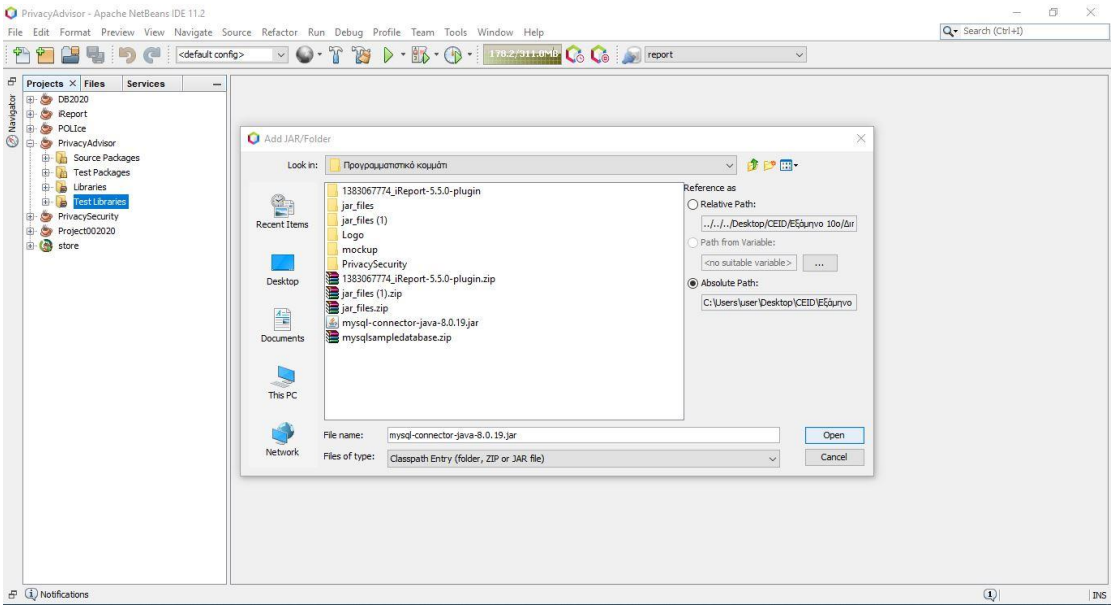


Εικόνα 4.3.4 Περιεχόμενα εφαρμογής που κάναμε import στο Apache Netbeans IDE.

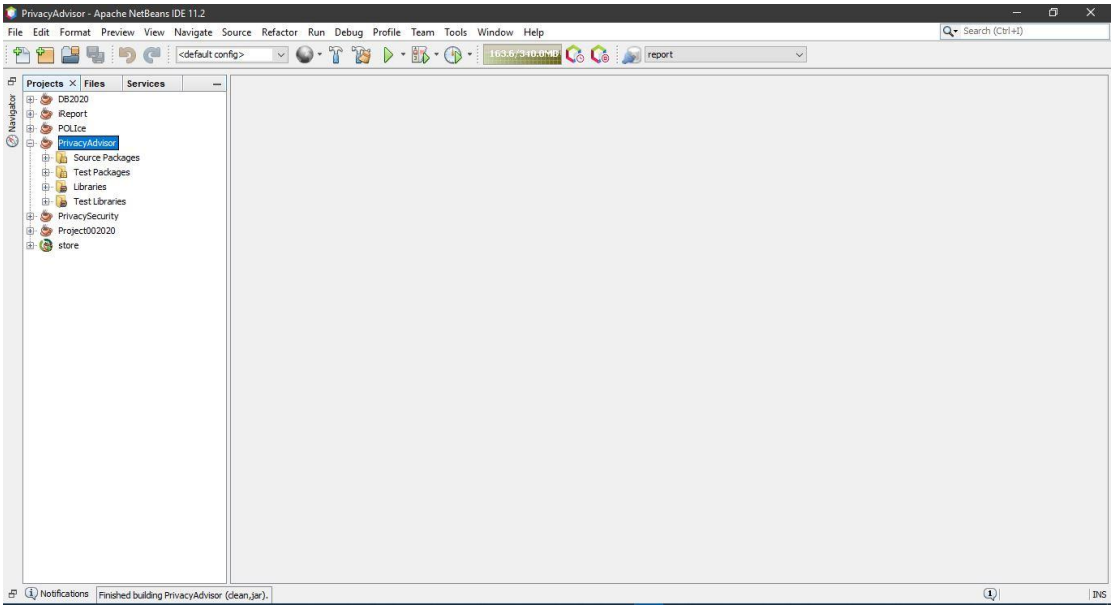
Τέλος, προσθέτουμε τις βιβλιοθήκες (jar files), κάνουμε *build and clean* και μετά *run*.



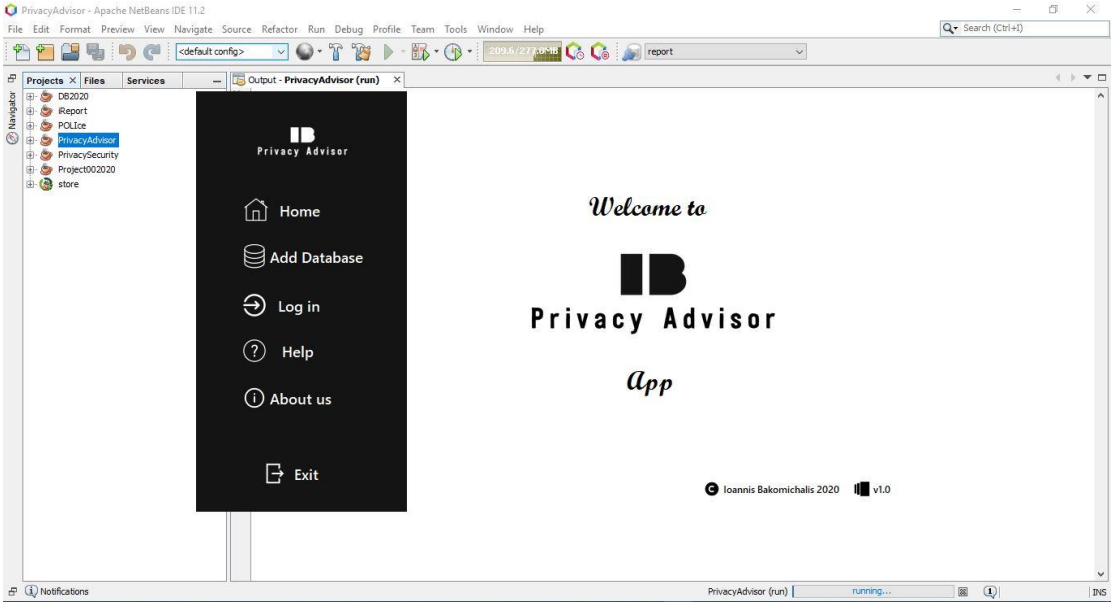
Εικόνα 4.3.5 Προσθήκη βιβλιοθήκης στην εφαρμογή.



Εικόνα 4.3.6 Προσθήκη mysql-connector-java-8.0.18 library.



Εικόνα 4.3.7 Clean and Build στην εφαρμογή.



Εικόνα 4.3.8 Run της εφαρμογής.

4.4 Βάση Δεδομένων (Database)

Η βάση δεδομένων αποτελεί το πιο σημαντικό στοιχείο μετά τον κώδικα της εφαρμογής για την ορθή και αποδοτική λειτουργία της. Είναι το κομβικό της σημείο, καθώς μέσω αυτής αποθηκεύονται τα προσωπικά δεδομένα του χρήστη, επιλέγεται η κατάλληλη μεταβλητή (attribute) από τον χρήστη και τέλος υπολογίζεται η πιθανότητα επίθεσης στην συγκεκριμένη μεταβλητή.

4.4.1 Κώδικας SQL

Η βάση δεδομένων της εφαρμογής αποτελείται από έναν πίνακα(table) με στοιχεία(fields):

Όνομα Πίνακα(table): *customers*

- Αριθμός Χρήστη(*customerid*): Ο αριθμός χρήστη της εφαρμογής.
- Όνομα(*customerName*): Το μικρό όνομα του χρήστη.
- Επίθετο(*customerSurname*): Το επώνυμο του χρήστη.
- Όνομα Χρήστη(*username*): Το username του χρήστη για σύνδεση στην εφαρμογή.
- Κωδικός(*password*): Το password του χρήστη για σύνδεση στην εφαρμογή.
- Διεύθυνση(*address*): Η διεύθυνση κατοικίας του χρήστη.
- Ταχυδρομικός Κώδικας(*postalCode*): Ο ταχυδρομικός κώδικας κατοικίας του χρήστη.
- Πόλη(*city*): Η πόλη κατοικίας του χρήστη.
- Χώρα(*country*): Η χώρα κατοικίας του χρήστη.

Είναι σημαντικό η βάση δεδομένων να περιέχει τον πίνακα *customers* με τα παραπάνω fields ανεξαρτήτου ονόματος της βάσης δεδομένων για την επιτυχή και ορθή εκτέλεση της εφαρμογής. Παρακάτω παρουσιάζεται ο κώδικας SQL της βάσης δεδομένων της εφαρμογής:

```sql
-- phpMyAdmin SQL Dump
-- version 4.9.0.1
-- https://www.phpmyadmin.net/
--
-- Φιλοξενητής: 127.0.0.1
-- Χρόνος δημιουργίας: 01 Οκτ 2020 στις 23:20:20
-- Έκδοση διακομιστή: 10.4.6-MariaDB
-- Έκδοση PHP: 7.1.31

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET AUTOCOMMIT = 0;
START TRANSACTION;
SET time_zone = "+00:00";


/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;

--
-- Βάση δεδομένων: `privacy`
--

-- --------------------------------------------------------

--
-- Δομή πίνακα για τον πίνακα `customers`
--

CREATE TABLE `customers` (
  `customerid` int(255) NOT NULL,
  `customerName` varchar(50) NOT NULL,
  `customerSurname` varchar(255) NOT NULL,
  `username` varchar(50) NOT NULL,
  `password` varchar(50) NOT NULL,
  `address` varchar(50) NOT NULL,
  `city` varchar(50) NOT NULL,
  `postalCode` int(255) NOT NULL,
  `country` varchar(50) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Άδειασμα δεδομένων του πίνακα `customers`
```

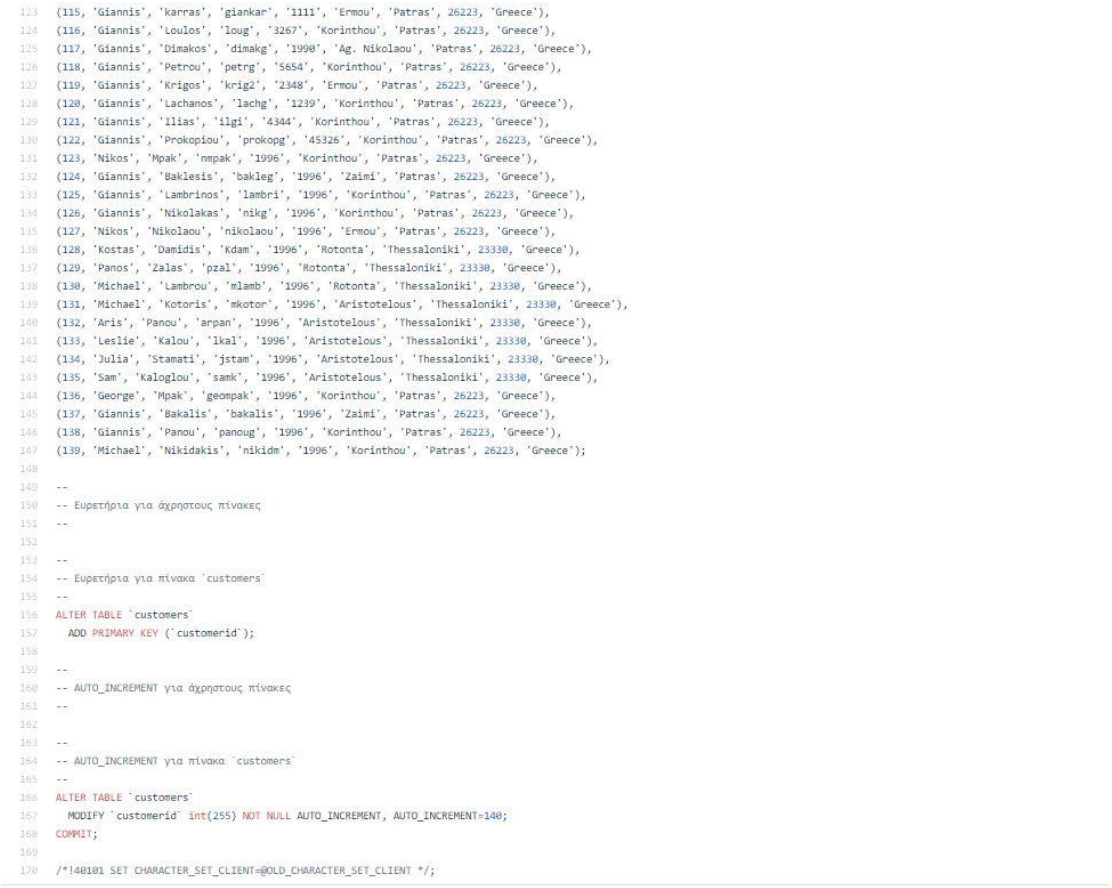
Εικόνα 4.4.1.1 Κώδικας SQL 1ο Μέρος.

```
--

INSERT INTO `customers` (`customerid`, `customerName`, `customerSurname`, `username`, `password`, `address`, `city`, `postalCode`, `country`) VALUES
(1, 'Giannis', 'Mpak', 'mpak', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(2, 'Giannis', 'Bakopoulos', 'bak', '1996', 'Zaimi', 'Patras', 26223, 'Greece'),
(3, 'Giannis', 'Papadopoulos', 'pap', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(4, 'Giannis', 'Nikolaou', 'nik', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(5, 'Nikos', 'Kalos', 'nkal', '1996', 'Ermou', 'Patras', 26203, 'Greece'),
(7, 'Kelvin', 'Leong', 'Kelvin', '1996', '7586 Pompton St.', 'Allentown', 70267, 'USA'),
(14, 'Valarie', 'Franco', 'Braun', '1996', '6251 Ingle Ln.', 'Boston', 51003, 'USA'),
(15, 'Juri', 'Yoshido', 'Juri', '1996', '8616 Spinnaker Dr.', 'Boston', 51003, 'USA'),
(17, 'Miguel', 'Barajas', 'Miguel', '1996', '7635 Spinnaker Dr.', 'Brickhaven', 58339, 'USA'),
(18, 'Allen', 'Nelson', 'Allen', '1996', '7825 Douglas Av.', 'Brickhaven', 58339, 'USA'),
(19, 'Leslie', 'Taylor', 'Leslie', '1996', '16780 Pompton St.', 'Brickhaven', 58339, 'USA'),
(20, 'Julie', 'King', 'Julie', '1996', '25593 South Bay Ln.', 'Bridgewater', 97562, 'USA'),
(21, 'Sue', 'Taylor', 'Sue', '1996', '2793 Furth Circle', 'Brisbane', 94217, 'USA'),
(23, 'Martha', 'Nelou', 'marthn', '1996', 'Ermou', 'Patras', 26223, 'Greece'),
(24, 'Steve', 'Thompson', 'Steve', '1996', '3675 Furth Circle', 'Burbank', 94019, 'USA'),
(25, 'Juri', 'Hashimoto', 'Juri', '1996', '9408 Furth Circle', 'Burlingame', 94217, 'USA'),
(26, 'Marta', 'Hernandez', 'Marta', '1996', '39323 Spinnaker Dr.', 'Cambridge', 51247, 'USA'),
(27, 'Jerry', 'Tseng', 'Jerry', '1996', '4658 Baden Av.', 'Cambridge', 51247, 'USA'),
(28, 'Mike', 'Gao', 'Mike', '1996', 'Bank of China Tower', 'Central Hong Kong', 34567, 'Hong Kong'),
(30, 'Adrian', 'Huxley', 'Adrian', '1996', 'Monitor Money Building', 'Chatswood', 2067, 'Australia'),
(31, 'Helen', 'Bennett', 'Helen', '1996', 'Garden House', 'Liverpool', 56434, 'UK'),
(34, 'Kalle', 'Suominen', 'Kalle', '1996', 'Kaln 23', 'Espoo', 23421, 'Finland'),
(39, 'Sean', 'Clenahan', 'Sean', '1996', '7 Allen Street', 'Glen Waverly', 3150, 'Australia'),
(40, 'Dan', 'Lewis', 'Dan', '1996', '2440 Pompton St.', 'Glendale', 97561, 'USA'),
(41, 'Mary', 'Young', 'Mary', '1996', '4097 Douglas Av.', 'Glendale', 92561, 'USA'),
(44, 'Matti', 'Karttunen', 'Matti', '1996', 'Keskuskatu 45', 'Helsinki', 21240, 'Finland'),
(45, 'Irini', 'Tsolka', 'irts', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(47, 'Jytte', 'Petersen', 'Jytte', '1996', 'Vinbæltet 34', 'Kobenhavn', 1734, 'Denmark'),
(49, 'Jean', 'King', 'Jean', '1996', '8489 Strong St.', 'Las Vegas', 83030, 'USA'),
(51, 'Martine', 'Rancé', 'Martine', '1996', '184, chaussée de Tournai', 'Lille', 59000, 'France'),
(52, 'Isabel', 'de Castro', 'Isabel', '1996', 'Estrada da saúde n. 58', 'Lisboa', 1756, 'Portugal'),
(53, 'Lino', 'Rodriguez', 'Lino', '1996', 'Jardim das rosas n. 32', 'Lisboa', 1675, 'Portugal'),
(54, 'Elizabeth', 'Devon', 'Elizabeth', '1996', '12, Berkeley Gardens Blvd', 'Liverpool', 56434, 'UK'),
(55, 'Ann', 'Brown', 'Ann', '1996', '35 King George', 'London', 76589, 'UK'),
(56, 'Thomas', 'Smith', 'Thomas', '1996', '120 Hanover Sq.', 'London', 76589, 'UK'),
(57, 'Brian', 'Chandler', 'Brian', '1996', '6047 Douglas Av.', 'Los Angeles', 91003, 'USA'),
(58, 'Christina', 'Berglund', 'Christina', '1996', 'Berguvsvägen  8', 'Luleå', 34256, 'Sweden'),
(59, 'Mary', 'Saveley', 'Mary', '1996', '2, rue du Commerce', 'Lyon', 69004, 'France'),
(65, 'Nikos', 'Kravas', 'nkrav', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(66, 'Rachel', 'Ashworth', 'Rachel', '1996', 'Fauntleroy Circus', 'Manchester', 76858, 'UK'),
(67, 'Hanna', 'Moos', 'Hanna', '1996', 'Forsterstr. 57', 'Mannheim', 68306, 'Germany'),
(68, 'Laurence', 'Lebihan', 'Laurence', '1996', '12, rue des Bouchers', 'Marseille', 13008, 'France'),
```

Εικόνα 4.4.1.2 Κώδικας SQL 2ο Μέρος.

```
(69, 'Petros', 'Balos', 'PeterB', '1996', 'Ag. Nikolaou', 'Patras', 26223, 'Greece'),
(71, 'Jim', 'Fragos', 'jimf', '1996', 'Zaimi', 'Patras', 26223, 'Greece'),
(76, 'Carine', 'Schmitt', 'Carine', '1996', '54, rue Royale', 'Nantes', 44000, 'France'),
(77, 'Dorothy', 'Young', 'Dorothy', '1996', '2304 Long Airport Avenue', 'Nashua', 62005, 'USA'),
(78, 'Violeta', 'Benitez', 'Violeta', '1996', '1785 First Street', 'New Bedford', 50553, 'USA'),
(79, 'Wing', 'Huang', 'Wing', '1996', '4575 Hillside Dr.', 'New Bedford', 50553, 'USA'),
(80, 'Keith', 'Franco', 'Keith', '1996', '149 Spinnaker Dr.', 'New Haven', 97823, 'USA'),
(81, 'Leslie', 'Murphy', 'Leslie', '1996', '567 North Pendale Street', 'New Haven', 97823, 'USA'),
(82, 'William', 'Brown', 'William', '1996', '7476 Moss Rd.', 'Newark', 94019, 'USA'),
(83, 'Anna', 'Hara', 'Anna', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(84, 'Yu', 'Choi', 'Yu', '1996', '5290 North Pendale Street', 'NYC', 10022, 'USA'),
(85, 'Michael', 'Frick', 'Michael', '1996', '2678 Kingston Rd.', 'NYC', 10022, 'USA'),
(86, 'Maria', 'Hernandez', 'Maria', '1996', '5905 Pompton St.', 'NYC', 10022, 'USA'),
(87, 'Kwai', 'Lee', 'Kwai', '1996', '897 Long Airport Avenue', 'NYC', 10022, 'USA'),
(88, 'Jeff', 'Young', 'Jeff', '1996', '4092 Furth Circle', 'NYC', 10022, 'USA'),
(90, 'Pirkko', 'Koskitalo', 'Pirkko', '1996', 'Ermou', 'Patras', 26223, 'Greece'),
(91, 'Marie', 'Bertrand', 'Marie', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(92, 'Daniel', 'Da Silva', 'Daniel', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(94, 'Michael', 'Leong', 'LeoM', '1996', '7586 Pompton St.', 'Allentown', 70267, 'USA'),
(101, 'Nick', 'Franco', 'nfra', '1996', '6251 Ingle Ln.', 'Boston', 51003, 'USA'),
(102, 'Jo', 'Yoshido', 'jyosh', '1996', '8616 Spinnaker Dr.', 'Boston', 51003, 'USA'),
(103, 'Nikos', 'Balaskas', 'baln', '1996', 'Zaimi', 'Patras', 26223, 'Greece'),
(104, 'Petros', 'Diakos', 'diakp', '1996', 'Tsakalof', 'Athens', 31108, 'Greece'),
(105, 'Kostas', 'Damianis', 'kdam', '1996', 'Tsakalof', 'Athens', 31108, 'Greece'),
(106, 'Ilias', 'Katopodis', 'ikat', '1996', 'Tsakalof', 'Athens', 31108, 'Greece'),
(107, 'Manolis', 'Maragkos', 'marm', '1996', 'Tsakalof', 'Athens', 31108, 'Greece'),
(108, 'Giorgos', 'Arvas', 'garva', '1996', 'Olgas', 'Athens', 31108, 'Greece'),
(109, 'Panos', 'Diakos', 'adiak', '1996', 'Olgas', 'Athens', 31108, 'Greece'),
(110, 'Manos', 'Arvas', 'marva', '1996', 'Olgas', 'Athens', 31108, 'Greece'),
(111, 'Antonis', 'Kalas', 'antk', '1996', 'Olgas', 'Athens', 31108, 'Greece'),
(112, 'George', 'Moras', 'gmoras', '1998', 'Ermou', 'Patras', 26223, 'Greece'),
(113, 'Giannis', 'Kalivas', 'kalg', '2349', 'Korinthou', 'Patras', 26223, 'Greece'),
(114, 'Giannis', 'Papanikolaou', 'papag', '2323', 'Ag. Nikolaou', 'Patras', 26223, 'Greece'),
(115, 'Giannis', 'karras', 'giankar', '1111', 'Ermou', 'Patras', 26223, 'Greece'),
(116, 'Giannis', 'Loulos', 'loug', '3267', 'Korinthou', 'Patras', 26223, 'Greece'),
(117, 'Giannis', 'Dimakos', 'dimakg', '1990', 'Ag. Nikolaou', 'Patras', 26223, 'Greece'),
(118, 'Giannis', 'Petrou', 'petrg', '5654', 'Korinthou', 'Patras', 26223, 'Greece'),
(119, 'Giannis', 'Krigos', 'krig2', '2348', 'Ermou', 'Patras', 26223, 'Greece'),
(120, 'Giannis', 'Lachanos', 'lachg', '1239', 'Korinthou', 'Patras', 26223, 'Greece'),
(121, 'Giannis', 'Ilias', 'ilgi', '4344', 'Korinthou', 'Patras', 26223, 'Greece'),
(122, 'Giannis', 'Prokopiou', 'prokopg', '45326', 'Korinthou', 'Patras', 26223, 'Greece');
```

Εικόνα 4.4.1.3 Κώδικας SQL 3ο Μέρος.



```
(115, 'Giannis', 'karras', 'giankar', '1111', 'Ermou', 'Patras', 26223, 'Greece'),
(116, 'Giannis', 'Loulos', 'loug', '3267', 'Korinthou', 'Patras', 26223, 'Greece'),
(117, 'Giannis', 'Dimakos', 'dimakg', '1990', 'Ag. Nikolaou', 'Patras', 26223, 'Greece'),
(118, 'Giannis', 'Petrou', 'petrg', '5654', 'Korinthou', 'Patras', 26223, 'Greece'),
(119, 'Giannis', 'Krigos', 'krig2', '2348', 'Ermou', 'Patras', 26223, 'Greece'),
(120, 'Giannis', 'Lachanos', 'lachg', '1239', 'Korinthou', 'Patras', 26223, 'Greece'),
(121, 'Giannis', 'Ilias', 'ilgi', '4344', 'Korinthou', 'Patras', 26223, 'Greece'),
(122, 'Giannis', 'Prokopiou', 'prokopg', '45326', 'Korinthou', 'Patras', 26223, 'Greece'),
(123, 'Nikos', 'Mpak', 'nmpak', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(124, 'Giannis', 'Baklesis', 'bakleg', '1996', 'Zaimi', 'Patras', 26223, 'Greece'),
(125, 'Giannis', 'Lambrinos', 'lambri', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(126, 'Giannis', 'Nikolakas', 'nikg', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(127, 'Nikos', 'Nikolaou', 'nikolaou', '1996', 'Ermou', 'Patras', 26223, 'Greece'),
(128, 'Kostas', 'Damidis', 'Kdam', '1996', 'Rotonta', 'Thessaloniki', 23330, 'Greece'),
(129, 'Panos', 'Zalas', 'pzal', '1996', 'Rotonta', 'Thessaloniki', 23330, 'Greece'),
(130, 'Michael', 'Lambrou', 'mlamb', '1996', 'Rotonta', 'Thessaloniki', 23330, 'Greece'),
(131, 'Michael', 'Kotoris', 'mkotor', '1996', 'Aristotelous', 'Thessaloniki', 23330, 'Greece'),
(132, 'Aris', 'Panou', 'arpan', '1996', 'Aristotelous', 'Thessaloniki', 23330, 'Greece'),
(133, 'Leslie', 'Kalou', 'lkal', '1996', 'Aristotelous', 'Thessaloniki', 23330, 'Greece'),
(134, 'Julia', 'Stamati', 'jstam', '1996', 'Aristotelous', 'Thessaloniki', 23330, 'Greece'),
(135, 'Sam', 'Kaloglou', 'samk', '1996', 'Aristotelous', 'Thessaloniki', 23330, 'Greece'),
(136, 'George', 'Mpak', 'geompak', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(137, 'Giannis', 'Bakalis', 'bakalis', '1996', 'Zaimi', 'Patras', 26223, 'Greece'),
(138, 'Giannis', 'Panou', 'panoug', '1996', 'Korinthou', 'Patras', 26223, 'Greece'),
(139, 'Michael', 'Nikidakis', 'nikidm', '1996', 'Korinthou', 'Patras', 26223, 'Greece');

--
-- Ευρετήρια για άχρηστους πίνακες
--

--
-- Ευρετήρια για πίνακα `customers`
--
ALTER TABLE `customers`
  ADD PRIMARY KEY (`customerid`);

--
-- AUTO_INCREMENT για άχρηστους πίνακες
--

--
-- AUTO_INCREMENT για πίνακα `customers`
--
ALTER TABLE `customers`
  MODIFY `customerid` int(255) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=140;
COMMIT;

/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
```

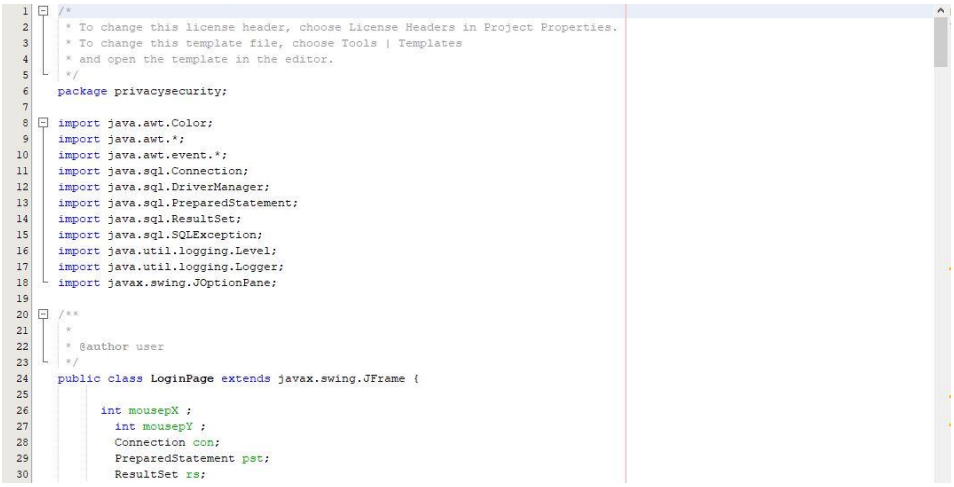
Εικόνα 4.4.1.4 Κώδικας SQL 4ο Μέρος.

Στον παραπάνω κώδικα SQL δημιουργείται η βάση δεδομένων της εφαρμογής δημιουργώντας έναν πίνακα *customers*(“CREATE TABLE”) με τα αντίστοιχα πεδία του και έπειτα δίνονται τιμές στα πεδία με την εντολή “INSERT INTO customers VALUES”.

4.4.2 Κώδικας σύνδεσης Apache Netbeans IDE με SQL

Εκτός από την συγγραφή του κώδικα της SQL και της βιβλιοθήκης mysql-connector-java-8.0.18 για την ορθή λειτουργία της εφαρμογής είναι απαραίτητη η συγγραφή κώδικα σε Java με την χρήση των κατάλληλων βιβλιοθηκών της Java για την σύνδεση του κώδικα της με την βάση δεδομένων. Ο απαιτούμενος κώδικας παρουσιάζεται παρακάτω:

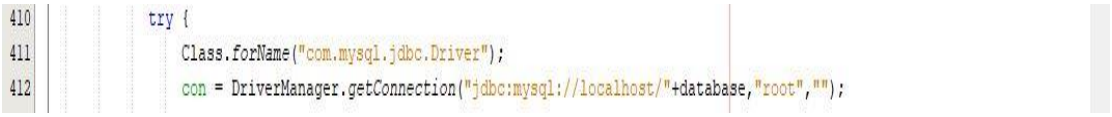
Αρχικά, η χρήση των κατάλληλων βιβλιοθηκών της Java.(*java.sql.Connection* και η μεταβλητή *Connection con*)



```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package privacysecurity;

import java.awt.Color;
import java.awt.*;
import java.awt.event.*;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.util.logging.Level;
import java.util.logging.Logger;
import javax.swing.JOptionPane;

/**
 *
 * @author user
 */
public class LoginPage extends javax.swing.JFrame {

        int mousepX ;
          int mousepY ;
          Connection con;
          PreparedStatement pst;
          ResultSet rs;
```

Εικόνα 4.4.2.1 Βιβλιοθήκες της Java για την σύνδεση με την βάση δεδομένων.

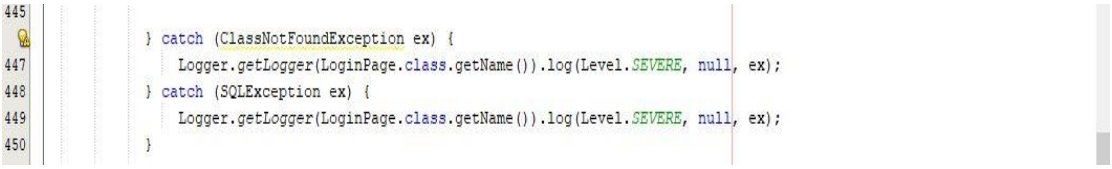
Έπειτα, η δημιουργία σύνδεσης με την βάση δεδομένων.



```
410         try {
411             Class.forName("com.mysql.jdbc.Driver");
412             con = DriverManager.getConnection("jdbc:mysql://localhost/"+database,"root","");
```

Εικόνα 4.4.2.2 Δημιουργία σύνδεσης Java με βάση δεδομένων.

Τέλος, η χρήση εξαιρέσεων (Exceptions) για την αποφυγή σφαλμάτων της σύνδεσης.



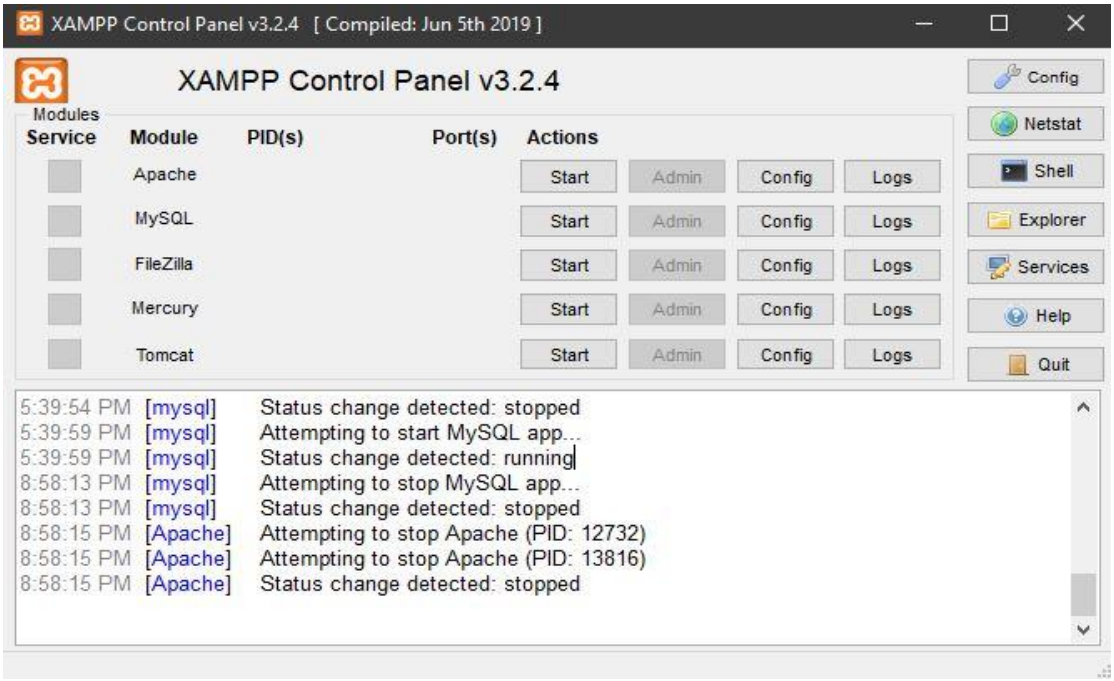
```
445
            } catch (ClassNotFoundException ex) {
447             Logger.getLogger(LoginPage.class.getName()).log(Level.SEVERE, null, ex);
448         } catch (SQLException ex) {
449             Logger.getLogger(LoginPage.class.getName()).log(Level.SEVERE, null, ex);
450         }
```

Εικόνα 4.4.2.3 Χρήση εξαιρέσεων (Exceptions).

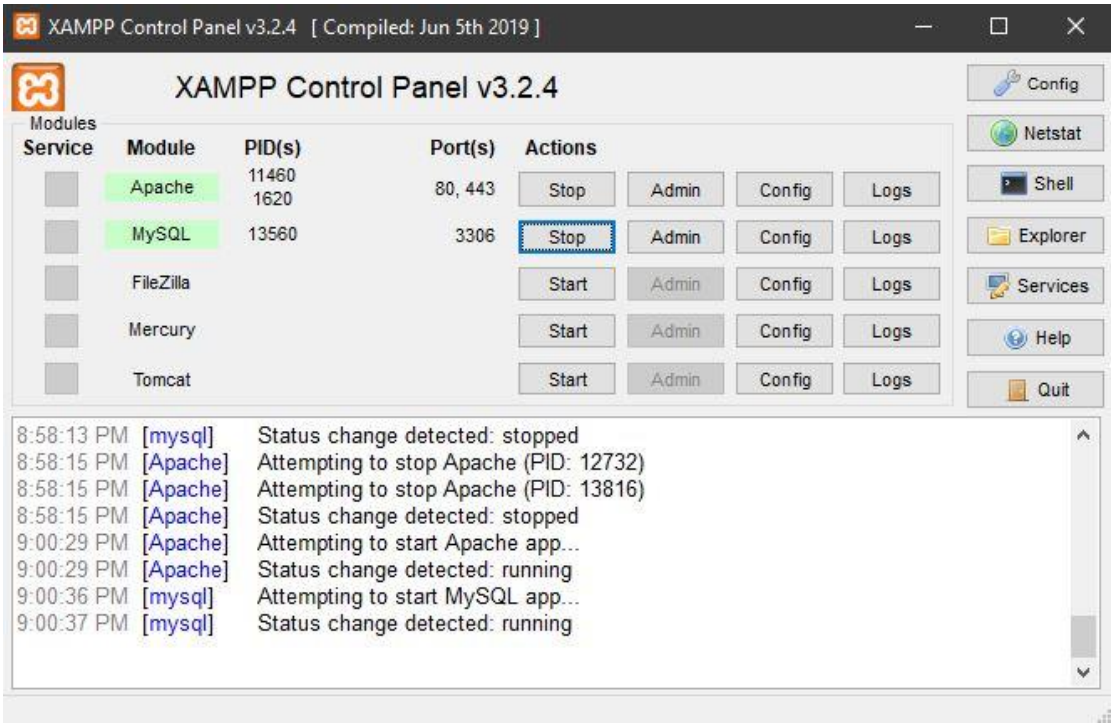
4.5 Τοπικός Server (Localhost Server)

Ο τοπικός server (Localhost server) βρίσκεται σε λειτουργία με την χρήση του xampp. Ο χρήστης με το άνοιγμα του Apache και της MySQL δίνει την δυνατότητα την αποθήκευση της βάσης δεδομένων του στον τοπικό server για την επιτυχή και ομαλή λειτουργία της εφαρμογής. Παρακάτω, παρουσιάζονται αναλυτικά τα απαραίτητα βήματα.

Αρχικά, ανοίγουμε το xampp και πατάμε *Start* στο Apache και στην MySQL.



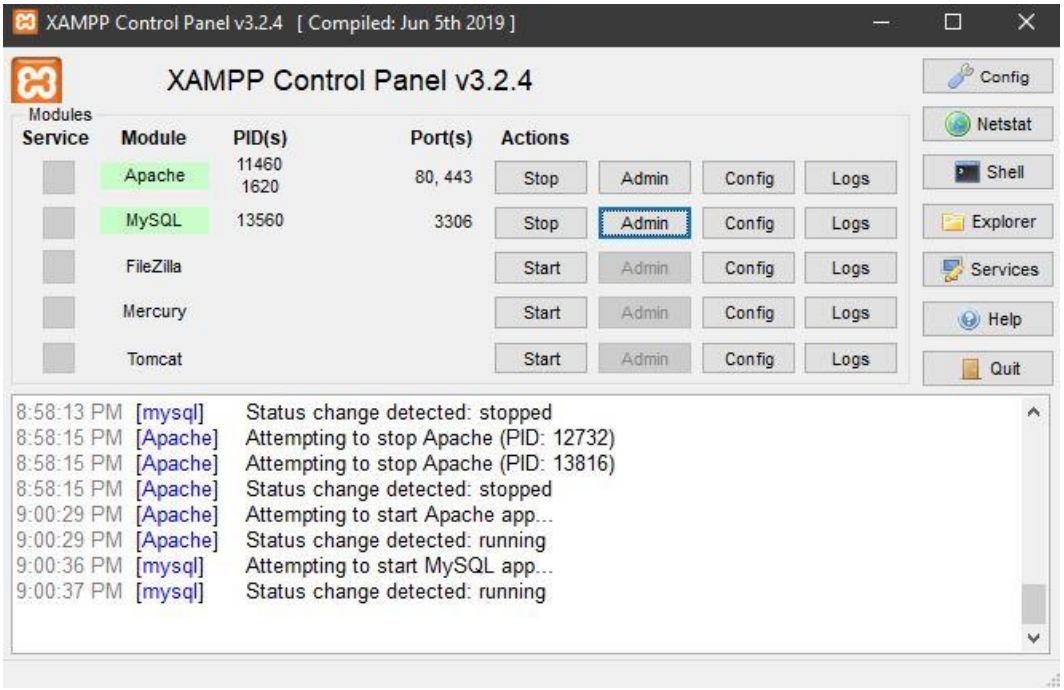
Εικόνα 4.5.1 Αρχική Οθόνη xampp.



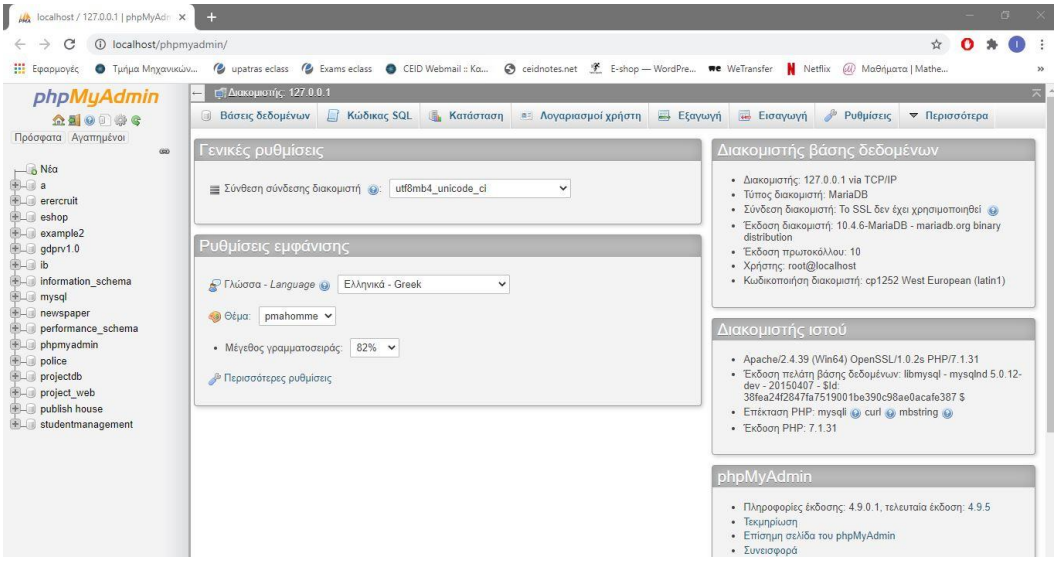
Εικόνα 4.5.2 Πατάμε *Start* στο Apache και την MySQL.

Είναι σημαντικό η MySQL να βρίσκεται στο *port:3306* για την ορθή λειτουργία της εφαρμογής.

Έπειτα, πατάμε στην MySQL το κουμπί *Admin* για να μεταφερθούμε στον localhost server.

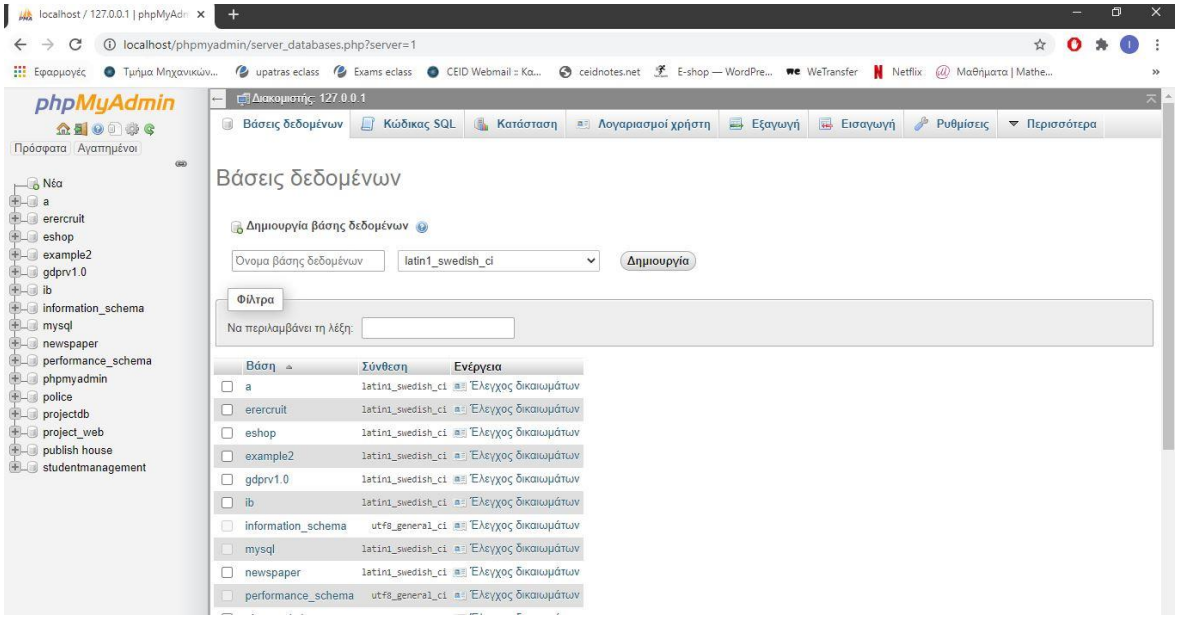


Εικόνα 4.5.3 Πατάμε *Admin* στην MySQL.

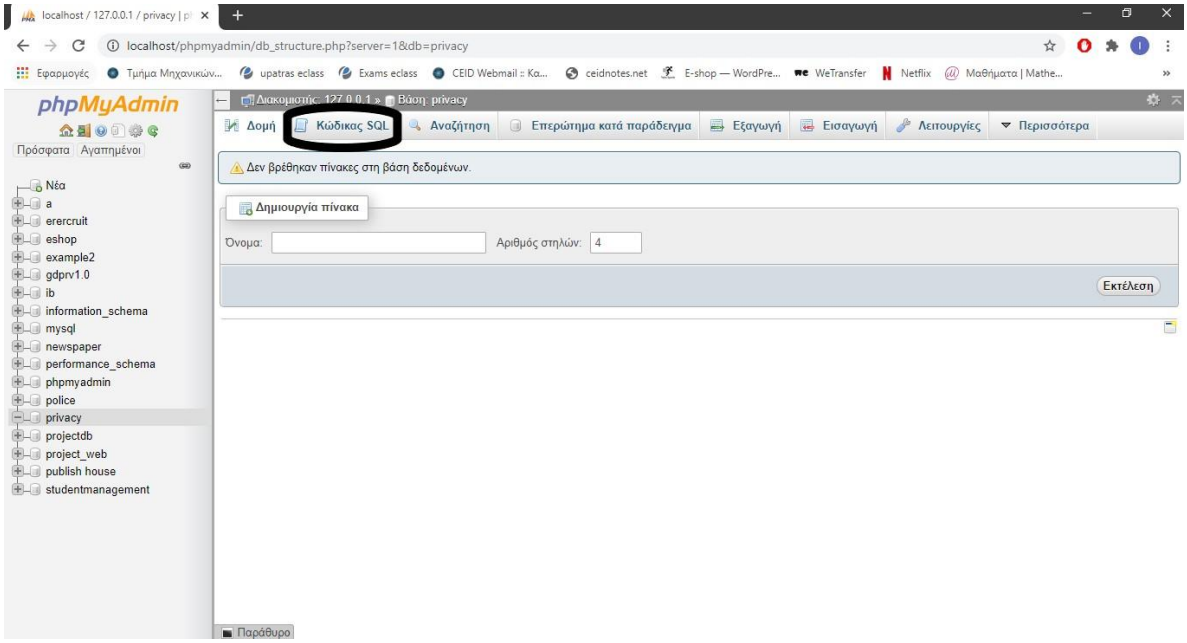


Εικόνα 4.5.4 Ανακατεύθυνση στον localhost server (http://localhost/phpmyadmin/).

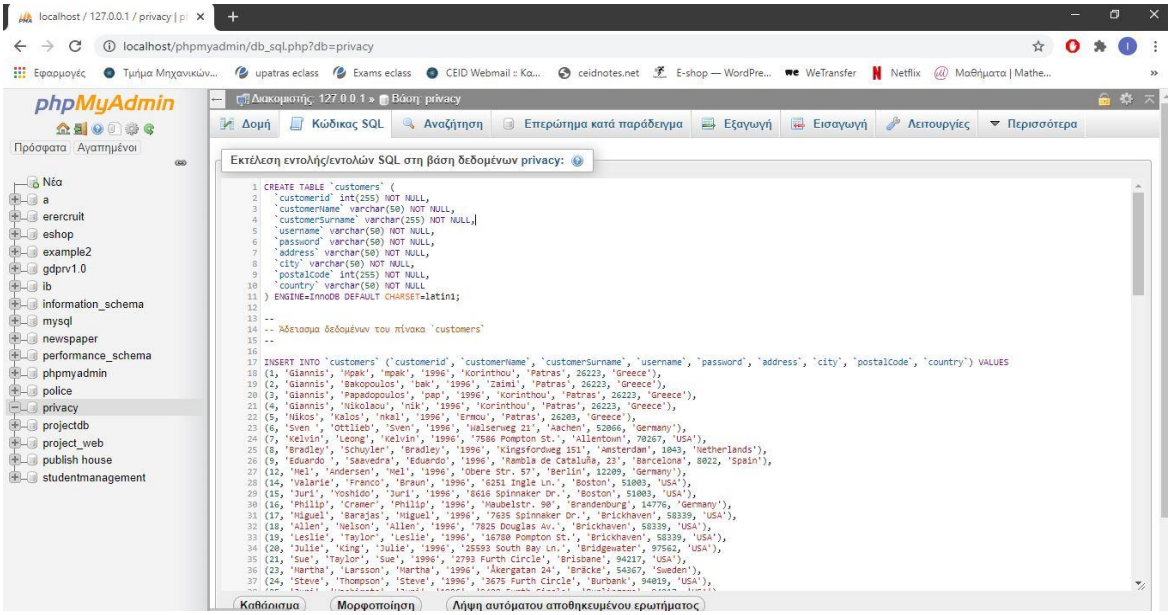
Στην συνέχεια, δημιουργούμε μία βάση δεδομένων με όποιο όνομα επιθυμούμε και προσθέτουμε τον κώδικα SQL της με τα χαρακτηριστικά που αναφέρθηκαν παραπάνω.



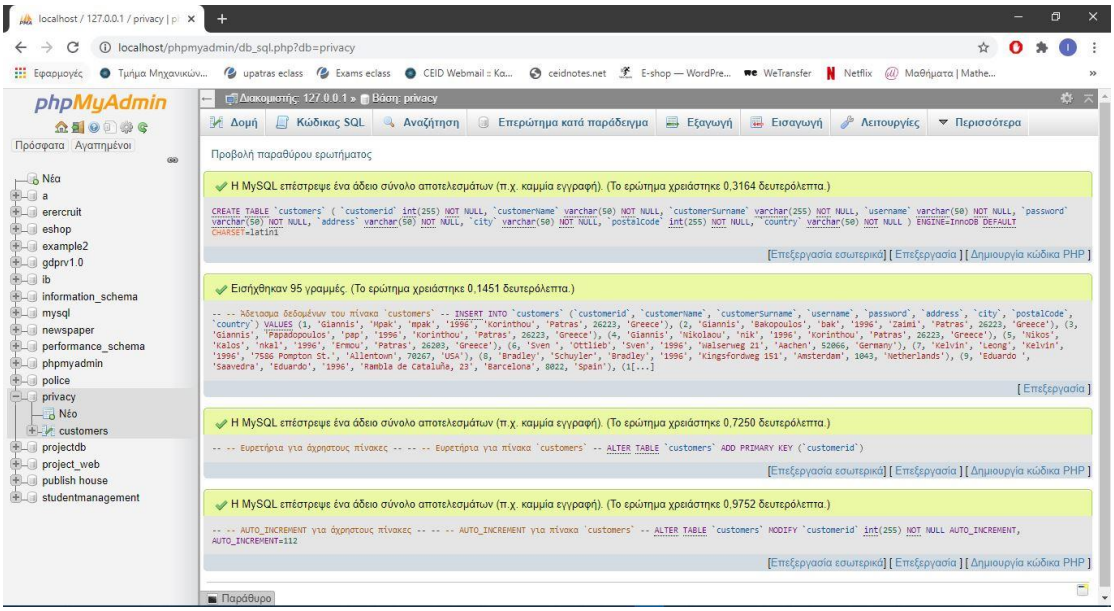
Εικόνα 4.5.5 Δημιουργία νέας βάσης δεδομένων εισάγοντας το όνομα που επιθυμούμε.



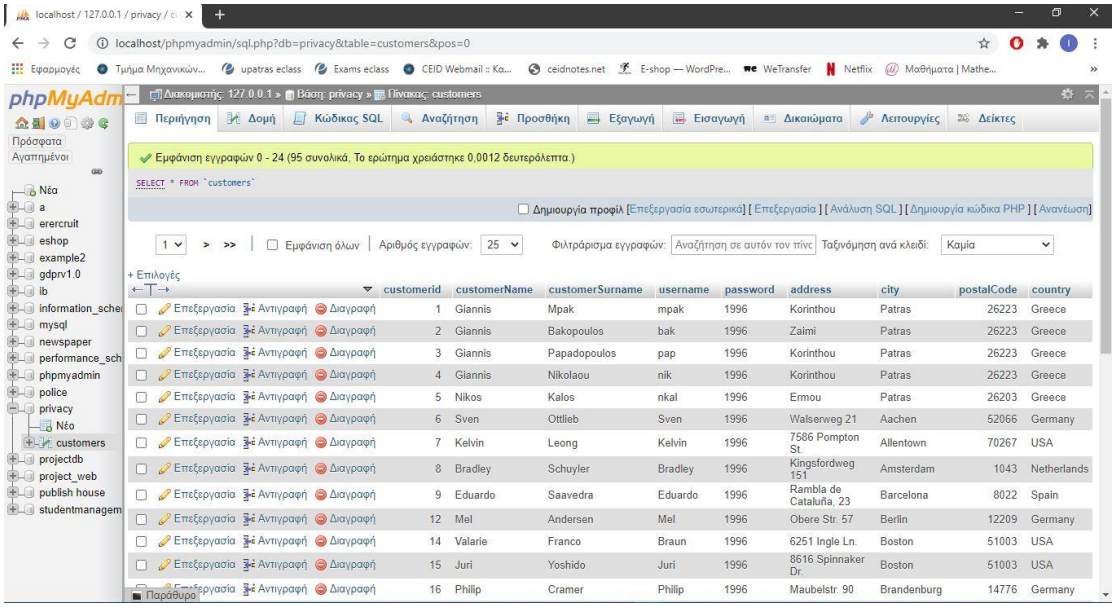
Εικόνα 4.5.6 Εισαγωγή του κώδικα SQL στην βάση δεδομένων που δημιουργήσαμε.



Εικόνα 4.5.7 Εισαγωγή κώδικα SQL στον editor.



Εικόνα 4.5.8 Εμφάνιση αποτελεσμάτων για επιτυχή εκτέλεση κώδικα.



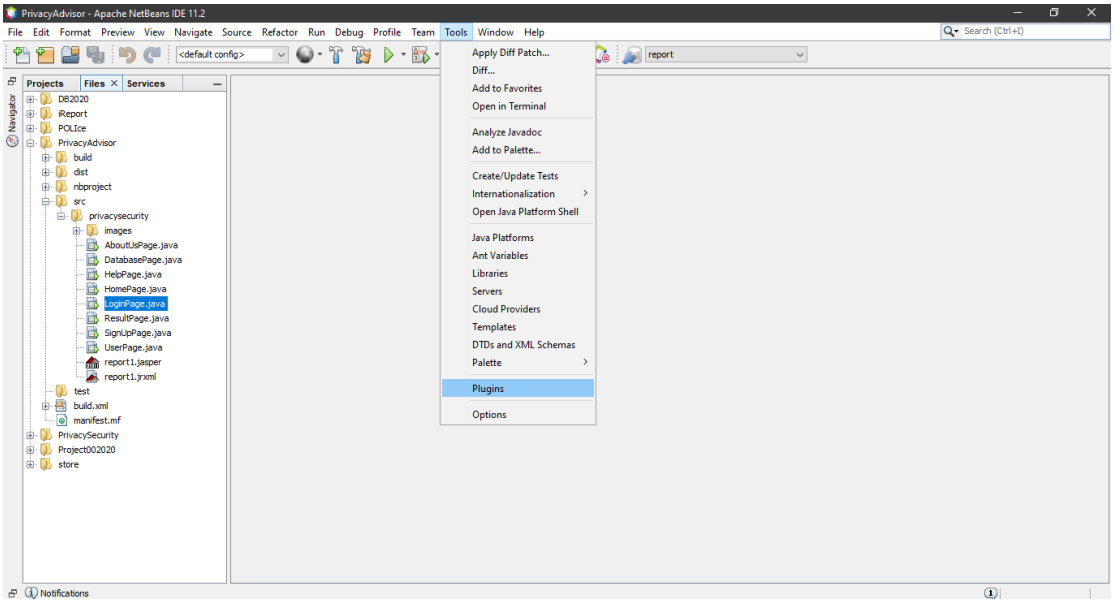
Εικόνα 4.5.9 Εμφάνιση table με τα αντίστοιχα inserts στα field του.

4.6 Αυτοματοποιημένη Αναφορά (i-Report)

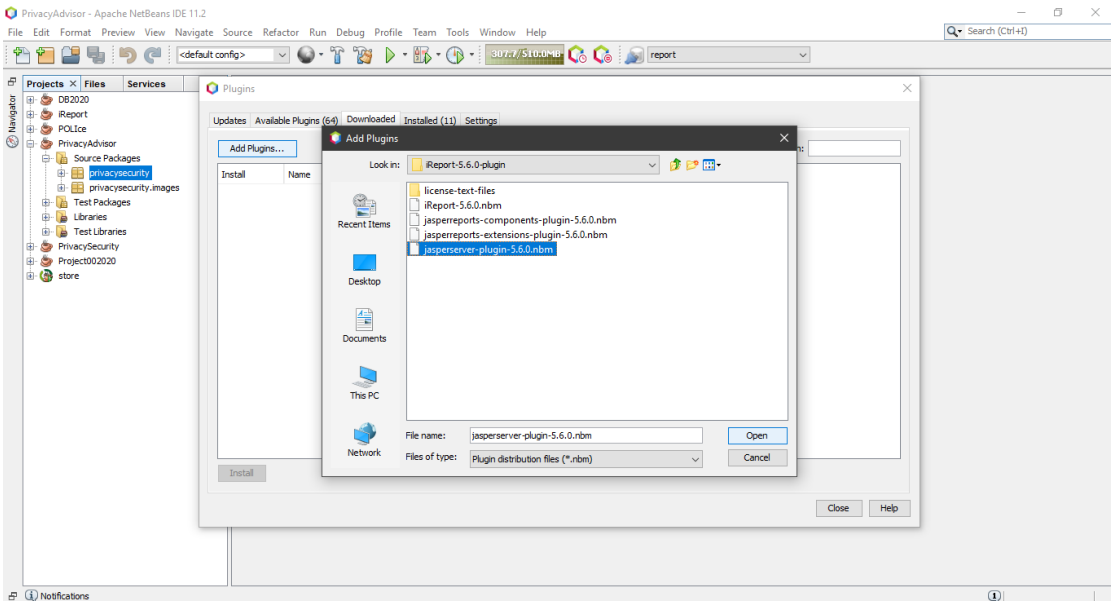
Η αυτοματοποιημένη αναφορά προσφέρει στον χρήστη την εξαγωγή των αποτελεσμάτων από την πιθανότητα επίθεσης σε μία συγκεκριμένη μεταβλητή καθώς και τα προσωπικά στοιχεία του ομαδοποιημένα που έχουν εισαχθεί στην βάση δεδομένων της εφαρμογής.

Η αναφορά αποτελεί ένα σημαντικό στοιχείο της εφαρμογής που αναπτύχθηκε για την δυναμική ανάλυση των αποτελεσμάτων της. Παρακάτω, παρουσιάζονται οι απαραίτητες ενέργειες που πρέπει να κάνει ο χρήστης για την επιτυχή εγκατάσταση της στο Apache Netbeans IDE και την ομαλή λειτουργία της εφαρμογής.

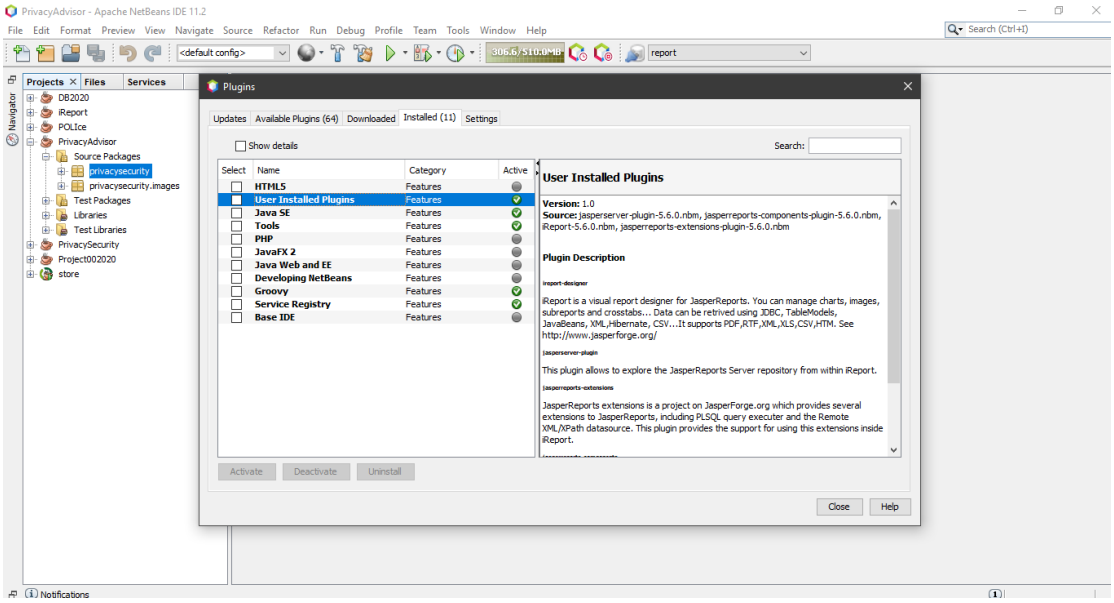
Αρχικά, έχοντα κατεβάσει ο χρήστης το *jasperreports-fonts-6.14.0* και *iReport-5.6.0-plugin* ανοίγει το Apache Netbeans IDE και προσθέτει το plugin.



Εικόνα 4.6.1 Επιλέγουμε τα *Tools* στην συνέχεια τα *Plugins.*

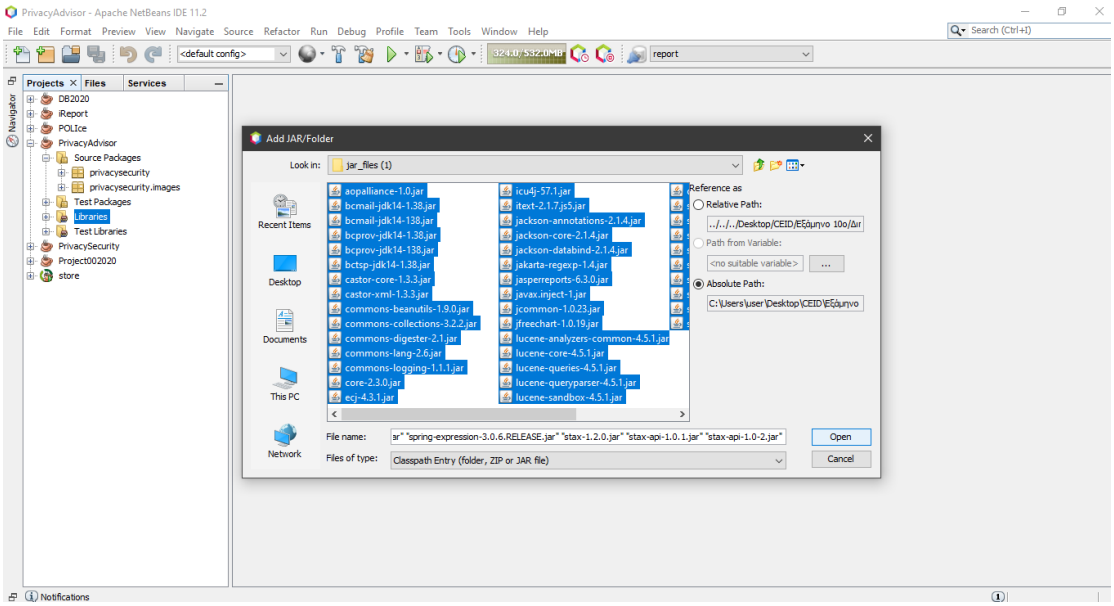


Εικόνα 4.6.2 Επιλέγουμε τα *Downloaded*, μετά πατάμε το *Add Plugins* και εισάγουμε το plugin μας.



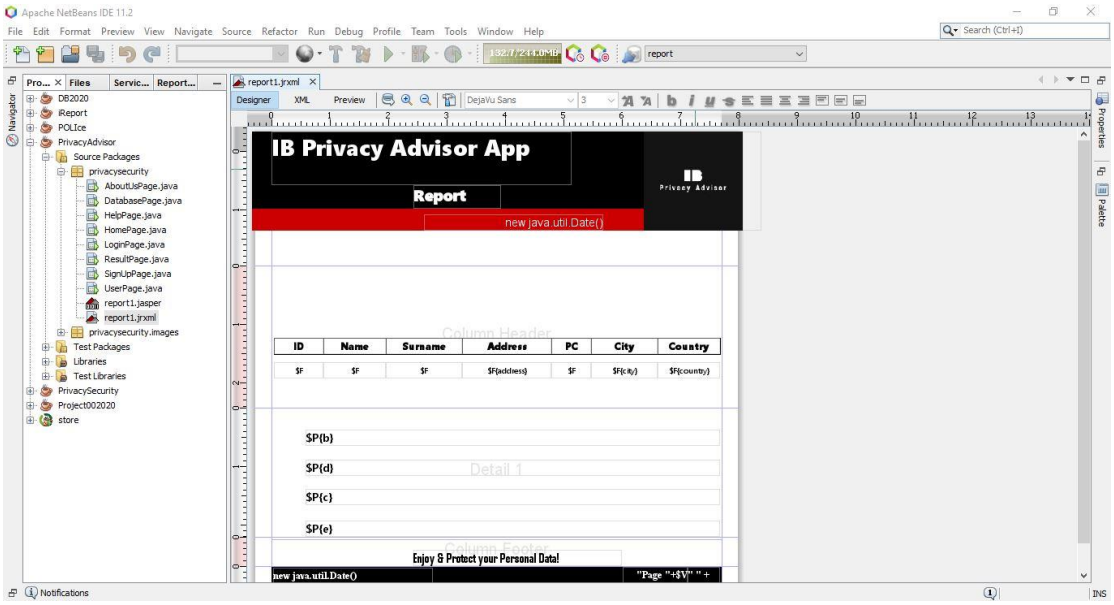
Εικόνα 4.6.3 Ελέγχουμε την επιτυχή εγκατάσταση του plugin μας.

Έπειτα, προσθέτουμε το *jasperreports-fonts-6.14.0* στις βιβλιοθήκες του project μας.



Εικόνα 4.6.4 Επιλέγουμε το *Add JAR/Folder*, επιλέγουμε όλα τα .jar αρχεία του αποσυμπιεσμένου αρχείου και τα προσθέτουμε στην βιβλιοθήκη του project.

Τέλος, παρουσιάζεται το format της αναφοράς.



Εικόνα 4.6.5 Format αναφοράς.

4.7 Sample Tests

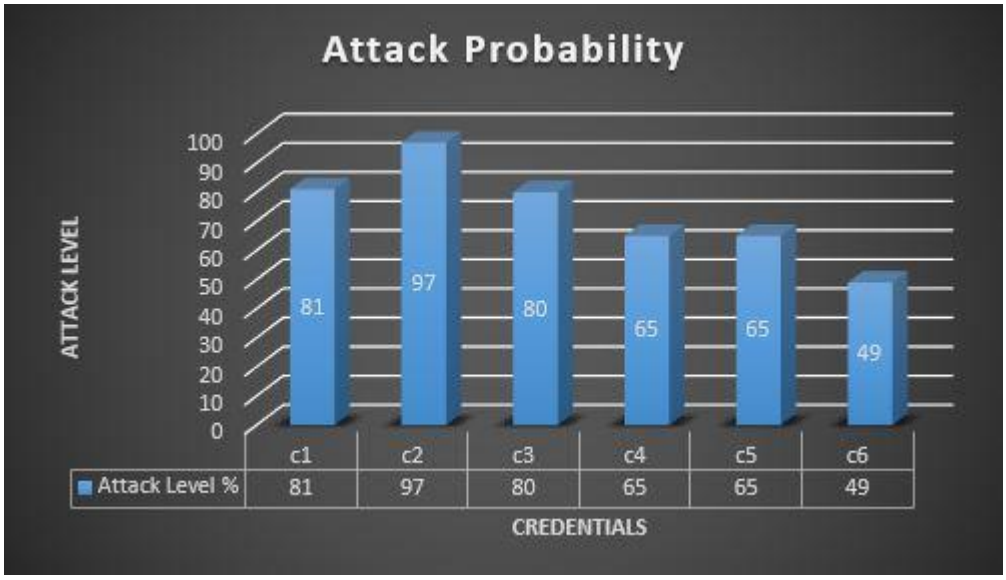
Με τον όρο Sample Tests εννοείται η χρήση τυχαίων μεταβλητών για την ορθή εξαγωγή συμπερασμάτων ύστερα από την εκτέλεση της εφαρμογής.

Στον παρακάτω πίνακα παρουσιάζεται η χρήση των έξι μεταβλητών της εφαρμογής παίρνοντας τυχαίες τιμές από ένα τυχαίο χρήστη για την εξαγωγή συμπερασμάτων.

Credential	Attribute
C1	Name=Giannis
C2	Surname=Mpak
C3	Address=Korinthou
C4	Postal Code=26223
C5	City= Patras
C6	Country= Greece

Εικόνα 4.7.1 Πίνακας Sample Test με τις μεταβλητές που χρησιμοποιήθηκαν.

Στον παρακάτω πίνακα εμφανίζονται οι πιθανότητες επίθεσης στις παραπάνω μεταβλητές ύστερα από την εκτέλεση της εφαρμογής.



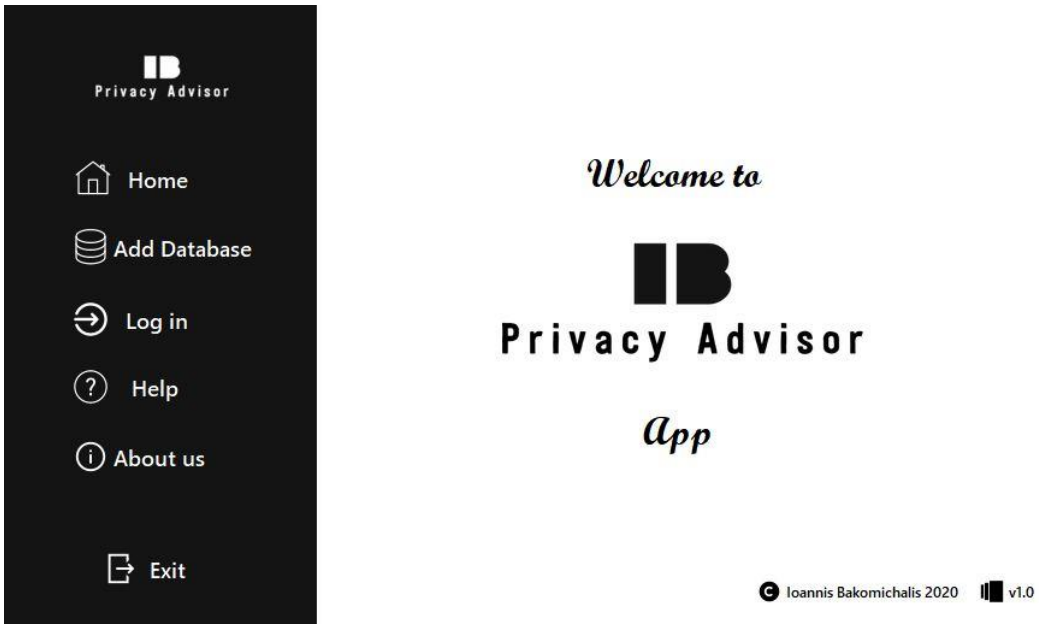
Εικόνα 4.7.2 Πίνακας Sample Test με τα αποτελέσματα της πιθανότητας επίθεσης.

Κεφάλαιο 5: Παρουσίαση Λειτουργίας

Στο κεφάλαιο αυτό παρουσιάζεται η λειτουργικότητα της εφαρμογής βήμα-βήμα με χρήση screenshots καθώς και με την κατάλληλη λεκτική περιγραφή.

5.1 Αρχική Σελίδα (Home Page)

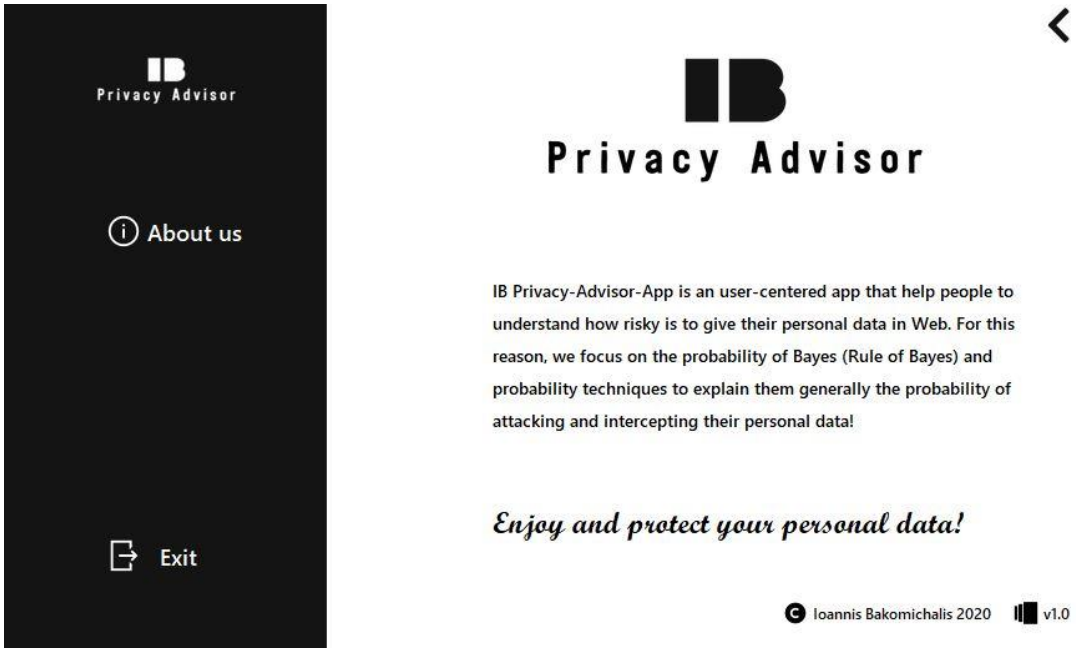
Ο χρήστης αφού κάνεις *run* τον κώδικα στο Apache Netbeans IDE ανακατευθύνεται στην *"Αρχική Σελίδα"* της εφαρμογής. Εκεί, εμφανίζεται το μενού της εφαρμογής "*IB Privacy Advisor App*" και αυτό περιλαμβάνει το Home, το Add Database, το Log in, το Help, το About us καθώς και το Exit.



5.1.1 Αρχική σελίδα εφαρμογής (Home Page).

5.2 Σελίδα Σχετικά με Εμάς (About us Page)

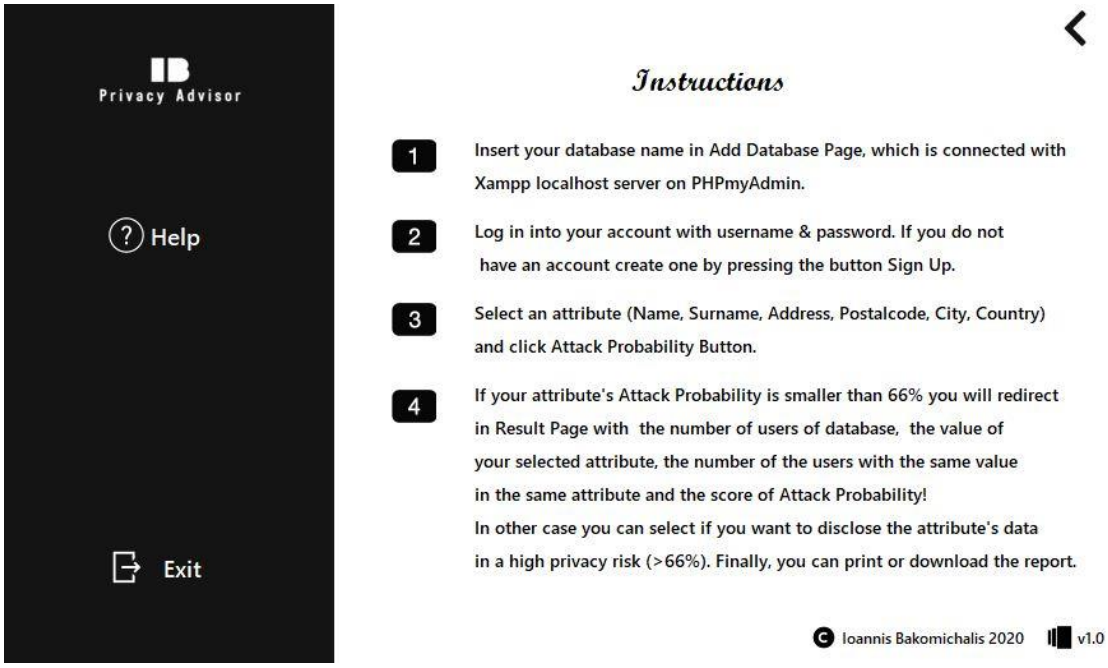
Στην "*Σελίδα Σχετικά με Εμάς"* ο χρήστης ενημερώνεται για τον σκοπό της εφαρμογής καθώς και για τις πιθανο-στατιστικές τεχνικές που χρησιμοποιεί για τον υπολογισμό της πιθανότητας επίθεσης στις μεταβλητές του συστήματος.



Εικόνα 5.2.1 Σελίδα Σχετικά με Εμάς (About us Page).

5.3 Σελίδα Βοήθειας (Help Page)

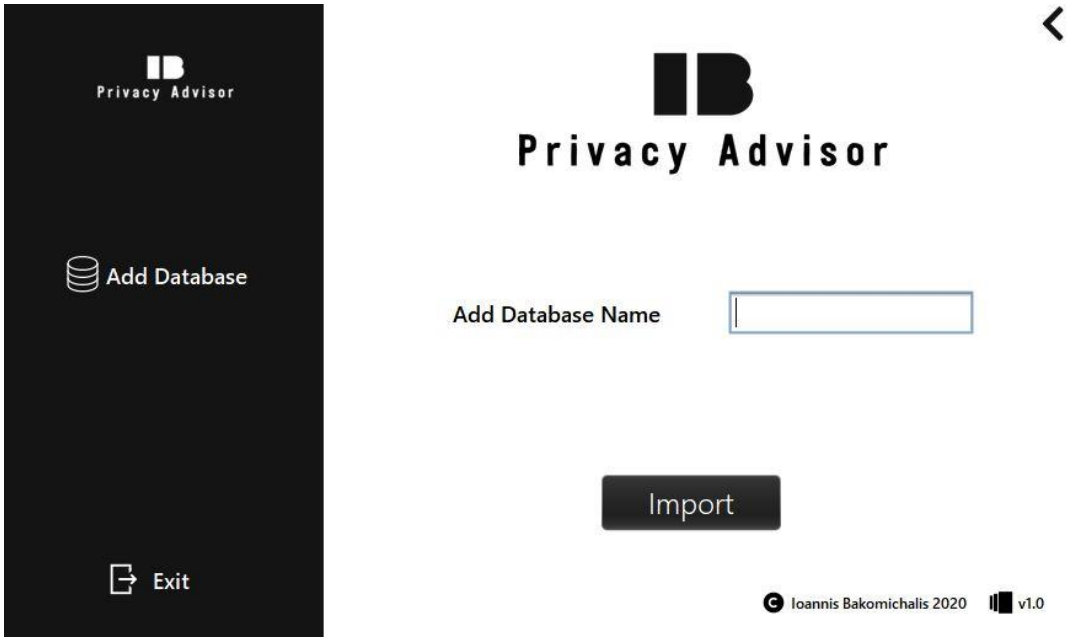
Στην *"Σελίδα Βοήθειας"* ο χρήστης λαμβάνει τις απαραίτητες οδηγίες προκειμένου να εκτελέσει με σειρά τα κατάλληλα βήματα για την ορθή και επιτυχή λειτουργία της εφαρμογής.



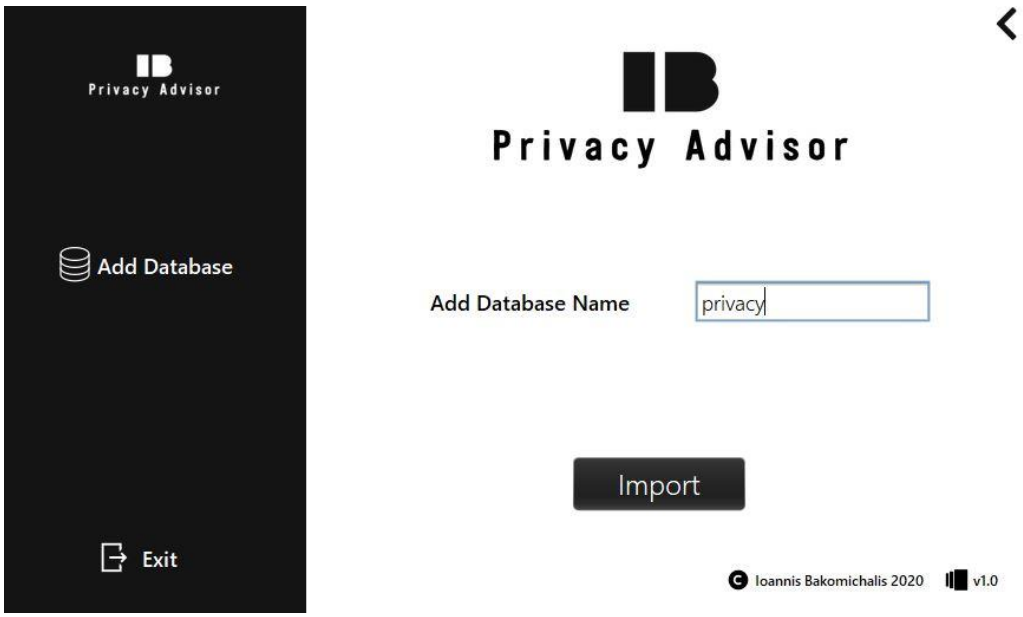
Εικόνα 5.3.1 Σελίδα Βοήθειας (Help Page).

5.4 Σελίδα Προσθήκης Βάσης Δεδομένων (Add Database Page)

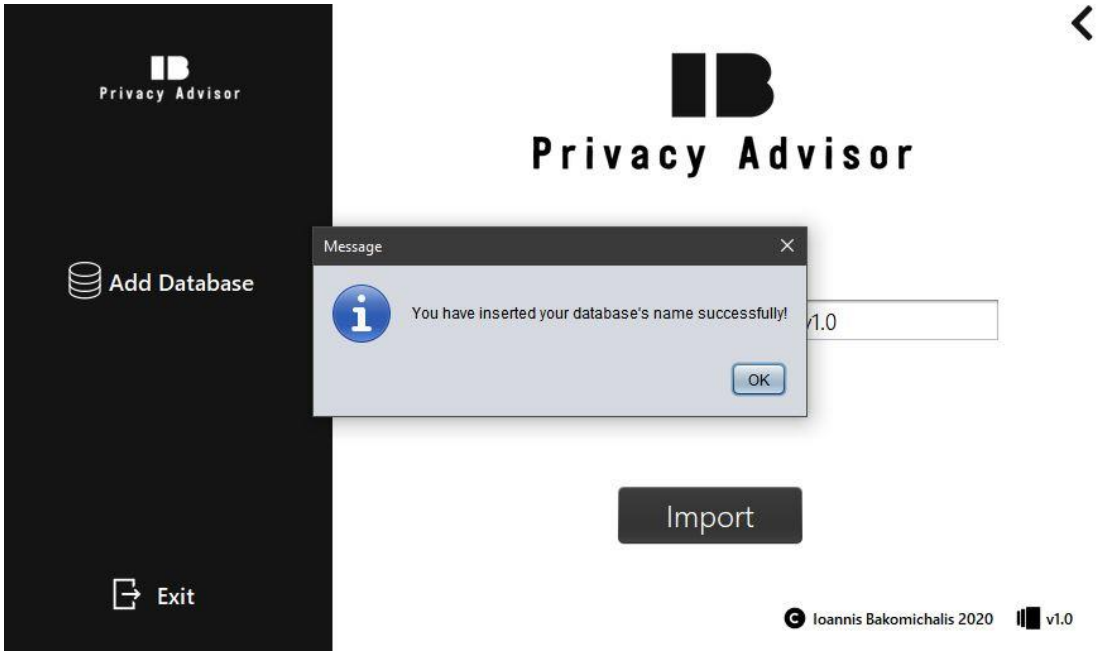
Η *"Σελίδα Προσθήκης Βάσης Δεδομένων"* αποτελεί το πρώτο και πιο βασικό βήμα που πρέπει να κάνει ο χρήστης για την επιτυχή λειτουργία της εφαρμογής. Εκεί, ο χρήστης προσθέτει το όνομα της βάσης δεδομένων που έχεις εισάγει μέσω του *xampp* στο *localhost*. Ο χρήστης αφού εισάγει το όνομα της βάσης δεδομένων, του εμφανίζεται στην οθόνη μήνυμα επιτυχίας και ανακατευθύνεται στην *Σελίδα Σύνδεσης* της εφαρμογής.



5.4.1 Σελίδα Προσθήκης Βάσης Δεδομένων (Add Database Page).



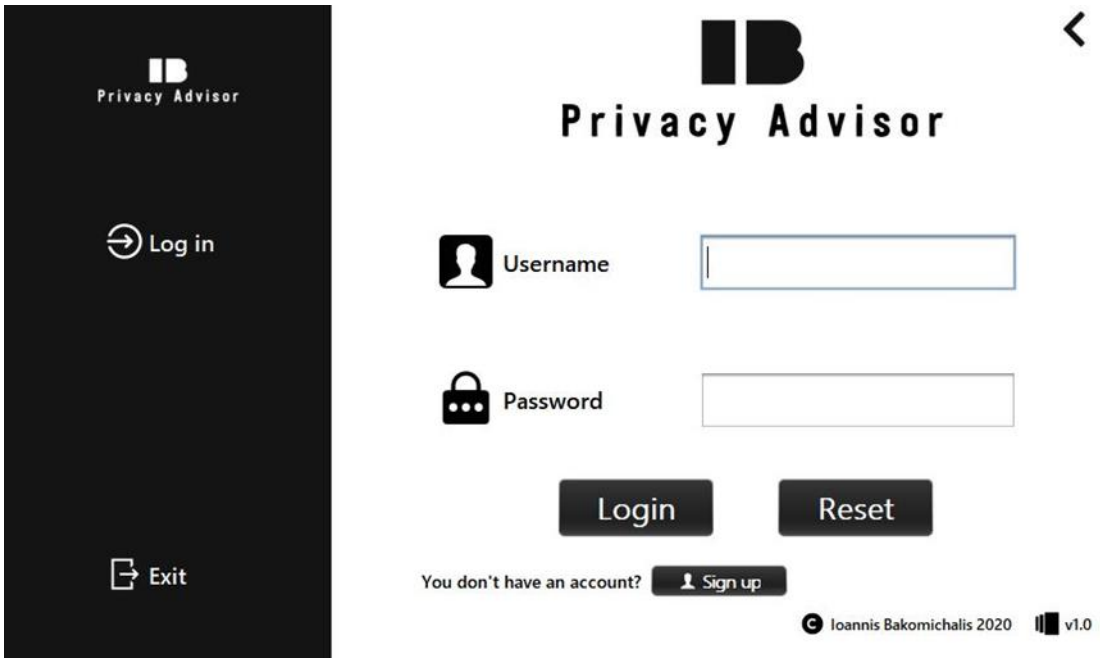
5.4.2 Εισαγωγή ονόματος βάσης δεδομένων.



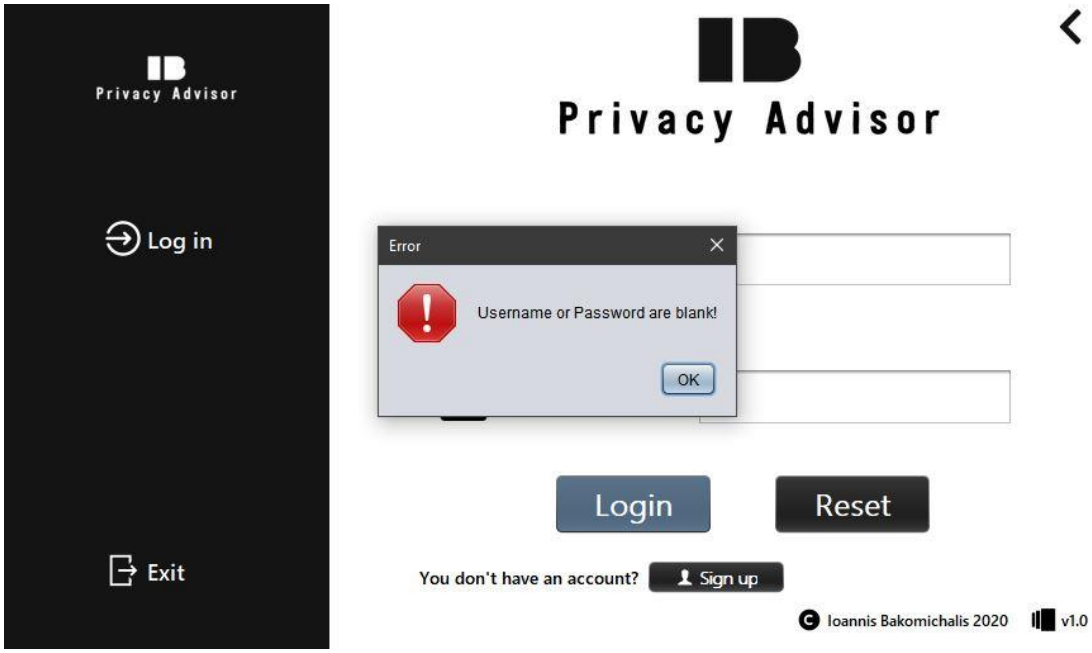
5.4.3 Μήνυμα για επιτυχή εισαγωγή ονόματος βάσης δεδομένων.

5.5 Σελίδα Σύνδεσης (Login Page)

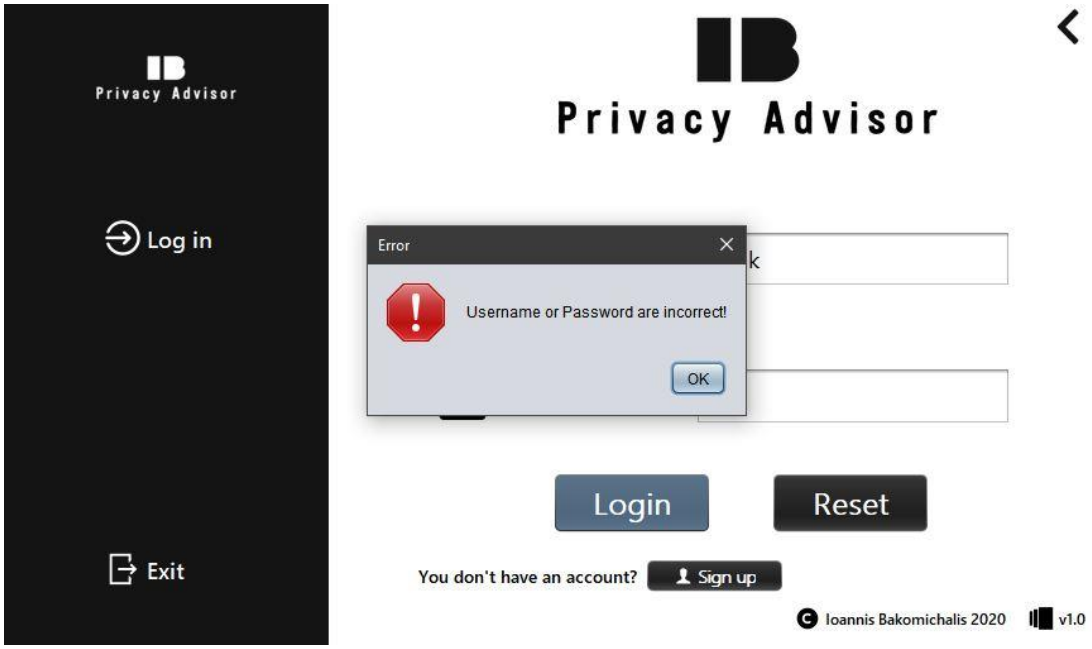
Στην "*Σελίδα Σύνδεσης"* ο χρήστης συνδέεται στο σύστημα της εφαρμογής και ταυτοποιείται μέσω του username και του password του. Αν ο χρήστης δεν έχει λογαριασμό στο σύστημα μπορεί να φτιάξει λογαριασμό πατώντας το κουμπί "*Sign up*". Ο χρήστης αφού ταυτοποιηθεί από το σύστημα, του εμφανίζονται τα κατάλληλα μηνύματα επιτυχίας ή αποτυχία αντίστοιχα και εφόσον ταυτοποιηθεί επιτυχώς ανακατευθύνεται στην "*Σελίδα Χρήστη"* της εφαρμογής.



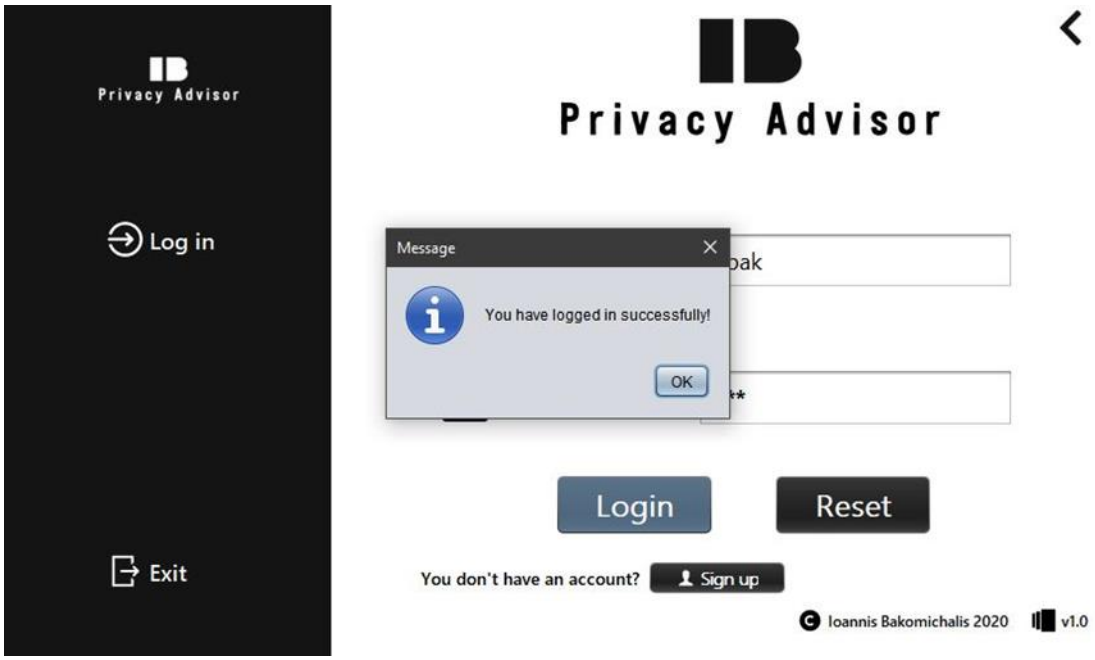
5.5.1 Σελίδα Σύνδεσης (Login Page).



5.5.2 Μήνυμα για εισαγωγή κενών πεδίων.



5.5.3 Μήνυμα για εισαγωγή λανθασμένων στοιχείων.

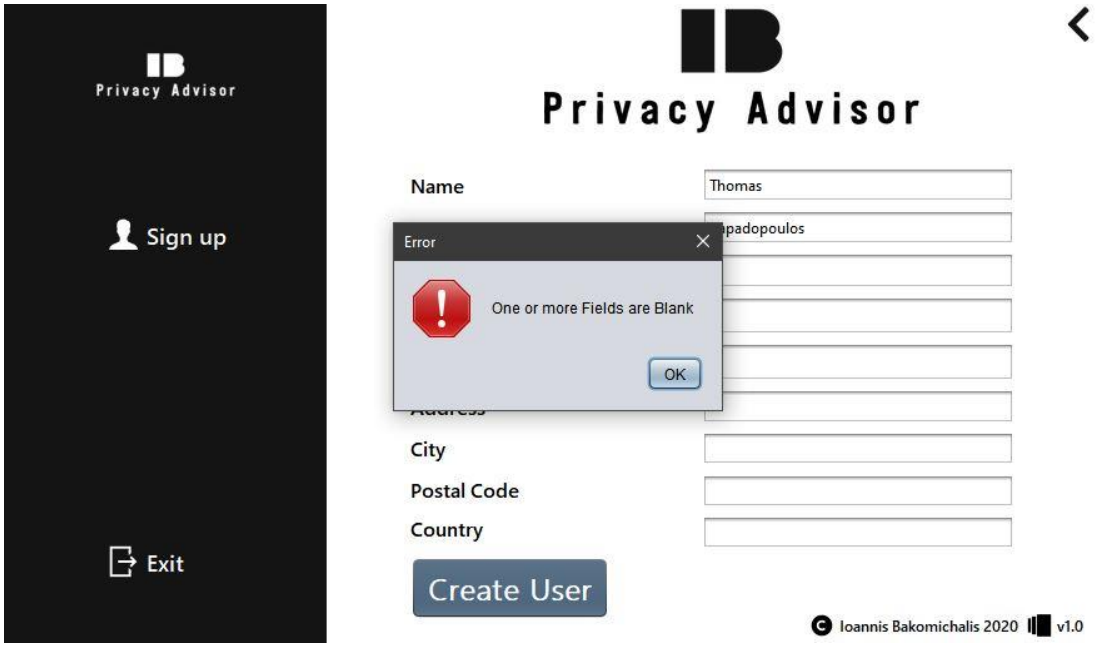


5.5.4 Μήνυμα για Επιτυχή σύνδεση στο σύστημα.

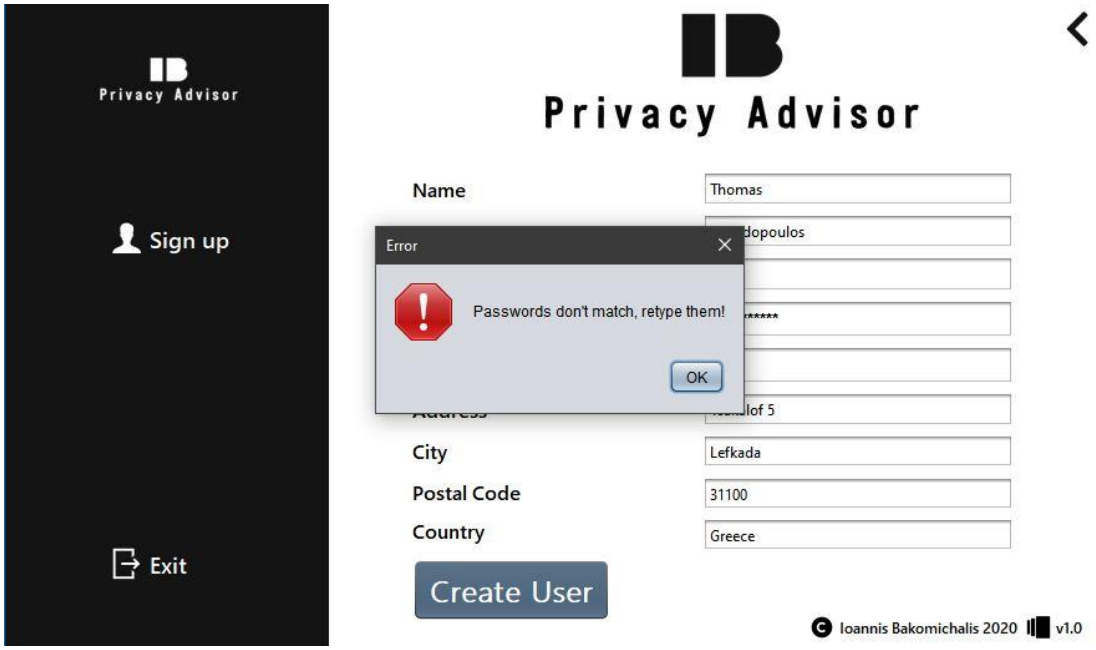
5.6 Σελίδα Δημιουργίας Λογαριασμού (Sign up Page)

Στην *"Σελίδα Δημιουργίας Λογαριασμού"* ο χρήστης εισάγει τα κατάλληλα στοιχεία στο σύστημα με σκοπό την δημιουργία λογαριασμού για να εισέλθει σε αυτό. Εκεί, γίνεται έλεγχος για τον κωδικό πρόσβασης για το αν συμπίπτει με την επιβεβαίωση κωδικού πρόσβασης αλλά και για το πόσο ισχυρός είναι, δηλαδή να περιέχει τουλάχιστον 8 ψηφία, 1 κεφαλαίο γράμμα, 1 πεζό γράμμα, 1 αριθμό και 1 ειδικό χαρακτήρα. Έπειτα, ο χρήστης ανακατευθύνεται στην "Σελίδα Σύνδεσης" της εφαρμογής.

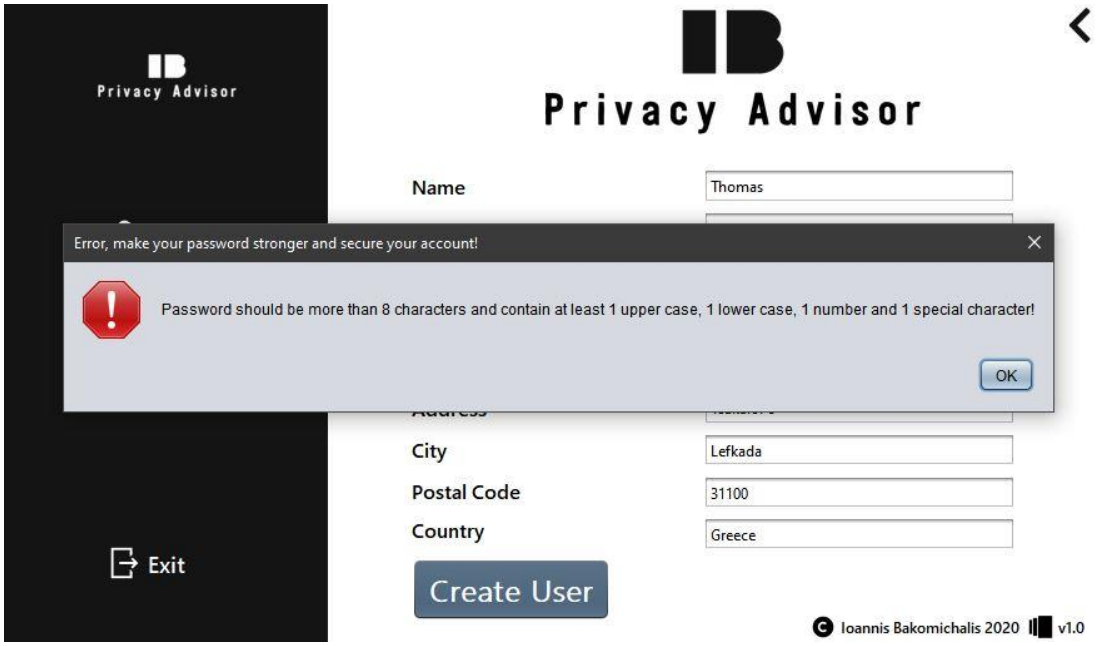
5.6.1 Σελίδα Δημιουργίας Λογαριασμού (Sign up Page).



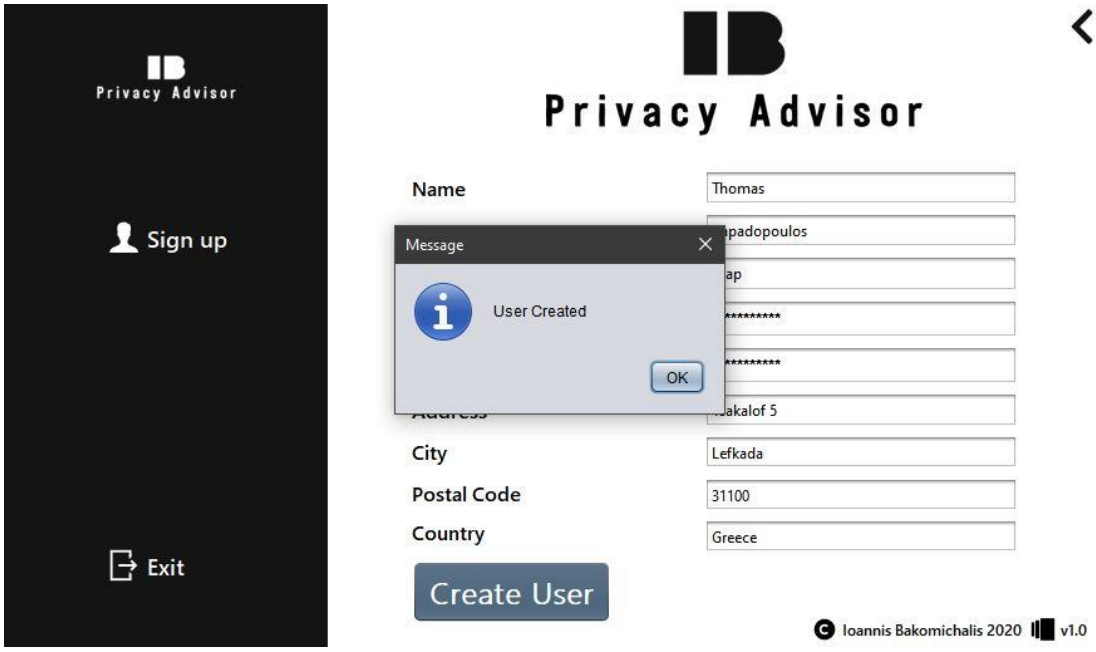
5.6.2 Μήνυμα για εισαγωγή κενών πεδίων.



5.6.3 Μήνυμα για εισαγωγή διαφορετικών κωδικών.



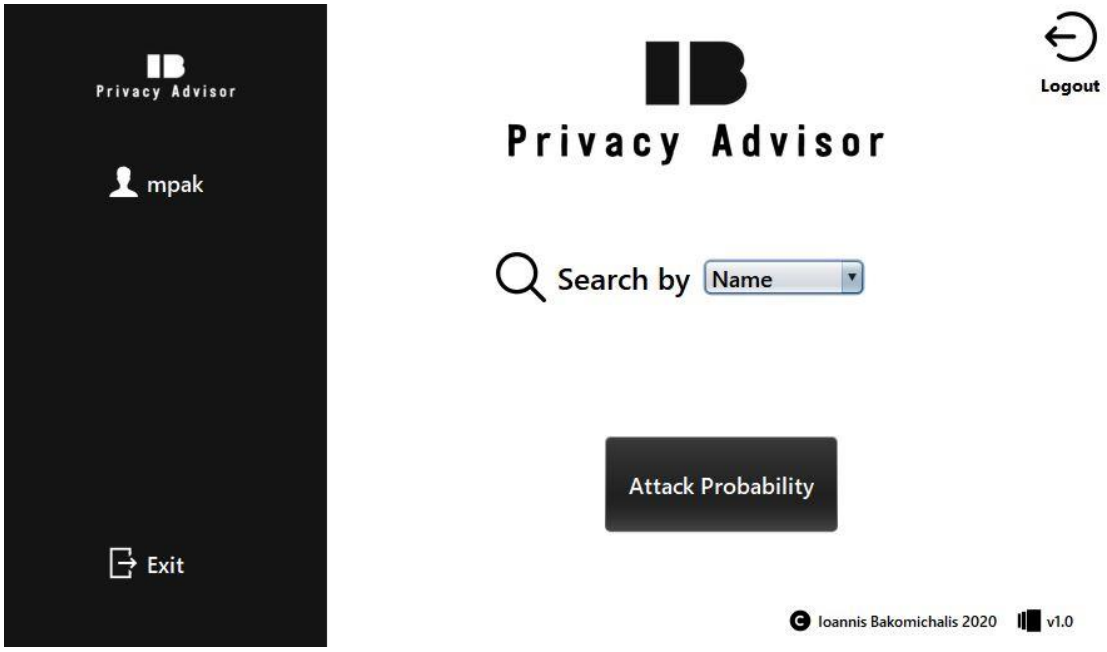
5.6.4 Μήνυμα για εισαγωγή μη ασφαλούς κωδικού.



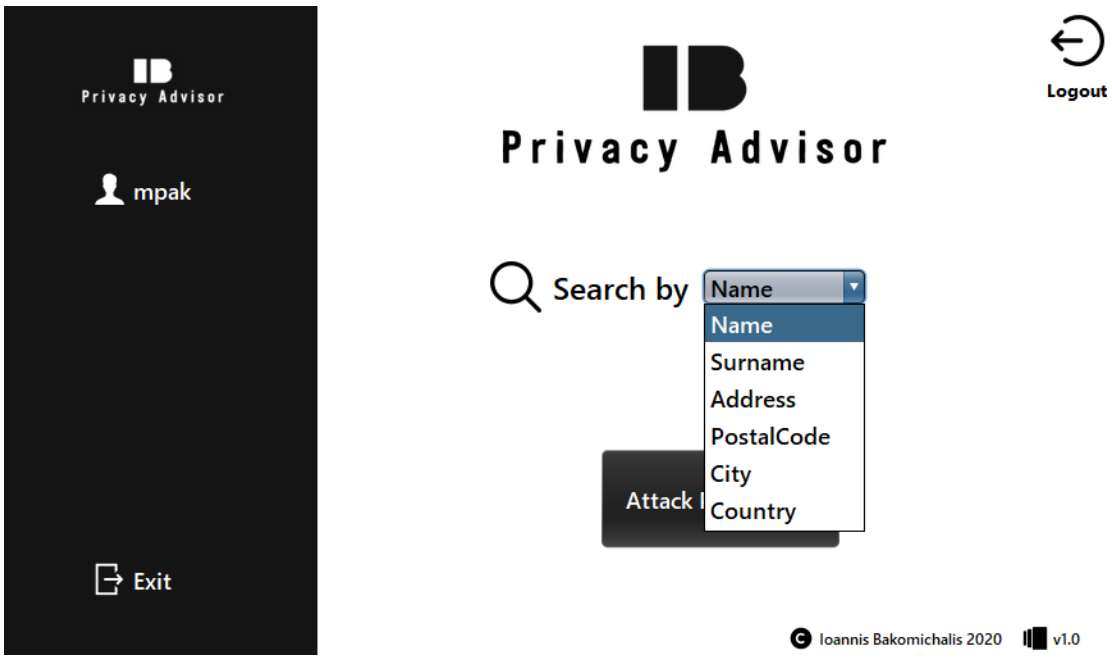
5.6.5 Μήνυμα για επιτυχή Δημιουργία Λογαριασμού.

5.7 Σελίδα Χρήστη (User Page)

Στην *"Σελίδα Χρήστη"* ο χρήστης επιλέγει την μεταβλητή (attribute), της οποίας θέλει να μάθει την πιθανότητα επίθεσης. Οι μεταβλητές εμφανίζονται μέσω JCombobox. Αφού επιλέξει μεταβλητή ο χρήστης πατάει το κουμπί "*Attack Probability*" και εμφανίζεται στην οθόνη του η πιθανότητα επίθεσης στην μεταβλητή που επέλεξε. Αν η πιθανότητα επίθεσης ανήκει στην κατηγορία "High Risk", δηλαδή είναι μεγαλύτερη από 66%, τότε ο χρήστης μπορεί να επιλέξει αν επιθυμεί ή όχι να δώσει το συγκεκριμένο προσωπικό δεδομένο του στο σύστημα και έπειτα ανακατευθύνεται στην "*Σελίδα Αποτελεσμάτων*". Σε κάθε άλλη περίπτωση, ανακατευθύνεται αυτόματα στην "*Σελίδα Αποτελεσμάτων*".



5.7.1 Σελίδα Χρήστη (User Page).



5.7.2 Επιλογή Μεταβλητής (Attribute).

5.7.3.1 Μήνυμα Μεγάλου Ρίσκου Πιθανότητας Επίθεσης.

5.7.3.2 Μήνυμα Μεγάλου Ρίσκου Πιθανότητας Επίθεσης επιλέγοντας όχι.

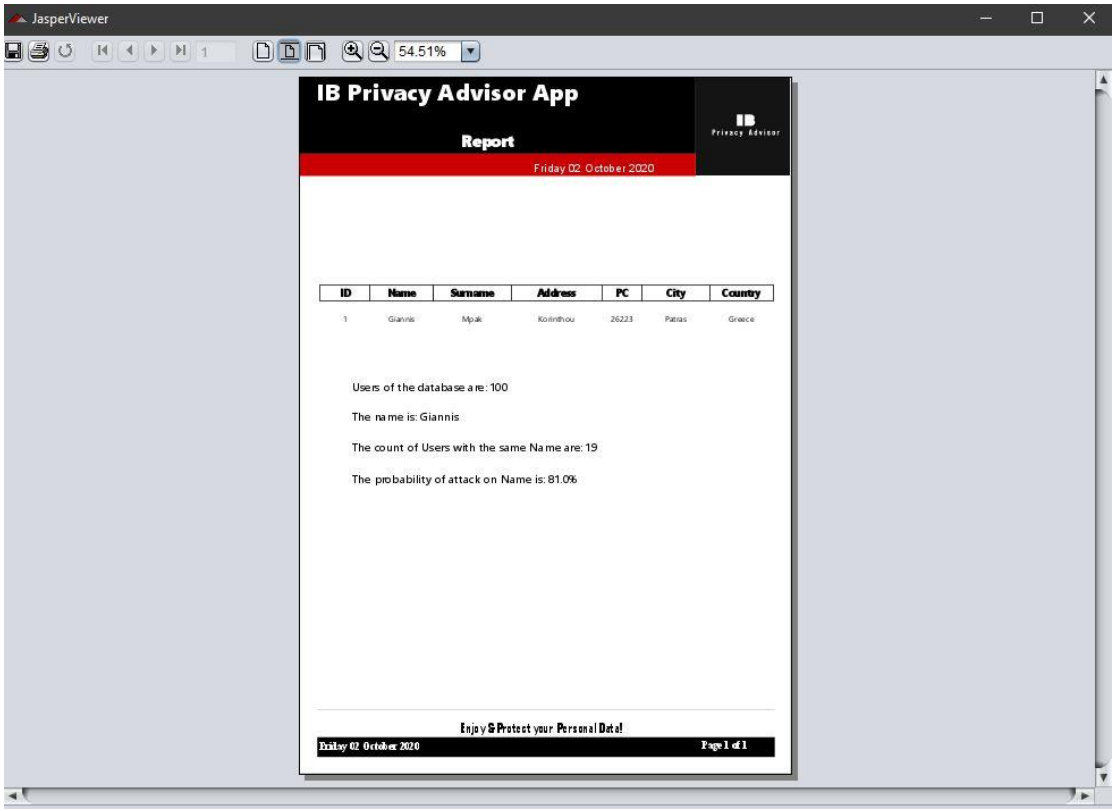
5.7.4 Μήνυμα Μικρού Ρίσκου Πιθανότητας Επίθεσης.

5.7.5 Αποσύνδεση από Λογαριασμό Χρήστη.

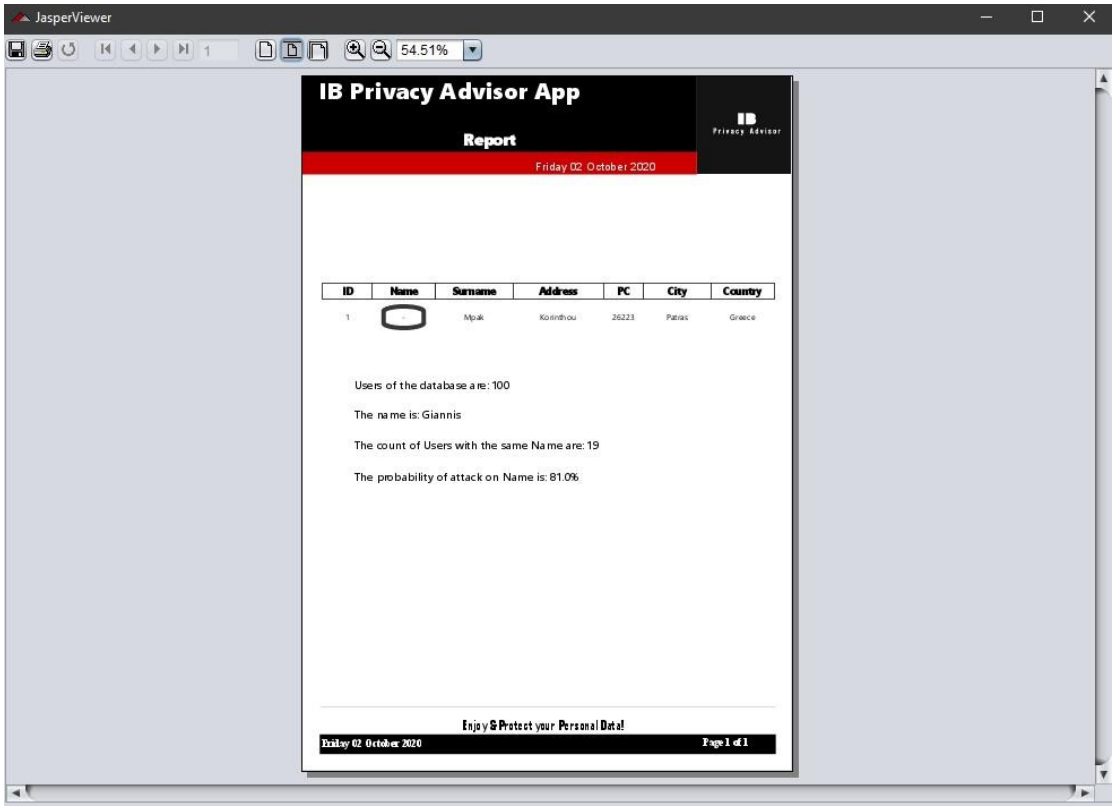
5.8 Σελίδα Αποτελεσμάτων (Result Page)

Στην *"Σελίδα Αποτελεσμάτων"* εμφανίζονται τα αποτελέσματα ύστερα από τον υπολογισμό της πιθανότητας επίθεσης της αντίστοιχης μεταβλητής που επέλεξε ο χρήστης. Επιπλέον δίνεται η δυνατότητα στον χρήστη να κατεβάσει ή να εκτυπώσει αναφορά με τα αντίστοιχα αποτελέσματα και με τα προσωπικά στοιχεία του.

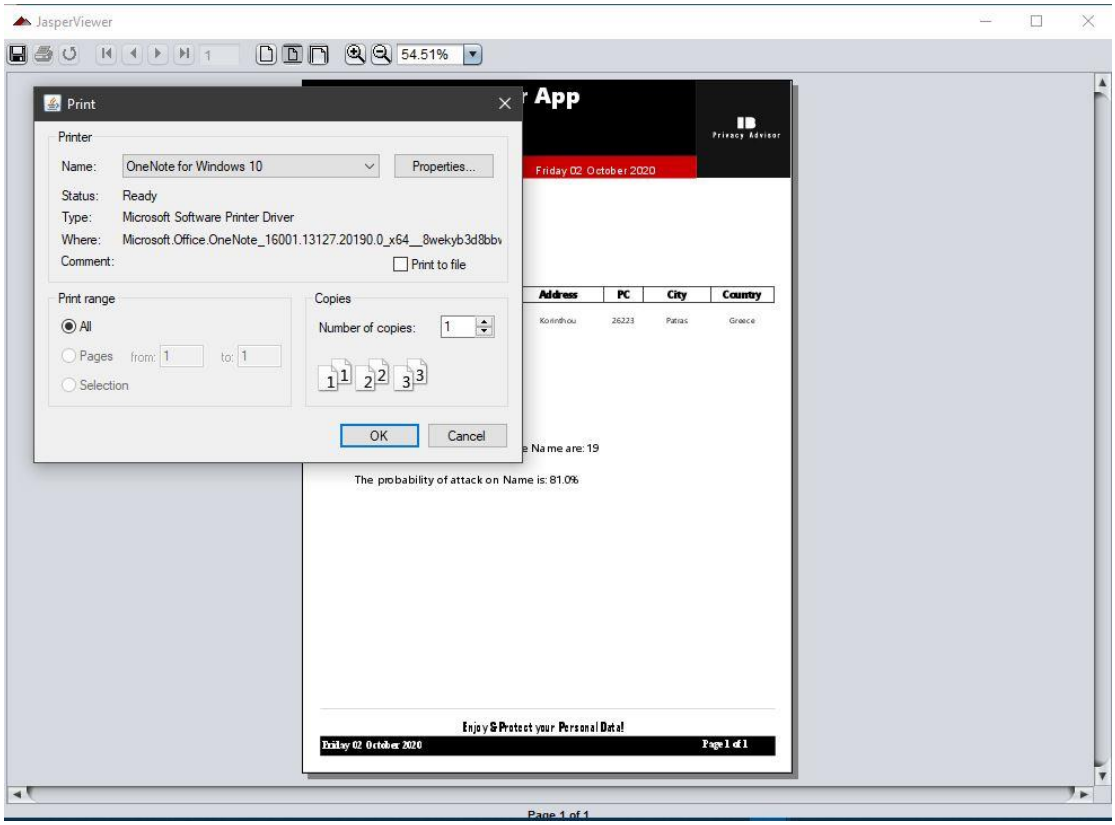
5.8.1 Σελίδα Αποτελεσμάτων (Result Page)



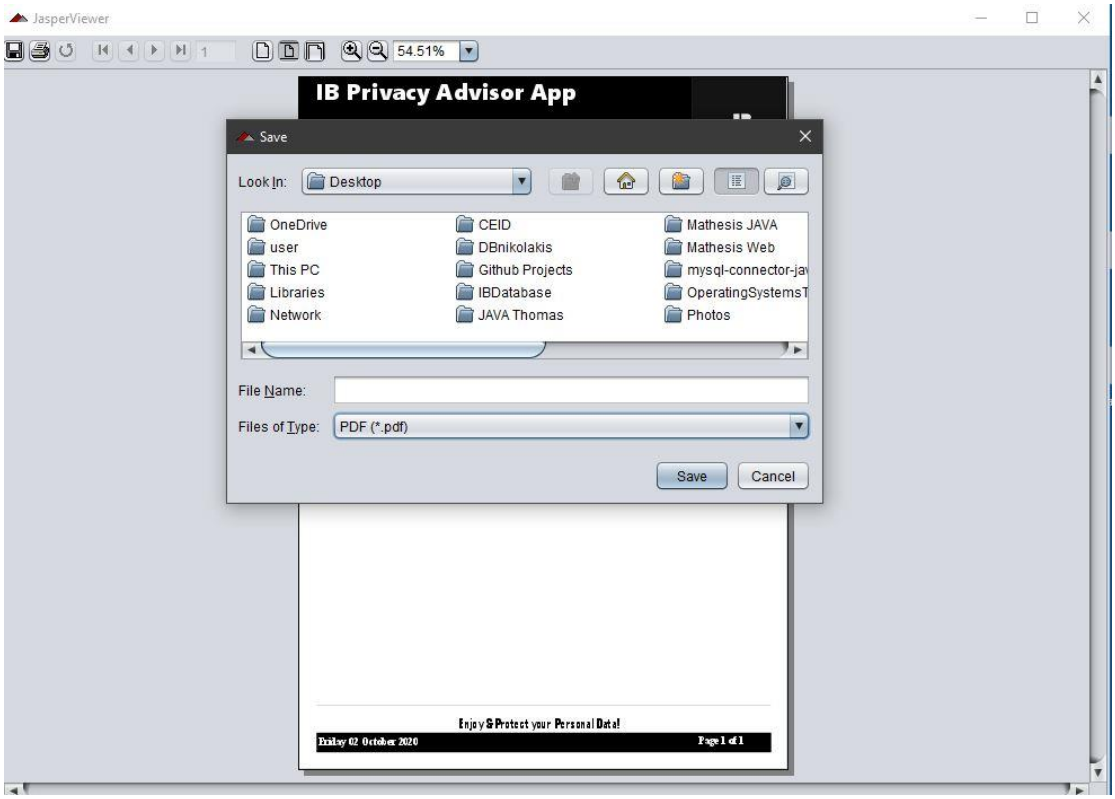
5.8.2.1 Αναφορά (Report)



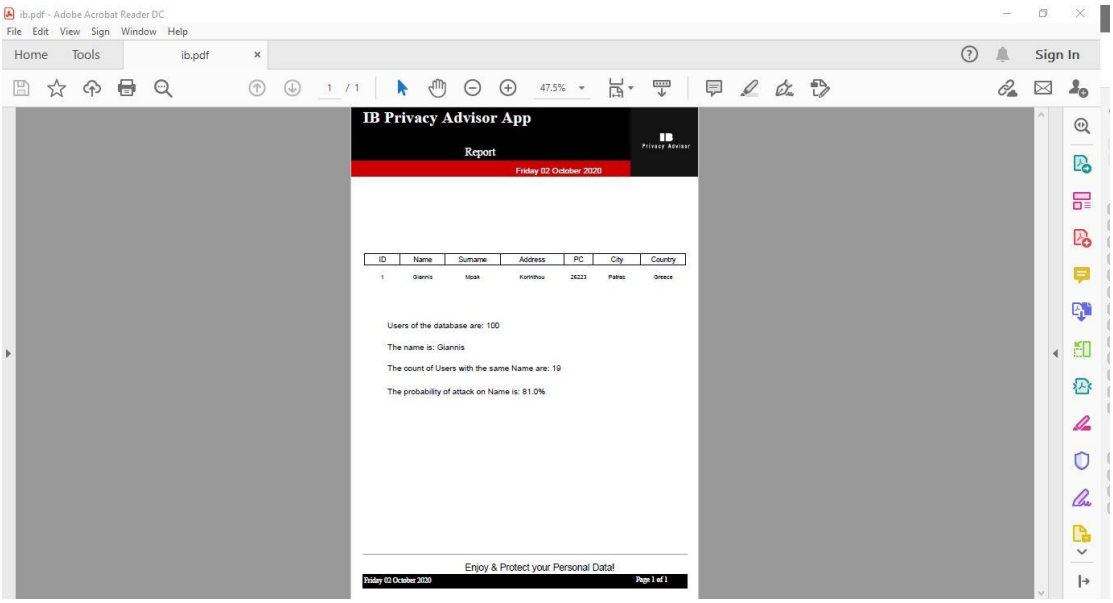
5.8.2.2 Αναφορά έχοντας επιλέξει να μην δώσουμε το στοιχείο μας την βάση δεδομένων.



5.8.3 Εκτύπωση Αναφοράς (Print Report)



5.8.4 Κατέβασμα Αναφοράς και επιλογή τύπου αρχείου (Download report as a type of file).



5.8.5 Pdf αρχείο Αναφοράς(Report pdf).

Κεφάλαιο 6: Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάζονται τα συμπεράσματα που προέκυψαν ύστερα από την υλοποίηση της εφαρμογής, τα κύρια σημεία της εργασίας, καθώς και οι μελλοντικές επεκτάσεις που μπορούν να γίνουν στην εφαρμογή που αναπτύχθηκε.

6.1 Σύνοψη

Όπως αναφέραμε και στην αρχή της εργασίας, η παραβίαση της ιδιωτικότητας και η υποκλοπή των προσωπικών δεδομένων βρίσκεται σε έξαρση λόγω της μεγάλης ανάπτυξης της τεχνολογίας, καθώς βρισκόμαστε στην ψηφιακή εποχή. Τα προσωπικά δεδομένα αποτελούν την ταυτότητα του κάθε ανθρώπου και για αυτό τον λόγο πρέπει να μάθουμε να τα προστατεύουμε καθώς και να τα χειριζόμαστε ορθά. Επιπλέον, παρά την χρήση μεθόδων για την προστασία των προσωπικών δεδομένων, οι περισσότεροι άνθρωποι γνωρίζουν μηδαμινά πράγματα για την σημασία και την χρήση τους. Για αυτόν τον λόγο, πρέπει όλοι να είμαστε ενημερωμένοι από την υπάρχουσα νομοθεσία τόσο της Ευρωπαϊκής Ένωσης (Ε.Ε.) όσο και της Ελλάδας για την χρησιμότητα και την προστασία τους. Η παρούσα εργασία κινείται σε αυτήν την κατεύθυνση, εστιάζοντας στην δημιουργία μίας εφαρμογής επικεντρωμένης στον χρήστη με απώτερο σκοπό την ενημέρωση των ανθρώπων για την πιθανότητα επίθεσης πάνω στα προσωπικά τους δεδομένα καθώς και για την προστασία τους από τυχόν απειλές, βασιζόμενη στο θεώρημα του Bayes και στην χρήση πιθανο-στατιστικών τεχνικών για την εξαγωγή ορθών αποτελεσμάτων της πιθανότητας επίθεσης στα προσωπικά δεδομένα.

Στην συνέχεια της εργασίας, παρουσιάστηκαν κάποιοι βασικοί όροι όπως των προσωπικών δεδομένων και της ιδιωτικότητας. Ακόμα περιγράφηκαν οι βασικοί λόγοι που οδηγούν σε υποκλοπή προσωπικών δεδομένων, καθώς και οι τρόποι με τον οποίο γίνονται. Επιπλέον, παρουσιάστηκαν οι απαιτήσεις της ιδιωτικότητας και οι βασικοί μέθοδοι για την προστασία των προσωπικών δεδομένων. Έπειτα, περιγράφηκαν τα ανώνυμα δεδομένα και το Inference Attack, μέσω του οποίου επιτυγχάνεται παραβίαση της ιδιωτικότητας, η νομοθεσία της Ευρωπαϊκής Ένωσης και της Ελλάδας για την προστασία των προσωπικών δεδομένων και οι τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίηση της εφαρμογής.

Στο τρίτο κεφάλαιο, παρουσιάστηκαν οι απαιτήσεις για την εγκατάσταση της εφαρμογής καθώς και τα απαραίτητα αρχεία και λογισμικά. Έπειτα, περιγράφηκε η ανάλυση της εφαρμογής τόσο σε επίπεδο αρχιτεκτονικής όσο και σε λογισμικού, δίνοντας έμφαση στην επιλογή μεταβλητής (Attribute Selector), στην πιθανότητα Bayes(Rule of Bayes), στην εμφάνιση αποτελεσμάτων(Results) και στην αναφορά(Report).

Στο τέταρτο κεφάλαιο, παρουσιάστηκε η υλοποίηση της εφαρμογής “IB Privacy Advisor App”. Πιο συγκεκριμένα, περιγράφηκε βήμα-βήμα και με την χρήση εικόνων(screenshots) η εγκατάσταση των απαραίτητων λογισμικών και αρχείων, παρουσιάστηκε το UML διάγραμμα των κλάσεων της εφαρμογής, ο κώδικας της βάσης δεδομένων σε SQL καθώς και ο απαραίτητος κώδικας σε java για την σύνδεση τους. Επιπλέον, παρουσιάστηκαν τα βήματα για την ορθή λειτουργία του Apache Netbeans IDE, του xampp, του localhost/phpMyAdmin καθώς και της αυτοματοποιημένη αναφοράς(Jasper Report - iReport) μαζί με το format της.

Στο πέμπτο κεφάλαιο, παρουσιάστηκε η λειτουργικότητα της εφαρμογής “IB Privacy Advisor App” με χρήση εικόνων καθώς και με την κατάλληλη λεκτική περιγραφή, ώστε να είναι κατανοητή η λειτουργία της.
Η εφαρμογή “IB Privacy Advisor App” είναι ικανή να εγκατασταθεί σε οποιονδήποτε server, αρκεί πρώτα να εγκατασταθούν τα απαραίτητα αρχεία και λογισμικά και να πραγματοποιηθούν οι απαραίτητες ρυθμίσεις σε αυτά. Στην συνέχεια, πρέπει να γίνει import στον localhost η βάση δεδομένων και στο Apache Netbeans IDE το αρχείο σε κώδικα java. Έπειτα, αφού ο χρήστης κάνει clean and build και μετά run το αρχείο της εφαρμογής πρέπει να προσθέσει το όνομα της βάσης δεδομένων που έκανε import προηγουμένως στην “*Σελίδα Προσθήκης Βάσης Δεδομένων”*. Τέλος, επιλέγει την μεταβλητή (attribute) που επιθυμεί να μάθει την πιθανότητα επίθεσης σε αυτή και ανακατευθύνεται στην “*Σελίδα Αποτελεσμάτων*”, έχοντας την δυνατότητα να κατεβάσει ή και να εκτυπώσει την αναφορά (Report).

6.2 Μελλοντικές Επεκτάσεις

Το αντικείμενο αυτής της εργασίας, δηλαδή η ανάπτυξη μίας εφαρμογής που υπολογίζει την πιθανότητα επίθεσης στα προσωπικά δεδομένα του χρήστη και δημιουργεί αυτοματοποιημένη αναφορά με τα αποτελέσματα της, γίνεται να δεχτεί περαιτέρω ανάπτυξη, βελτίωση και έρευνα.

Μία από τις βελτιώσεις που μπορούν να γίνουν στην εφαρμογή είναι η χρήση τεχνικών ανίχνευσης κινδύνων απορρήτου από πληροφορίες για την υλοποίηση ενός ευφυούς συστήματος χρησιμοποιώντας Machine Learning. Επιπλέον, μπορεί να δοθεί η άδεια στον χρήστη να καθορίσει πολιτικές για τα προσωπικά του δεδομένα, τις οποίες η εφαρμογή μπορεί να χρησιμοποιεί αυτόματα για να εκτιμήσει τον πιθανότητα επίθεσης προσαρμοσμένη στον συγκεκριμένο χρήστη. Τέλος, η εφαρμογή αυτή μπορεί να υλοποιηθεί ως web application για χρήση στο ηλεκτρονικό εμπόριο (e-shop) με αμφότερο σκοπό τόσο την προστασία των πελατών όσο και της επιχείρησης για την εφαρμογή και την απόδειξη της προστασίας των προσωπικών δεδομένων, δίνοντας στον καταναλωτή την βεβαιότητα που επιθυμεί ώστε να δώσει τα προσωπικά του δεδομένα με ασφάλεια και για να χρησιμοποιηθούν ορθά από την αντίστοιχη επιχείρηση.

Βιβλιογραφία

[1] pQUANT: A User-centered Privacy Risk Analysis Framework Welderufael B. Tesfay, Dimitra Nastouli, Yannis C. Stamatiou, and Jetzabel M. Serna.

[2] 28. Solove Daniel J. , “A taxonomy of Privacy”, University of Pensylvania, 2006.

[3] S.D. Warren and L.D. Brandeis, “The Right to Privacy”, Harvard Law Review, 1890.

[4] 4. A.F. Westin, The right to Privacy, Antheneum, 1967.

[5] R.O. Mason, “Four Ethical Issues of the Information Age” MIS Quarterly, 1986 and D. O'Neil, “Analysis of Internet Users’ Level ofOnline Privacy Concerns”, Social Science Computer Review, 2001.

[6] ‘Τι είναι τα δεδομένα προσωπικού χαρακτήρα’; *Ευρωπαϊκή Επιτροπή - European Commission*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el.

[7] Solove Daniel J. , “A taxonomy of Privacy”, University of Pensylvania, 2006.

[8] ‘Δούρειος Ίππος (υπολογιστές)’. Βικιπαίδεια. Wikipedia, https://el.wikipedia.org/w/index.php?title=%CE%94%CE%BF%CF%8D%CF%81%CE%B5%CE%B9%CE%BF%CF%82_%CE%8A%CF%80%CF%80%CE%BF%CF%82_(%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AD%CF%82)&oldid=8228934.

[9] K.M. Goertzel., “Malware” Information Assurance Tools Online Report, September 2009.

[10] Χ. Καλλονιάτης, «Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας», Σημειώσεις μαθήματος, Πανεπιστήμιο Αιγαίου.

[11] ‘Κρυπτογραφία’. *Βικιπαίδεια*, 4 Απρίλιος 2020. *Wikipedia*, https://el.wikipedia.org/w/index.php?title=%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1&oldid=8156273.

[12] ‘*K*-Anonymity’. *Wikipedia*, 15 Σεπτέμβριος 2020. *Wikipedia*, https://en.wikipedia.org/w/index.php?title=K-anonymity&oldid=978515436.

[13] Testing the robustness of anonymization techniques: acceptable versus unacceptable inferences - Draft Version Gergely Acs, Claude Castelluccia, Daniel Le Metayer.
[14] Inference Attack'. *Wikipedia*, 17 Μάρτιος 2020. *Wikipedia*, https://en.wikipedia.org/w/index.php?title=Inference_attack&oldid=946060450.

[15] 'Προστασία δεδομένων στην ΕΕ'. *Ευρωπαϊκή Επιτροπή - European Commission*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

[16] 'Τι είναι η παραβίαση δεδομένων και τι πρέπει να κάνουμε σε περίπτωση παραβίασης δεδομένων'; *Ευρωπαϊκή Επιτροπή - European Commission*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el.

[17] *ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ - e-nomothesia.gr | Τράπεζα Πληροφοριών Νομοθεσίας*. https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/.

[18] *Introduction to Java*. https://www.w3schools.com/java/java_intro.asp.

[19] 'Java'. *Βικιπαίδεια. Wikipedia*, https://el.wikipedia.org/w/index.php?title=Java&oldid=8452116.

[20] 'SQL'. *Βικιπαίδεια. Wikipedia*, https://el.wikipedia.org/w/index.php?title=SQL&oldid=8189922.

[21]*SQL Introduction*. https://www.w3schools.com/sql/sql_intro.asp.

[22] *NetBeans IDE - Overview*. https://netbeans.org/features/index.html.

[23] *Welcome to Apache NetBeans*. https://netbeans.apache.org/.

[24] *XAMPP Installers and Downloads for Apache Friends*. https://www.apachefriends.org/index.html.

[25] 'Localhost (127.0.0.1)'. *IONOS Digitalguide*, https://www.ionos.com/digitalguide/server/know-how/localhost/.

[26] 'JasperReports Library - Tutorial'. *Jaspersoft Community*, https://community.jaspersoft.com/wiki/jasperreports-library-tutorial.

[27] 'Θεώρημα Μπέυζ'. *Βικιπαίδεια. Wikipedia*, https://el.wikipedia.org/w/index.php?title=%CE%98%CE%B5%CF%8E%CF%81%CE%B7%CE%BC%CE%B1_%CE%9C%CF%80%CE%AD%CF%85%CE%B6&oldid=8441149.