Ατομική Διπλωματική Εργασία

ΥΛΟΠΟΙΗΣΗ ΣΥΣΤΗΜΑΤΟΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

Κυριάκος Γεωργίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Υλοποίηση συστήματος ηλεκτρονικής ψηφοφορίας

Κυριάκος Γεωργίου

Επιβλέπουσα Καθηγήτρια

Δρ. Άννα Φιλίππου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2021

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στην επιβλέπουσα καθηγήτρια μου, κυρία Άννα Φιλίππου που μου έδωσε την ευκαιρία να ασχοληθώ ένα τόσο ενδιαφέρον θέμα. Η καθοδήγηση και καλή διάθεση της ήταν σημαντικοί παράγοντες στης μελέτη μου. Χωρίς τον πολύτιμο της χρόνο και τις συμβουλές της δεν θα μπορούσα να ολοκληρώσω την διπλωματική μου εργασία.

Επίσης, θα ήθελα να ευχαριστήσω την ομάδα ατόμων όπου έλαβαν μέρος στις διάφορες αξιολογήσεις της εφαρμογής μου. Με βοήθησα να ανακαλύψω διάφορα σφάλματα και απροσεξίες που υπήρχαν στην εφαρμογή. Επίσης οι εισηγήσεις τους με βοήθησαν να βελτιώσω την εφαρμογή μου.

Περίληψη

Η ηλεκτρονική ψηφοφορία είναι ένα εργαλείο για την αύξηση της αποδοτικότητας, ασφάλειας και ευκολία ψήφου στην εκλογική διαδικασία. Δυστυχώς, όπως αρκετές τεχνολογικές αναβαθμίσεις, η υλοποίηση της ηλεκτρονικής ψηφοφορίας είναι δύσκολο να πραγματοποιηθεί. Η ηλεκτρονική ψηφοφορία ίσως να είναι μία από τις δυσκολότερες τεχνολογικές αναβαθμίσεις, επειδή επηρεάζει τον πυρήνα της δημοκρατίας ενός κράτους, με συνέπεια η ηλεκτρονική ψηφοφορία να λαμβάνει περισσότερη κριτική και αντίσταση από τις πλείστες τεχνολογικές αλλαγές.

Στην παρούσα διπλωματική εργασία μελετήθηκε σε βάθος το θέμα της ηλεκτρονικής ψηφοφορίας. Αρχικά, μελετήθηκαν γενικές πληροφορίες για την ηλεκτρονική ψηφοφορία. Στην συνέχεια μελετήθηκαν οι πέντε βασικές απαιτήσεις ασφάλειας, δηλαδή η μυστικότητα, η επαληθευσιμότητα, η αυθεντικοποίηση, η ακεραιότητα και η διαθεσιμότητα. Ακόμη, μελετήθηκαν τα θετικά, τα αρνητικά και το μέλλον της ηλεκτρονικής ψηφοφορίας στην Ευρωπαϊκή Ένωση. Επίσης, μελετήθηκαν διάφορες τεχνικές κρυπτογράφησης, όπως τυφλές υπογραφές, ElGamal και ομομορφική κρυπτογράφηση. Επιπλέον, μελετήθηκε το πρωτόκολλο ηλεκτρονικής ψηφοφορίας του Fujioka, Okamoto, Ohta και του Juels, Catalano, Jakobsson. Επιπρόσθετα μελετήθηκαν τα συστήματα ηλεκτρονικής ψηφοφορίας Helios και Voatz.

Ο τελικός στόχος είναι η δημιουργία ενός συστήματος ηλεκτρονικής ψηφοφορίας. Το σύστημα θα αποτελείται από μία android εφαρμογή και τις οντότητες διαχειριστής, μετρητής και κοινό, όπου έχουν το ρόλο των εξυπηρετητών διαδικτύου, με σκοπό τη διεξαγωγή της διαδικασίας των φοιτητικών εκλογών. Έχει ως βασικό στόχο τις 5 απαιτήσεις ασφάλειας ηλεκτρονικής ψηφοφορία. Επιπρόσθετα, ως απαιτήσεις ευχρηστίας ορίστηκαν οι 10 κανόνες ευχρηστίας του Jakob Nielsen. Μέρος της διαδικασίας υλοποίησης είναι οι έλεγχοι της εφαρμογής από πιθανούς χρήστες για την αύξηση της ασφάλειας, μείωση των λαθών και βελτίωση της εμπειρίας του χρήστη. Στο τέλος της διαδικασίας υλοποίησης έχει πραγματοποιηθεί ένας έλεγχος ευχρηστίας βάσει των 10 κανόνων του Jakob Nielsen και ένας έλεγχος βάση των απαιτήσεων ασφάλειας για να αξιολογηθεί σε ποιο βαθμό ικανοποιούνται και ποιοι είναι οι κίνδυνοι όπου παραμένουν.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Υποκίνηση διπλωματική εργασίας

Η ασφάλεια είναι ένας σημαντικός παράγοντας στη καθημερινή ζωή ενός ατόμου. Το ίδιο άτομο, αλλά και η ίδια η κοινωνία έχει διάφορους μεθόδους ώστε να διατηρεί την ασφάλεια τους. Για παράδειγμα ένα άτομο κλειδώνει την πόρτα του σπιτιού του για να προστατευτεί από ανεπιθύμητους επισκέπτες, μία πόλη έχει τον αστυνομικό της σταθμό για να σταματήσει τις κακόβουλες ενέργειες από ύπουλα άτομα στο εσωτερικό της πόλης και μία χώρα έχει το στρατό της για να προστατέψει την εδαφική της ακεραιότητα. Η ασφάλεια επιτρέπει σε ένα άτομο να ζήσει ελεύθερα τη ζωή του, χωρίς φόβο ή άγχος από τους διάφορους κινδύνους που κρύβονται μέσα στη καθημερινότητα.

Εκτός από τη φυσική ζωή, ένα άτομο έχει τη ψηφιακή του ζωή, δηλαδή τη συμπεριφορά του στο διαδίκτυο. Η ασφάλεια στο διαδίκτυο είναι εξίσου σημαντική με την ασφάλεια στην φυσική ζωή. Η προστασία των προσωπικών δεδομένων ενός ανθρώπου είναι μία μορφή ασφάλειας στο διαδίκτυο, επειδή προστατεύει την ταυτότητα του από ύπουλα άτομα που θα ήθελα να την χρησιμοποιήσουν για το δικό τους κέρδος. Η προστασία προσωπικών δεδομένων είναι τόσο σημαντική με αποτέλεσμα η Ευρωπαϊκή Ένωση να έχει δημιουργήσει διάφορους νόμους, ένας από αυτούς είναι οι γενικοί κανονισμοί προστασία δεδομένων (GDPR) [29].

Ένα από τα πιο σημαντικά δικαιώματα που έχει ένας πολίτης σε μία δημοκρατική χώρα είναι το δικαίωμα ψήφου. Όπως στις υπόλοιπες πτυχές της ζωής του, ένα άτομο αναμένει να έχει την δυνατότητα να ψηφίσει το άτομο που επιθυμεί με ασφάλεια, χωρίς κίνδυνο ή φόβο στη

ζωή του. Στο παραδοσιακό τρόπο ψηφοφορίας, κάποιο άτομο μπορεί να πάει στο εκλογικό κέντρο που του αναλογεί, με ένα απλό τρόπο να αποδείξει ότι έχει το δικαίωμα να ψηφήσει, όπως δείχνοντας την ταυτότητα του, και να καταχωρήσει τη μυστική του ψήφο. Είναι λογικό ο ψηφοφόρος να αναμένει παρόμοια ασφάλεια στις διαδικασίες ηλεκτρονικής ψηφοφορίας.

Ο ηλεκτρονικός τρόπος ψηφοφορία διαφέρει από τον παραδοσιακό. Η ηλεκτρονική ψηφοφορία έχει τα δικά της οφέλη, αλλά έχει και τα δικά της μειονεκτήματα. Επίσης, έχει τις δικές τις προκλήσεις και κινδύνους που είναι απαραίτητο να ξεπεράσει. Ακόμη, χρησιμοποιεί διαφορετικές μεθόδους για να αντιμετωπίσει τα ίδια προβλήματα με την παραδοσιακή ψηφοφορία. Η επίτευξη ασφάλειας σε ένα σύστημα ηλεκτρονικής ψηφοφορίας είναι ένα προκλητικό πρόβλημα, όπου αν δεν λυθεί, τότε δεν θα είναι δυνατό να αντικαταστήσει τις παραδοσιακές μεθόδους.

Η ηλεκτρονική ψηφοφορία είναι ένα θέμα που με ενδιαφέρει πολύ. Αρκετές πτυχές της ζωής ενός ατόμου μεταφέρονται στον ψηφιακό κόσμο για τη διευκόλυνση του αλλά η ψηφοφορία παραμένει σταθερή. Οι διάφορες προκλήσεις που απαιτεί να αντιμετωπίσει η ηλεκτρονική ψηφοφορία για να αντικαταστήσει τον παραδοσιακό τρόπο με υποκίνησαν να ασχοληθώ μαζί της. Έτσι μέσα από τη διπλωματική μου εργασία έχω αποκτήσει σημαντικές για την ηλεκτρονική ψηφοφορία, τις προκλήσεις που υπάρχουν και διάφορα πρωτόκολλα ή συστήματα ηλεκτρονικής ψηφοφορίας όπου αντιμετωπίζουν κάποιες από τις προκλήσεις. Στο τέλος, έχω εφαρμόσει όσα είχα μάθει για να αναπτύξω το δικό μου σύστημα ηλεκτρονικής ψηφοφορίας, το οποίο μπορεί να χρησιμοποιηθεί σε πραγματικές εκλογές.

1.2 Στόχοι Διπλωματικής εργασίας

Η διπλωματική μου εργασία έχει στόχο την μελέτη και υλοποίηση συστήματος ηλεκτρονικής ψηφοφορίας. Πιο συγκεκριμένα, η μελέτη θα επικεντρωθεί στις απαιτήσεις ασφάλειας των συστημάτων ηλεκτρονικής ψηφοφορίας. Οι βασικές απαιτήσεις ασφάλειας είναι η μυστικότητα, η επαληθευσιμότητα, η αυθεντικοποίηση, η ακεραιότητα και η διαθεσιμότητα [20][30]. Η μυστικότητα είναι η απουσία συνδέσμου μεταξύ ψηφοφόρου και ψηφοδελτίου. Η επαληθευσιμότητα είναι δυνατότητα του ψηφοφόρου να ελέγχει την κατάσταση της ψήφος του, δηλαδή αν υπάρχει στο σύστημα ή αν μετρήθηκε. Η αυθεντικοποίηση είναι ο έλεγχος του κάθε χρήστη για να επικυρωθεί ότι είναι έγκυρος ψηφοφόρος. Η ακεραιότητα αφορά το τελικό αποτέλεσμα, δηλαδή είναι ο έλεγχος ότι το τελικό αποτέλεσμα είναι δίκαιο και ορθό. Η διαθεσιμότητα είναι η ικανότητα του

συστήματος να είναι προσβάσιμο από όλους τους εξουσιοδοτημένους χρήστες, όταν οι ίδιοι το αιτούνται.

Ο τελικός στόχος είναι η δημιουργία ενός συστήματος ηλεκτρονικής ψηφοφορίας. Πιο συγκεκριμένα είναι μία android εφαρμογή με στόχο τη διεξαγωγή της διαδικασίας των φοιτητικών εκλογών. Η εφαρμογή έχει ως βασική απαίτηση την μυστικότητα του χρήστη, αλλά όλες οι απαιτήσεις ασφάλειας έχουν ικανοποιηθούν. Επίσης, έχει ως απαιτήσεις ευχρηστίας τους 10 κανόνες ευχρηστίας του Jakob Nielsen. Το σύστημα δεν βασίζεται σε κάποιο υπαρκτό πρωτόκολλο αλλά έχει δημιουργηθεί ένα νέο πρωτόκολλο μέσα από την μελέτη υφιστάμενων πρωτοκόλλων και συστημάτων.

1.3 Δομή Εργασίας

Η εργασία αποτελείται από ακόμη πέντε κεφάλαια ως εξής.

Στο δεύτερο κεφάλαιο θα παρουσιαστούν πληροφορίες για την ηλεκτρονική ψηφοφορία. Αρχικά θα γίνει μια γενική αναφορά για τα συστήματα ηλεκτρονικής ψηφοφορίας. Ακολούθως, θα αναλυθούν οι πέντε απαιτήσεις ασφάλειας, οι οποίες είναι η μυστικότητα, η επαληθευσιμότητα, η αυθεντικοποίηση , η ακεραιότητα και η διαθεσιμότητα. Μετά θα αναφερθούν τα θετικά και τα αρνητικά της ηλεκτρονικής ψηφοφορίας. Στο τέλος θα αναφερθεί το μέλλον της ηλεκτρονικής ψηφοφορίας στην Ευρωπαϊκή Ένωση.

Στο τρίτο κεφάλαιο θα παρουσιαστούν δύο πρωτόκολλα ηλεκτρονικής ψηφοφορίας και δύο συστήματα ηλεκτρονικής ψηφοφορίας. Αρχικά θα αναφερθεί το πρωτόκολλο των Fujioka, Okamoto, Ohta το οποίο έχει ως βασικό στόχο την μυστικότητα της ψήφου και του ψηφοφόρου [1]. Μετά θα αναφερθεί το πρωτόκολλο των Juels, Catalano, Jakobsson το οποίο έχει ως βασικό στόχο να καταπολεμήσει τον εξαναγκασμό του ψηφοφόρου να ψηφίσει κάποιο υποψήφιο που δεν θέλει [19]. Στη συνέχεια θα αναφερθεί το σύστημα ηλεκτρονικής ψηφοφορίας Helios, που είναι ένα σύστημα διαδικτυακής ψηφοφορίας μέσω ενός πλοηγού και προσφέρει διάφορους τρόπους επαλήθευσης [17]. Στο τέλος θα αναφερθεί το Voatz, το οποίο είναι ένα διαδικτυακό σύστημα ψηφοφορίας για τα κινητά τηλέφωνα, με στόχο τη ασφάλεια, προσβασιμότητα, διαθεσιμότητα και ευκολία χρήσης [7].

Στο τέταρτο κεφάλαιο θα παρουσιαστούν οι προδιαγραφές του συστήματος ηλεκτρονικής ψηφοφορίας που έχω δημιουργήσει. Αρχικά θα γίνει μία σύντομη περιγραφή του συστήματος και των τυπικών χρηστών. Στη συνέχεια θα αναφερθεί η μέθοδος σχεδίασης που

ακολούθησα κατά την ανάπτυξη τους συστήματος και τα εργαλεία που χρησιμοποίησα. Ακολούθως, θα αναφερθούν οι απαιτήσεις του συστήματος που προέκυψαν από την συνέντευξη και ερωτηματολόγιο που δημιούργησα, καθώς και τα αποτελέσματα του ερωτηματολογίου. Μετά θα αναλυθεί οι οντότητες (βάσεις δεδομένων) και το πρωτόκολλο ψηφοφορίας που ακολουθεί η εφαρμογή. Στο τέλος θα αναλυθούν οι βασικές λειτουργίες της android εφαρμογής και θα παρουσιαστούν εικόνες που δείχνουν την εμφάνιση αυτών των λειτουργιών.

Στο πέμπτο κεφάλαιο θα αναλυθούν οι αξιολογήσεις που πραγματοποιήθηκαν στο σύστημα. Αρχικά πραγματοποιήθηκαν τρεις αξιολογήσεις στα πρωτότυπα του συστήματος κατά τη διάρκεια της ανάπτυξης τους. Ο σκοπός των αξιολογήσεων ήταν η ανίχνευση και διόρθωση των προβλημάτων που υπάρχουν στη εφαρμογή. Επίσης, έγινε μία αξιολόγηση ευχρηστίας βάσει των 10 κανόνων ευχρηστίας του Jakob Nielsen. Στο τέλος έγινε μία ολική αξιολόγηση στο τελικό σύστημα. Ο κύριος στόχος της τελικής αξιολόγησης είναι να εξεταστεί αν το σύστημα ικανοποιεί τις απαιτήσεις ασφάλειας των συστημάτων ηλεκτρονικής ψηφοφορίας. Επίσης, υπάρχει μία σύγκριση του συστήματος που έχει υλοποιηθεί με το σύστημα διαδικτυακής ψηφοφορίας της Εσθονίας.

Στο έκτο κεφάλαιο θα αναφερθούν τα συμπεράσματα και εισηγήσεις για μελλοντικές επεκτάσεις.

Κεφάλαιο 2

Ηλεκτρονική Ψηφοφορία

2.1 Συστήματα ηλεκτρονικής ψηφοφορίας

Στο κεφάλαιο 2 θα γίνει μία γενική ανασκόπηση των συστημάτων ηλεκτρονικής ψηφοφορίας. Θα οριστεί ο όρος των συστημάτων ηλεκτρονικής ψηφοφορίας και θα αναφερθούν κάποιες γενικές πληροφορίες για αυτά τα συστήματα. Επιπρόσθετα, θα αναφερθούν οι απαιτήσεις ασφάλειας, τα θετικά και αρνητικά των συστημάτων ηλεκτρονικής ψηφοφορίας. Στο τέλος, θα συζητηθεί το μέλλον της ηλεκτρονικής ψηφοφορίας στην Ευρώπη.

Ο όρος των συστημάτων ηλεκτρονική ψηφοφορίας είναι πολύ γενικός. Αν κάποιο σύστημα περιλαμβάνει τεχνολογίες της πληροφορικής για την καταγραφή ή και καταμέτρηση των ψήφων, τότε είναι ένα σύστημα ηλεκτρονικής ψηφοφορίας. Αυτό συνεπάγεται ότι υπάρχουν διάφορα είδη συστημάτων όπως τη μηχανή ηλεκτρονικής ψηφοφορίας άμεσης καταγραφής οι οποίες είναι μηχανές παρόμοιες με υπολογιστές όπου γίνεται η ψηφοφορία στα εκλογικά κέντρα, μέχρι πλήρης ηλεκτρονική ψηφοφορία από το σπίτι μέσω ηλεκτρονικών συσκευών όπως κινητά και ηλεκτρονικό υπολογιστής [30].

Η ηλεκτρονική ψηφοφορία χρησιμοποιείται από αρκετές δημοκρατίες σε όλο το κόσμο. Κάποια παραδείγματα κρατών όπου χρησιμοποιούν πετυχημένα την ηλεκτρονική ψηφοφορία σε κάποιο βαθμό είναι η Εσθονία και οι Ηνωμένες Πολιτείες Αμερικής. Αρκετές άλλες χώρες πειραματίζονται με συστήματα ηλεκτρονική ψηφοφορίας. Η εισαγωγή της τεχνολογίας της πληροφορικής στις εκλογές είναι μία δύσκολη διαδικασία και απαιτεί

αρκετό χρόνο και δοκιμές. Παρόλα αυτά, πολλές χώρες επιμένουν λόγω ότι η ηλεκτρονική ψηφοφορία θεωρείται σαν ένα εργαλείο προόδου της δημοκρατίας και αύξησης της αξιοπιστίας, εμπιστοσύνης και αποδοτικότητας στις εκλογές [30].

Δυστυχώς, όχι όλα τα κράτη κατάφεραν να εισάγουν αποδοτικά και αξιόπιστα συστήματα ηλεκτρονικής ψηφοφορίας στην εκλογική τους διαδικασία. Η τεχνολογία αυτών των συστημάτων είναι νέα και όχι εξελιγμένη στο επίπεδο όπου δεν υπάρχουν προβλήματα. Επίσης υπάρχουν διάφορες προκλήσεις που κάνουν την εισαγωγή των συστημάτων αδύνατη, όπως νομικές, οικονομικές και κοινωνικές. Κάποιες χώρες που προσπάθησαν αλλά απέτυχαν να ξεπεράσουν τις προκλήσεις είναι Γερμανία, Ελβετία, Ιρλανδία, και Κάτω Χώρες [30].

2.2 Απαιτήσεις Ασφάλειας Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Σε αυτό το υποκεφάλαιο θα αναφερθούν οι απαιτήσεις των συστημάτων της ηλεκτρονική ψηφοφορίας, οι οποίες είναι απαραίτητες για μία δίκαιη ψηφοφορία. Αυτές οι απαιτήσεις λαμβάνουν υπόψη παράγοντες όπως αναξιόπιστες αρχές, αναξιόπιστους ψηφοφόρους και τυχόν λάθη στο σύστημα. Οι βασικές απαιτήσεις είναι η μυστικότητα, η επαληθευσιμότητα, η αυθεντικοποίηση , η ακεραιότητα και η διαθεσιμότητα [6][14][20][30].

Η πρώτη απαίτηση είναι η μυστικότητα, η οποία είναι η κεντρική απαίτηση σε όλα τα συστήματα ηλεκτρονικής ψηφοφορίας. Σε κάθε περίπτωση η ψήφος δεν πρέπει να συνδέεται με τον ψηφοφόρο. Επίσης τα προσωπικά στοιχεία και η ψήφος του χρήστη πρέπει να είναι κρυφά και να είναι γνωστά μόνο όταν είναι αναγκαίο στη διαδικασία ψηφοφορίας. Αυτό είναι απαραίτητο για να προστατευθεί ο ψηφοφόρος από κακοήθεις εξουσίες του συστήματος ή το κακοήθες κοινό όπου θέλει να εξαναγκάσει τον ψηφοφόρο να ψηφίσει με βάση τις δικές του πολιτικές απόψεις. Επίσης, η μυστικότητα μαζί με τη δυνατότητα του ψηφοφόρο να ψηφίσει πάνω από μια φορά αποτρέπει τον ψηφοφόρο από το πουλάει την ψήφο του, αφού δεν θα μπορεί να αποδείξει σε ένα τρίτο άτομο ότι δεν θα αλλάξει τη ψήφο του. Στις περισσότερες δημοκρατικές χώρες η μυστικότητα στην εκλογική διαδικασία είναι νομική υποχρέωση, έτσι το παραδοσιακό σύστημα ψηφοφορίας προσφέρει μεγάλο βαθμό μυστικότητας και αναμένεται ότι και τα ηλεκτρονικά συστήματα θα προσφέρουν το ίδιο ή μεγαλύτερο βαθμό.

Η δεύτερη απαίτηση είναι η επαληθευσιμότητα της ψήφου μετά την ψηφοφορία. Ο ψηφοφόρος πρέπει να έχει τη δυνατότητα να ελέγχει την κατάσταση της ψήφου του, δηλαδή αν η ψήφος του είναι ακέραια, δεν διαγράφηκε ή άλλαξε, και αν μετρήθηκε κατά τη

διαδικασία καταμέτρησης των ψήφων. Αυτό συνεπάγεται ότι το σύστημα ή η εξουσία δεν θα μπορούν να διαγράφουν ή αλλάζουν ψήφους με σκοπό να αλλάξουν το τελικό αποτέλεσμα. Επίσης, η επαληθευσιμότητα αυξάνει την εμπιστοσύνη των ψηφοφόρων στο σύστημα και στο τελικό αποτέλεσμα. Χωρίς ένα αξιόπιστο και αναμφισβήτητο τρόπο επαληθευσιμότητας, το τελικό αποτέλεσμα μπορεί να είναι δίκαιο αλλά το κοινό ίσως να μην το αποδέχεται.

Η τρίτη απαίτηση είναι η αυθεντικοποίηση του ψηφοφόρου. Κάθε ψηφοφόρος, πριν τη διαδικασία της ψηφοφορίας, πρέπει να ελέγχεται αν δικαιούται να ψηφίσει. Επιπλέον, πρέπει να υπάρχει έλεγχος για να αποτρέπει τις πολλαπλές ψήφους από το ίδιο άτομο. Ακόμη, η αυθεντικοποίηση πρέπει να αποτρέπει κακόβουλα άτομα να ψηφίσουν στην θέση άλλων ψηφοφόρων παραποιώντας το τελικό αποτέλεσμα. Τα κακόβουλα άτομα μπορεί να είναι η ίδια η κυβέρνηση ή ξένες κυβερνήσεις, οι οποίες διαθέτουν μεγάλο αριθμό πόρων, έτσι η αυθεντικοποίηση πρέπει να είναι αδύνατο να νικηθεί.

Η τέταρτη απαίτηση είναι η ακεραιότητα του συστήματος και των αποτελεσμάτων της ψηφοφορίας. Δεν πρέπει να υπάρχει η δυνατότητα σε αναξιόπιστες αρχές να προσθέτουν μη έγκυρες ψήφους και να παραποιήσουν ή να διαγράψουν έγκυρες ψήφους. Επιπρόσθετα, δεν πρέπει να υπάρχει κάποιο πρόβλημα στο σύστημα, το οποίο να εμποδίζει την επιτυχή διαδικασία ψηφοφορίας, για παράδειγμα να διαγράφονται ψήφοι ή να δημιουργούνται αντίγραφα ψήφων. Το τελικό αποτέλεσμα της ψηφοφορίας πρέπει να είναι το δίκαιο αποτέλεσμα, δηλαδή μόνο οι πραγματικοί ψήφοι πρέπει να καταμετρηθούν.

Η πέμπτη απαίτηση είναι η διαθεσιμότητα του συστήματος ηλεκτρονικής ψηφοφορίας. Κατά την περίοδο της ψηφοφορίας το σύστημα πρέπει είναι προσβάσιμο από όλους τους εξουσιοδοτημένους χρήστες. Ο χρήστης πρέπει να έχει τη δυνατότητα να ψηφίσει γρήγορα και χωρίς καθυστερήσεις. Η διακοπής της διαθεσιμότητας του συστήματος, έστω για ένα μικρό χρονικό διάστημα, μπορεί να προκαλέσει αρνητικά συναισθήματα στον ψηφοφόρο σε μεγάλο βαθμό. Με αποτέλεσμα ο ψηφοφόρος να νιώθει απογοήτευση και να μειωθεί η εμπιστοσύνη του στο σύστημα ηλεκτρονικής ψηφοφορίας. Επίσης, κάποιοι ψηφοφόροι μπορεί να μην ψηφίσουν καθόλου ή μην ξαναχρησιμοποιήσουν το σύστημα ηλεκτρονικής ψηφοφορίας.

2.3 Θετικά Ηλεκτρονικής Ψηφοφορίας

Σε αυτό το υποκεφάλαιο, θα γίνει μια αναφορά των πλεονεκτημάτων που προκύπτουν από την ηλεκτρονική ψηφοφορία. Τα πλεονεκτήματα αυτά θα εξηγηθούν μέσα από τη σύγκριση

της ηλεκτρονικής και παραδοσιακής ψηφοφορίας. Θα αναφερθούν μόνο τα τέσσερα πιο σημαντικά πλεονεκτήματα [11][30].

Το πρώτο πλεονέκτημα είναι η πιο γρήγορη και ακριβής μέτρηση των ψήφων στα ηλεκτρονικά συστήματα ψηφοφορίας. Στο παραδοσιακό σύστημα ψηφοφορίας οι ψήφοι μετρούνται χειρωνακτικά από ανθρώπους. Η χειρωνακτική μέτρηση είναι χρονοβόρα, κουραστική, και μπορεί να οδηγήσει σε ανθρώπινα λάθη κατά τη μέτρηση. Επιπρόσθετα, η χειρωνακτική μέτρηση ξεκινά στο τέλος της διαδικασίας της ψηφοφορίας. Αντίθετα, στα ηλεκτρονικά συστήματα ψηφοφορίας η μέτρηση μπορεί να γίνεται κατά την διάρκεια της ψηφοφορίας, είναι πολύ πιο γρήγορη αφού γίνεται από μηχανές και αν η ψήφος καταχωρήθηκε τότε σίγουρα θα μετρηθεί.

Το δεύτερο πλεονέκτημα είναι η μείωση των μη έγκυρων ψηφοδελτίων. Στο παραδοσιακό σύστημα ψηφοφορίας, δεν υπάρχει κάποιος άνθρωπος να ελέγχει την εγκυρότητα του ψηφοδελτίου αφού αυτό θα παραβίαζε τη μυστικότητα της ψήφου. Με συνέπεια, τα λάθη που γίνονται στα ψηφοδέλτια να μην αναγνωρίζονται έγκαιρα και να «χάνονται» οι ψήφοι των ατόμων. Αντίθετα, η διεπαφή χρήστη των ηλεκτρονικών συστημάτων ψηφοφορίας θα προειδοποιεί τον χρήστη για μη έγκυρο ψηφοδέλτιο και θα δίνει οδηγίες ώστε το ψηφοδέλτιο να γίνει έγκυρο, μειώνονται σε μεγάλο βαθμό, αν όχι πλήρως, τα μη έγκυρα ψηφοδέλτια.

Το τρίτο πλεονέκτημα είναι η μακρόχρονη μείωση του κόστους στην διαδικασίας ψηφοφορίας. Στο παραδοσιακό σύστημα ψηφοφορίας, πρέπει να τυπώνονται χάρτινα ψηφοδέλτια και να μεταφέρονται σε όλους τους εκλογικούς σταθμούς, σε όλη τη χώρα. Επίσης, η διαδικασία ψηφοφορίας απαιτεί αρκετό ανθρώπινο δυναμικό για να διεκπεραιωθεί. Αντίθετα, τα περισσότερα ηλεκτρονικά συστήματα ψηφοφορίας χρειάζονται λίγο χαρτί για μορφή απόδειξης ψηφοφορίας ή δεν χρειάζονται καθόλου χαρτί. Επίσης, χρειάζονται πολύ λίγο προσωπικό για όλη την διαδικασία ψηφοφορίας. Δεν υπάρχει ανάγκη προσωπικού να ελέγχει αν κάποιο άτομο έχει το δικαίωμα να ψηφήσει ή να μετρήσει τις τελικούς ψήφους.

Το τέταρτο πλεονέκτημα είναι η μείωση της απάτης σε όλη την εκλογική διαδικασία λόγω ανθρώπινης παρέμβασης. Στο παραδοσιακό σύστημα ψηφοφορίας, υπάρχει ανθρώπινη παρέμβαση σε όλη την εκλογική διαδικασία. Αν ένα εκλογικός σταθμός ή περιφέρεια θέλουν να αλλάξουν το αποτέλεσμα παραβιάζοντας τις ψήφους τότε μπορούν να το κάνουν. Αντίθετα, αν ένα ηλεκτρονικό σύστημα ψηφοφορίας πέρασε όλους τους ελέγχους και είναι πραγματικά ασφαλές, τότε θα είναι πολύ δύσκολο να υπάρχει ανθρώπινη απάτη. Αυτό

συμβαίνει λόγω ότι υπάρχει πολύ λίγη ανθρώπινη αλληλεπίδραση με το σύστημα άρα υπάρχουν πολύ λίγες ευκαιρίες για παρέμβαση και απάτη.

2.4 Αρνητικά Ηλεκτρονικής Ψηφοφορίας

Σε αυτό το υποκεφάλαιο, θα γίνει μια αναφορά των μειονεκτημάτων που προκύπτουν από την ηλεκτρονική ψηφοφορία. Τα μειονεκτήματα αυτά θα εξηγηθούν με παρόμοιο τρόπο όπως τα πλεονεκτήματα στο προηγούμενο υποκεφάλαιο, δηλαδή μέσα από την σύγκριση της ηλεκτρονικής και παραδοσιακής ψηφοφορίας. Θα αναφερθούν μόνο τα τέσσερα, πιο σημαντικά μειονεκτήματα [12][30].

Το πρώτο μειονέκτημα είναι η έλλειψη διαφάνειας του ηλεκτρονικού συστήματος ψηφοφορίας. Ο παραδοσιακός τρόπος ψηφοφορίας υπάρχει για αρκετά χρόνια, ο τρόπος διεξαγωγής τους είναι γνωστός και σε κάθε εκλογική διαδικασία ελέγχεται από πολλά άτομα. Αυτό έχει κερδίσει την εμπιστοσύνης της κοινωνίας λόγω της μεγάλης διαφάνειας του. Αντίθετα, η ηλεκτρονική ψηφοφορία είναι σαν ένα μαύρο κουτί, δεν υπάρχει καθόλου διαφάνεια προς τον τρόπο λειτουργίας της. Ο περισσότερος πληθυσμός δεν γνωρίζει πως λειτουργεί όλο το σύστημα λόγω της πολυπλοκότητας του. Σαν αποτέλεσμα, η κοινωνία δεν εμπιστεύεται το αποτέλεσμα της ψηφοφορίας, ανεξάρτητα αν το σύστημα είναι απόλυτα ασφαλές, χωρίς περιθώριο απάτης και το αποτέλεσμα είναι νόμιμο.

Το δεύτερο μειονέκτημα είναι η απάτη από τους δημιουργούς ή τους χειριστές του συστήματος. Στα παραδοσιακά συστήματα ψηφοφορίας υπάρχει μεγάλος αριθμός ανθρώπινης αλληλεπίδρασης. Για να γίνει κάποια απάτη η οποία θα αλλάξει το αποτέλεσμα της ψηφοφορίας, τότε πρέπει να εξαγοραστούν πολλοί άνθρωποι, το οποίο αυξάνει τον κίνδυνο ανακάλυψης της απάτης. Επίσης, ο παραδοσιακός τρόπος υπάρχει για αρκετά χρόνια και διάφοροι τρόποι απάτης δοκιμάστηκαν και αντιμετωπίστηκαν. Αντιθέτως, τα ηλεκτρονικά συστήματα ψηφοφορίας δημιουργήθηκαν και διαχειρίζονται από μια μικρή ομάδα ατόμων. Αυτά τα άτομα έχουν τα δικαιώματα να κάνουν όποιες αλλαγές θέλουν στο σύστημα, άρα εύκολα νοθεύουν τα αποτελέσματα. Επίσης, είναι ένα δύσκολο πρόβλημα η δημιουργία ενός συστήματος ηλεκτρονικής ψηφοφορίας που τηρεί όλες τις απαιτήσεις ασφάλειας και ακόμη πιο δύσκολο πρόβλημα η εύρεση των αδυναμιών του.

Το τρίτο μειονέκτημα είναι η μεγάλη περιπλοκότητα και η έλλειψη εκπαίδευσης όσο αφορά τα ηλεκτρονικά συστήματα. Τα παραδοσιακά συστήματα ψηφοφορίας είναι πολύ απλά προς τον ψηφοφόρο. Ο ψηφοφόρος δείχνει την ταυτότητα του στον ελεγκτή, παίρνει το

ψηφοδέλτιο, σημειώνει την επιλογή του το ψηφοδέλτιο και βάζει τη ψήφο στο κουτί. Αντίθετα, τα ηλεκτρονικά συστήματα είναι πιο περίπλοκα επειδή έχουν περισσότερες λειτουργίες. Πιθανόν ο χρήστης θα πρέπει να θυμάται κάποιο κωδικό ή πως να χρησιμοποιήσει κάποιο άλλο αποδεικτικό στοιχείο για να του επιτραπεί να ψηφήσει. Επίσης, άτομα μεγαλύτερης ηλικίας δεν ξέρουν πως να χειρίζονται το πληκτρολόγιο, ποντίκι ή οθόνες αφής για να αλληλοεπιδράσουν με την διεπαφή χρήστη και να ψηφίσουν, με αποτέλεσμα, τα πιο πάνω προβλήματα να είναι σε τέτοιο βαθμό ώστε ο χρήστης να μην μπορεί να ψηφίσει.

Το τέταρτο μειονέκτημα είναι το τεράστιο και συνήθως άγνωστο αρχικό κόστος για την δημιουργία και εγκατάσταση των συστημάτων ηλεκτρονικής ψηφοφορίας. Ο παραδοσιακός τρόπος ψηφοφορίας χρησιμοποιείται για αρκετά χρόνια και έχει ένα γνωστό κόστος. Το κράτος γνωρίζει πως να προετοιμάσει ανάλογα τον προϋπολογισμό του για να καλύψει τα έξοδα. Αντίθετα, το κόστος των ηλεκτρονικών συστημάτων ψηφοφορίας είναι δύσκολο να υπολογισθεί με ακρίβεια. Το κράτος πιθανό να αναγκαστεί να δαπανήσει πολύ περισσότερα χρήματα φέρνοντας σε ρίσκο την οικονομία. Στην χειρότερη περίπτωση μπορεί να αναγκαστεί να ακυρώσει την εγκατάσταση των νέων συστημάτων, δηλαδή πλήρης σπατάλη όλων το χρημάτων που χρειάστηκαν .

2.5 Μέλλον Ηλεκτρονικής Ψηφοφορίας στην Ευρώπη

Σε αυτό το υποκεφάλαιο, θα γίνει μια αναφορά της άποψης της Ευρωπαϊκή Ένωσης για την ηλεκτρονική ψηφοφορία. Υπάρχουν αρκετές ευρωπαϊκές χώρες που προσπάθησαν να εισάγουν συστήματα ηλεκτρονικής ψηφοφορίας με διαφορετικούς βαθμούς επιτυχίας. Τα παραδείγματα που θα αναφερθούν είναι η Εσθονία και η Ελβετία.

Η Ευρωπαϊκή Ένωση έχει επιδείξει ενδιαφέρον στην ηλεκτρονική ψηφοφορία. Η ηλεκτρονική ψηφοφορία για την Ευρωπαϊκή Ένωση είναι ένα μέσο σύνδεσης των πολιτών της με την Ευρωπαϊκή πολιτική. Υπάρχει ένα κύμα ευρωσκεπτικισμού, το οποίο υπονομεύει την εμπιστοσύνη στους Ευρωπαϊκούς θεσμούς και η συμμετοχή στις ευρωπαϊκές εκλογές είναι υπερβολικά χαμηλή. Η Ευρώπη ελπίζει ότι τα πλεονεκτήματα της ηλεκτρονικής ψηφοφορίας θα αυξήσουν τον αριθμό των ψηφοφόρων στις Ευρωπαϊκές εκλογές, με αποτέλεσμα να αυξηθεί η εμπιστοσύνη στην Ευρωπαϊκή Ένωση [25].

Η Εσθονία είναι ένα παράδειγμα επιτυχίας όσο αφορά την ψηφοφορία μέσω διαδικτύου. Η ψηφοφορία μέσω διαδικτύου προσφέρθηκε για πρώτη φορά το 2005 [2]. Αρχικά μόνο ένα

μικρό ποσοστό την χρησιμοποιούσε αλλά το 2019 περίπου το 45% των Εσθονών ψηφοφόρων προτίμησαν την ηλεκτρονική ψηφοφορία. Η Εσθονία τηρούσε κάποιες από τις πιο σημαντικές προϋποθέσεις για την ηλεκτρονική ψηφοφορία, όπως μεγάλα ποσοστά πληθυσμού με γνώση χρήσης ηλεκτρονικών συστημάτων και σύγχρονες υποδομές [8][9]. Κάποια από τα χαρακτηριστικά του συστήματος είναι η δυνατότητα πολλαπλών ψήφων αλλά μόνο η τελευταία ψήφος μετρά, η απλότητα και ταχύτητα στη ψηφοφορία, η δυνατότητα επικύρωσης της ψήφου και το χαμηλό κόστος [9].

Η Ελβετία είναι ένα παράδειγμα σταδιακής και κατανεμημένης εισαγωγής της ψηφοφορίας μέσω διαδικτύου [3]. Η Ελβετία ξεκίνησε την εισαγωγή της διαδικτυακής ψηφοφορίας σε ορισμένες επαρχίες (Γενεύη , Ζυρίχη). Μετά από τις επιτυχημένες προσπάθειες περισσότερες επαρχίες και πολίτες του εξωτερικού μπορούσαν να ψηφίσουν μέσω διαδικτύου. Επίσης υπήρχε ένα όριο για τον αριθμό των διαδικτυακών ψήφων ώστε να περιοριστούν οι ζημίες σε περίπτωση λαθών του συστήματος. Αυτή η σταδιακή και κατανεμημένη εισαγωγή δημιούργησε εμπιστοσύνη προς το σύστημα από τους πολίτες, οι οποίοι ζητούν την πλήρη εισαγωγή της ηλεκτρονικής ψηφοφορίας. Το Ιούνιο 2019 , η Ελβετία απαγόρευσε προσωρινά την ηλεκτρονική ψηφοφορία λόγω των σοβαρών λαθών στον πηγαίο κώδικα των συστημάτων που χρησιμοποιούσε [4] . Υπάρχουν προσπάθειες για την εισαγωγή ενός νέου, πιο ασφαλούς και διαφανής συστήματος ηλεκτρονικής ψηφοφορίας μετά το τέλος του 2023 [18].

Κεφάλαιο 3

Πρωτόκολλα και Συστήματα ηλεκτρονικής ψηφοφορίας

3.1 Εισαγωγή στα πρωτόκολλα και συστήματα ηλεκτρονικής ψηφοφορίας

Το πρόβλημα δημιουργίας κάποιου πρωτοκόλλου ή συστήματος ηλεκτρονικής ψηφοφορίας είναι ένα δύσκολο πρόβλημα λόγω των πολλών απαιτήσεων του. Όπως αναφέρθηκε σε προηγούμενα κεφάλαια οι απαιτήσεις των συστημάτων ηλεκτρονικής ψηφοφορίας δεν συνεργάζονται όλες μεταξύ τους και κάποιες έρχονται σε αντίθεση. Για παράδειγμα ένα πρωτόκολλο μπορεί να έχει στόχο τη πλήρη μυστικότητα του χρήστη με αποτέλεσμα να μην υπάρχει πλήρης δυνατότητα επαλήθευσης.

Σε αυτό το κεφάλαιο θα αναφερθούν 2 πρωτόκολλα και συστήματα ηλεκτρονικής ψηφοφορίας. Τα 2 πρωτόκολλα που θα αναφερθούν είναι το πρωτόκολλο των Fujioka, Okamoto και Ohta και το πρωτόκολλο των Juels, Catalano και Jakobsson. Το πρωτόκολλο των Fujioka, Okamoto και Ohta έχει στόχο τη μυστικότητα του ψηφοφόρου. Το πρωτόκολλο των Juels, Catalano και Jakobsson επιτρέπει στο ψηφοφόρο να αντικαταστήσει τη ψήφο του, με στόχο την καταπολέμηση του εξαναγκασμού του ψηφοφόρου να ψηφίσει κάποιο υποψήφιο που δεν θέλει. Τα 2 συστήματα ηλεκτρονικής πληροφορίας που θα αναφερθούν είναι το Helios και το Voatz. Το Helios είναι ένα γνωστό σύστημα διαδικτυακής ψηφοφορίας όπου έχει μελετηθεί από διάφορους ερευνητές και προσφέρει πλήρης επαλήθευση. Το Voatz, ένα σχετικά νέο σύστημα διαδικτυακής ψηφοφορίας για τα κινητά τηλέφωνα όπου έχει στόχο την ασφάλεια, προσβασιμότητα, διαθεσιμότητα και ευκολία χρήσης.

Επίσης, σε αυτό το υποκεφάλαιο θα γίνει μία σύντομη αναφορά στις τυφλές υπογραφές, ομομορφική κρυπτογράφηση και ElGamal κρυπτογράφηση. Αυτές οι 3 μέθοδοι θα εμφανιστούν στην συνέχεια.

Η ομομορφική κρυπτογράφηση είναι μία ασυμμετρική μέθοδος κρυπτογράφησης όπου επιτρέπει στα δεδομένα να παραμείνουν κρυπτογραφημένα καθώς το σύστημα τα επεξεργάζεται ή τα μεταβάλει [24]. Για παράδειγμα, ένα τρίτος οργανισμός θέλει να επεξεργαστεί τα προσωπικά δεδομένα μιας εταιρίας, η εταιρία όμως δεν θέλει να αποκαλύψει τα δεδομένα της. Με τη χρήση ομομορφική κρυπτογράφησης, η εταιρία δίνει τα κρυπτογραφημένα δεδομένα στον τρίτο οργανισμό, ο τρίτος οργανισμός τα επεξεργάζεται καθώς είναι κρυπτογραφημένα και τα επιστρέφει πίσω. Για να πάρει η εταιρία το αποτέλεσμα και να καταλάβει τη σημασία του πρέπει να αποκρυπτογραφήσει τα επεξεργασμένα δεδομένα.

Επίσης, η ομομορφική κρυπτογράφηση ενισχύει την μυστικότητα στα συστήματα ηλεκτρονικής ψηφοφορίας αφού οι ψήφοι δεν είναι αναγκαίο να αποκρυπτογραφηθούν. Ο κάθε ψήφος είναι σε μία συγκεκριμένη μορφή όπου η ομομορφική κρυπτογράφηση μπορεί να τον επεξεργαστεί. Για παράδειγμα «0» αν δεν ψηφίσθηκε ο υποψήφιος και «1» αν ψηφίσθηκε ο υποψήφιος. Κάθε επιλογή είναι κρυπτογραφημένη, έτσι μία ψήφος θα έχει κρυπτογραφημένα μηνύματα ίσο με τον αριθμό των υποψηφίων. Στο τέλος της εκλογικής διαδικασίας οι κρυπτογραφημένοι ψήφοι μετριόνται, ανά υποψήφιο, ώστε να υπολογιστεί το κρυπτογραφημένο τελικό αποτέλεσμα για κάθε επιλογή. Για να αποκρυπτογραφηθεί το αποτέλεσμα, μια ομάδα από έμπιστα άτομα αποκρυπτογραφούν και δημοσιεύουν το αποτέλεσμα.

Η τυφλή υπογραφή είναι ένα είδος ψηφιακής υπογραφής [22]. Η βασική διαφορά της από τις παραδοσιακές ψηφιακές υπογραφές είναι ότι το περιεχόμενο του μηνύματος γίνεται «τυφλό», δηλαδή μεταμφιέζεται σε κάτι άλλο, πριν να υπογραφτεί. Στην ηλεκτρονική ψηφοφορία οι τυφλές υπογραφές χρησιμοποιούνται κατά την διάρκεια της ψηφοφορίας, όπου η μυστικότητα και η ανωνυμία είναι απαραίτητες.

Ένα παράδειγμα χρήση της τυφλής υπογραφής είναι το ακόλουθο. Ο ψηφοφόρος στέλνει τα προσωπικά του στοιχεία και τη τυφλή υπογραφή της ψήφου στο διαχειριστή. Ο διαχειριστής θα υπογράψει την μόνο αν ο ψηφοφόρος έχει το δικαίωμα να ψηφίσει. Επίσης, ο διαχειριστής δεν γνωρίζει το περιεχόμενο της ψήφου αφού είναι «τυφλό», άρα διατηρείται η μυστικότητα της ψήφου. Στη συνέχεια ο ψηφοφόρος αφαιρεί την δική υπογραφή του και στέλνει την

ψήφο του, χωρίς να είναι «τυφλή», με την υπογραφή του διαχειριστή στο μετρητή. Ο μετρητής ελέγχει την υπογραφή του διαχειριστή για έλεγχο εγκυρότητας του ψηφοδελτίου. Η υπογραφή του διαχειριστή δεν περιέχει προσωπικά στοιχεία του ψηφοφόρου έτσι η ψήφος δεν συνδέεται με τον ψηφοφόρο.

Ο αλγόριθμος του ElGamal είναι ένας ασυμμετρικός αλγόριθμος κρυπτογράφησης [15][16]. Ο αλγόριθμος του ElGamal, όπως και οι υπόλοιποι αλγόριθμοι ασυμμετρικής κρυπτογράφησης χρησιμοποιούν 2 κλειδιά. Στην πιο κάτω εξήγηση του αλγορίθμου θα χρησιμοποιηθεί το παράδειγμα του Ανδρέα και της Άννας για να γίνει πιο κατανοητή. Υποθέτω ότι ο Ανδρέας και Άννα θέλουν να επικοινωνήσουν μεταξύ τους.

Μια απλή εξήγηση για την δημιουργία και ανταλλαγή των κλειδιών είναι η ακόλουθη:

1) Ο Ανδρέας επιλέγει ένα μεγάλο αριθμό (q) και μία κυκλική ομάδα F_q.
2) Από την κυκλική ομάδα F_q, ο Ανδρέας επιλέγει ένα στοιχείο (g) και ένα στοιχείο (a) ώστε a και q να είναι co-primes (gcd(a, q) = 1).
3) Ο Ανδρέας υπολογίζει το $h = g^a$.
4) Το δημόσιο κλειδί είναι το F, $h = g^a$, q , g και το ιδιωτικό κλειδί είναι το a.

Η μέθοδος κρυπτογράφησης του μηνύματος είναι η ακόλουθη:

1) Η Άννα επιλέγει ένα στοιχείο (k) από τη κυκλική ομάδα F ώστε k και q να είναι co-primes (gcd(k, q) = 1).
2) Η Άννα υπολογίζει $p = g^k$ και $s = h^k = g^{ak}$ και πολλαπλασιάζει το s με το μήνυμα.
3) Στο τέλος η Άννα στέλνει $(p, M*s) = (g^k, M*s)$. (M είναι το μήνυμα)

Η μέθοδος αποκρυπτογράφησης του μηνύματος είναι η ακόλουθη:

1) Ο Ανδρέας υπολογίζει το $s' = p^a = g^{ak}$
2) Ο Ανδρέας υπολογίζει το M μέσο M*s/ s'. Το s=s'

Ο Ανδρέας κρατά το ιδιωτικό κλειδί και δίνει το δημόσιο κλειδί στη Άννα. Η Άννα χρησιμοποιεί το δημόσιο κλειδί για να κρυπτογραφήσει το μήνυμα και ο Ανδρέας χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το μήνυμα.

3.3 Fujioka, Okamoto και Ohta πρωτόκολλο

Σε αυτό το υποκεφάλαιο θα αναφερθεί το πρωτόκολλο του Fujioka, Okamoto and Ohta , γνωστό ως FOO πρωτόκολλο [1]. Το πρωτόκολλο αυτό έχει ως βασικό στόχο την

μυστικότητα της ψήφου και του ψηφοφόρου. Τα βασικά μέρη του πρωτοκόλλου, με τη σειρά που εκτελούνται, είναι το στάδιο της προετοιμασίας, το στάδιο της διαχείρισης, το στάδιο της ψηφοφορίας, το στάδιο συλλογής ψήφων, το στάδιο του ανοίγματος και το στάδιο της μέτρησης.

Επίσης, σε αυτό το υποκεφάλαιο χρησιμοποιούνται οι πιο κάτω συμβολισμοί:
V_i : Ψηφοφόρος i
$\xi(v, \kappa)$: Σχέδιο δέσμευσης (bit commitment scheme) για μήνυμα v και κλειδί κ
$\sigma_i(m)$: Σχέδιο υπογραφής ψηφοφόρου i για το μήνυμα m
$\sigma_A(m)$: Σχέδιο υπογραφής διαχειριστή για το μήνυμα m
$\chi_A(m,r)$: Τεχνική τύφλωσης για το μήνυμα m και τυχαίος αριθμός r
$\delta_A(s,r)$: Τεχνική ανάκτησης τυφλής υπογραφής για υπογραφή s και τυχαίος αριθμός r

Το πρώτο στάδιο του πρωτόκολλου είναι η διαδικασία προετοιμασίας. Ο ψηφοφόρος επιλέγει τον υποψήφιο που επιθυμεί στο ηλεκτρονικό ψηφοδέλτιο, δημιουργεί το μήνυμα χρησιμοποιώντας την τεχνική τυφλής κρυπτογράφησης και το στέλνει το διαχειριστή. Πιο αναλυτικά:

1. Ο ψηφοφόρος V_i επιλέγει την ψήφο του v_i και συμπληρώνει το ψηφοδέλτιο του $x_i = \xi(v_i, k_i)$, όπου v_i είναι η ψήφος και το k_i είναι ένα τυχαίο κλειδί.
2. Ο ψηφοφόρος V_i υπολογίζει το κρυπτογραφημένο μήνυμα e_i, όπου περιέχει τη ψήφο, με χρήση τυφλής κρυπτογράφησης, $e_i = \chi(x_i,r_i)$. Το r_i είναι ο παράγοντας τύφλωσης.
3. Ο ψηφοφόρος V_i υπογράφει το μήνυμα e_i ($s_i = \sigma_ι(e_i)$) και στέλνει στον διαχειριστή το υπογραμμένο (και κρυπτογραφημένο) μήνυμα s_i, το κρυπτογραφημένο μήνυμα e_i και την ταυτότητα του.

Το δεύτερο στάδιο του πρωτόκολλου είναι η διαδικασία διαχείρισης. Ο διαχειριστής υπογράφει το μήνυμα όπου περιέχει το ψηφοδέλτιο του ψηφοφόρου και το επιστρέφει σε αυτόν. Πιο αναλυτικά:

1. Ο διαχειριστής ελέγχει αν ο ψηφοφόρος V_i έχει το δικαίωμα να ψηφίσει. Αν όχι, τότε ο διαχειριστής απορρίπτει την ψήφο.
2. Ο διαχειριστής ελέγχει αν ο ψηφοφόρος V_i δεν έχει κάνει είδη αίτηση για υπογραφή. Αν έχει κάνει αίτηση, τότε ο διαχειριστής απορρίπτει την ψήφο.
3. Ο διαχειριστής ελέγχει την υπογραφή s_i του μηνύματος e_i. Αν είναι έγκυρη τότε υπογράφει το μήνυμα e_i, $d_i = \sigma_A(e_i)$ και στέλνει το d_i σαν πιστοποιητικό στον ψηφοφόρο V_i.

4. Στο τέλος ολόκληρης της διαδικασίας διαχείρισης, ο κάθε διαχειριστής ανακοινώνει τον αριθμό των υποψήφιων όπου υπόγραψε το ψηφοδέλτιο τους και δημοσιεύει μία λίστα με την ταυτότητα του υποψηφίου, το κρυπτογραφημένο μήνυμα e_i και το υπογραμμένο (και κρυπτογραφημένο) μήνυμα $s_{i.}$.

Το τρίτο στάδιο του πρωτοκόλλου είναι το στάδιο της ψηφοφορίας. Ο ψηφοφόρος παίρνει το υπογραμμένο ψηφοδέλτιο από τον διαχειριστή και το στέλνει ανώνυμα για να καταμετρηθεί. Πιο αναλυτικά:

1) Ο ψηφοφόρος V_i ανακτά την υπογραφή y_i του ψηφοδελτίου x_i μέσω $y_i = \delta(d_i, r_i)$.
2) Ο ψηφοφόρος V_i ελέγχει αν το y_i είναι η υπογραφή του διαχειριστή. Αν όχι, τότε ο ψηφοφόρος V_i το αναφέρει, δείχνοντας ότι $\{x_i, y_i\}$, δεν είναι έγκυρο το ψηφοδέλτιο.
3) Ο ψηφοφόρος V_i στέλνει το ψηφοδέλτιο του και την υπογραφή του διαχειριστή, $\{x_i, y_i\}$, στο μετρητή μέσο ένα ανώνυμο κανάλι επικοινωνίας.

Το τέταρτο στάδιο η συλλογή των ψήφων. Ο μετρητής δημοσιεύει μία λίστα με όλα τα ψηφοδέλτια όπου παρέλαβε. Πιο αναλυτικά:

1) Ο μετρητής ελέγχει την υπογραφή y_i του ψηφοδελτίου x_i χρησιμοποιώντας το εργαλείο επαλήθευσης του διαχειριστή. Αν ο έλεγχος είναι επιτυχής, τότε προσθέτει στη λίστα με αριθμό l, το ψηφοδέλτιο του και την υπογραφή του διαχειριστή $\{l, x_i, y_i\}$.
2) Όταν ψηφίσουν όλοι οι ψηφοφόροι, τότε ο μετρητής δημοσιεύει την λίστα σε όλους του ψηφοφόρους.

Το πέμπτο στάδιο είναι το άνοιγμα. Ο υποψήφιος ανοίγει την ψήφο του στέλνοντας ανώνυμα το κλειδί κρυπτογράφησης του. Πιο αναλυτικά:

1) Ο ψηφοφόρος V_i ελέγχει αν ο αριθμός των ψηφοδελτίων είναι ίσος με τον αριθμό των ψήφων. Αν όχι , τότε ανοίγει το τυφλό παράγοντα r_i όπου χρησιμοποιήθηκε στην κρυπτογράφηση.
2) Ο ψηφοφόρος V_i ελέγχει αν το ψηφοδέλτιο του είναι στη λίστα των ψηφοδελτίων. Αν όχι, τότε ανοίγει το έγκυρο ψηφοδέλτιο του και την υπογραφή του διαχειριστή $\{x_i, y_i\}$.
3) Ο ψηφοφόρος V_i στέλνει το κλειδί k_i με τον αριθμό του στη λίστα συλλογής των ψήφων l στο μετρητή μέσω ανώνυμου καναλιού.

Το έκτο στάδιο είναι η μέτρηση. Ο μετρητής μετρά όλες τις ψήφου και ανακοινώνει το τελικό αποτέλεσμα. Πιο αναλυτικά:

1) Ο μετρητής ανοίγει το ψηφοδέλτιο x_i, ανακτά την ψήφο v_i και ελέγχει αν η ψήφος είναι έγκυρη.

2) Ο μετρητής μετράει τις ψήφους και ανακοινώνει το τελικό αποτέλεσμα.

Το πρωτόκολλο διατηρεί την μυστικότητα του χρήστη και είναι αδύνατο να δημιουργηθεί σύνδεση μεταξύ της ψήφου και του ψηφοφόρου. Η ψήφος είναι κρυφή μέσω της τυφλής υπογραφής. Επίσης, το ψηφοδέλτιο x_i και το κλειδί k_i στέλνονται μέσω ανώνυμου καναλιού για να διατηρηθεί ο ψηφοφόρος κρυφός και να είναι αδύνατο να ανιχνευθεί ψηφοφόρο από επιτιθέμενους. Ακόμη και στις περιπτώσεις όπου το σύστημα έχει κάποιο λάθος, ο ψηφοφόρος δεν πρέπει να δείξει την ψήφο του για να αποδείξει στους υπόλοιπους το λάθος που έγινε. Το ψηφοδέλτιο και η υπογραφή του διαχειριστή $\{x_i,y_i\}$, είναι επαρκής για να αποδείξουν κάποιο σφάλμα στο στάδιο ψηφοφορίας ή άνοιγμα ψήφων.

Επιπρόσθετα, το πρωτόκολλο εγγυάται ότι το τελικό αποτέλεσμα είναι το δίκαιο αποτέλεσμα και δεν παραποιήθηκε ούτε από κάποιο διαχειριστή. Αν κάποιος προσπαθήσει να αλλάξει το αποτέλεσμα αποτρέποντας κάποιο ψηφοδέλτιο να προστεθεί στην λίστα ψηφοφορίας, τότε ο ψηφοφόρος δείχνει την ψήφο του και την υπογραφή του διαχειριστή στο σύστημα αποδεικνύοντας ότι είναι έγκυρος ψηφοφόρος. Αν όλοι οι ψηφοφόροι ψηφήσουν τότε είναι αδύνατο να προστεθούν νέοι ψεύτικοι ψήφοι, αφού θα ανακαλυφθεί ότι υπάρχουν περισσότερα ψηφοδέλτια από ψηφοφόρους. Επιπλέον, οι ψεύτικοι ψήφοι μπορούν να αναγνωριστούν εύκολα επειδή δεν θα έχουν την υπογραφή του διαχειριστή.

3.3 Juels, Catalano και Jakobsson πρωτόκολλο

Σε αυτό το υποκεφάλαιο θα αναφερθεί το πρωτόκολλο του Juels, Catalano, Jakobsson, γνωστό ως JCJ πρωτόκολλο [19]. Είναι ένα από τα πιο γνωστά πρωτόκολλα όπου προσπαθούν να καταπολεμήσουν τον εξαναγκασμό του ψηφοφόρου να ψηφίσει κάποιο υποψήφιο που δεν θέλει. Όμως αυτό το πρωτόκολλο υποφέρει από υπερβολική πολυπλοκότητα λόγω των διάφορων μεθόδων καταπολέμησης του εξαναγκασμού. Το JCJ πρωτόκολλο αποτελείται από 3 στάδια, το στάδιο εγγραφής, ψηφοφορίας και καταμέτρησης.

Επίσης, σε αυτό το υποκεφάλαιο χρησιμοποιούνται οι πιο κάτω συμβολισμοί:
V_i : Ψηφοφόρος i
Αρχειοφύλακες R : οι οντότητες όπου είναι υπεύθυνες να δημιουργούν τα στοιχεία των υποψήφιων και να τα κατανέμουν σε αυτούς.
Διαχειριστές T : οι οντότητες όπου είναι υπεύθυνες για την επεξεργασία των ψηφοδελτίων, καταμέτρηση των ψήφων και δημοσίευση του αποτελέσματος.
sk_R : Μυστικό κλειδί του αρχειοφύλακα

pk_R : Δημόσιο κλειδί του αρχειοφύλακα

sk_T : Μυστικό κλειδί του διαχειριστή

pk_T : Δημόσιο κλειδί του διαχειριστή

$E_{pkT}(m)$: Υπογραφή μηνύματος m με χρήση pk_T

Το πρώτο στάδιο του πρωτόκολλου είναι η εγγραφή. Οι έγκυροι ψηφοφόροι παίρνουν τα πιστοποιητικά στοιχεία τους για να μπορούν να ψηφίσουν. Πιο αναλυτικά:

1) Τα ιδιωτικά και δημόσια κλειδιά του σταδίου εγγραφής, (sk_R, pk_R) και καταμέτρησης (sk_T , pk_T) δημιουργούνται με ένα ασφαλή τρόπο.
2) Οι αρχειοφύλακες R δημιουργούν και στέλνουν στον ψηφοφόρο V_i μία τυχαία σειρά από χαρακτήρες σ_i που είναι το πιστοποιητικό του.
3) Οι αρχειοφύλακες R βάζουν την κρυπτογράφηση του σ_i , $S_i = E_{pkT}(\sigma_i)$ σε μία λίστα L και υπογράφεται ψηφιακά από τον αρχειοφύλακα R.

Το δεύτερο στάδιο του πρωτόκολλου είναι η ψηφοφορία. Ο ψηφοφόρος δημιουργεί το ψηφοδέλτιο του, επιλέγει το υποψήφιο που επιθυμεί και μαζί με το πιστοποιητικό του καταθέτει την ψήφο του. Πιο αναλυτικά:

1) Οι διαχειριστές του συστήματος δημοσιεύουν μια λίστα C με τα ονόματα και τα μοναδικά αναγνωριστικά των υποψήφιων και ένα τυχαίο εκλογικό αναγνωριστικό e.
2) Ο ψηφοφόρος V_i δημιουργεί το ψηφοδέλτιο του με την χρήση του αλγόριθμου κρυπτογράφησης ElGamal (E_1,E_2) για τον υποψήφιο c_j όπου επίλεξε και με το πιστοποιητικό του σ_i.. Το E_1 είναι η κρυπτογράφηση του c_j και το E_2 η κρυπτογράφηση του σ_i.
3) Ο ψηφοφόρος V_i υπολογίζει μη διαδραστική απόδειξη μηδενικής γνώσης (Non-Interactive zero-knowledge proof) για την γνώση και ορθότητα του πιστοποιητικού σ_i και υποψήφιου c_j. Αυτή η απόδειξη είναι το P_f.
4) Ο ψηφοφόρος V_i δημοσιεύει το ψηφοδέλτιο του (E_1,E_2) και την απόδειξη P_f ως B_i = (E_1,E_2, P_f) στο πίνακα ανακοινώσεων μέσω ενός ανώνυμου καναλιού.

Το τρίτο στάδιο είναι η καταμέτρηση ψήφων. Για να γίνει η καταμέτρηση των ψήφων πρώτα πρέπει να αφαιρεθούν οι διπλοί και μη έγκυρη ψήφοι. Αυτή η διαδικασία έχει πολυπλοκότητα $O(n^2)$ όπου n είναι ο αριθμός των ψήφων. Τα βήματα για την καταμέτρηση είναι τα ακόλουθα:

1) Ο διαχειριστής T ελέγχει όλες τις απόδειξης στο πίνακα ανακοινώσεων και απορρίπτει όλα τα ψηφοδέλτια με άκυρες αποδείξεις. Υποθέτουμε ότι A_1 είναι οι

έγκυρες κρυπτογραφημένες επιλογές υποψηφίων E_1 όπου απέμειναν και B_1 είναι τα κρυπτογραφημένα πιστοποιητικά E_2 όπου απέμειναν.

2) Ο διαχειριστής Τ εκτελεί κατά ζεύγη τεχνολογίες ενίσχυσης της μυστικότητας σε όλα τα στοιχεία στο B_1 και διαγράφει τους διπλούς ψήφους βάση κάποιων σταθερών κριτηρίων όπως η χρονολογία δημοσίευσης στο πίνακα ανακοινώσεων. Για κάθε στοιχείο όπου διαγράφεται από το B_1 το αντίστοιχο στοιχείο με το ίδιο δείκτη διαγράφεται από το A_1. Οι νέες λίστες με τα διαγραμμένα στοιχεία είναι B_1' και A_1'.
3) Ο διαχειριστής Τ εφαρμόζει ανάμιξη δικτύου στο B_1' και A_1', με την ίδια μυστική μετάθεση και το αποτέλεσμα είναι οι λίστες B_2 και A_2.
4) Ο διαχειριστής Τ εφαρμόζει ανάμιξη δικτύου στη κρυπτογραφημένη λίστα L με τα πιστοποιητικά των ψηφοφόρων και συγκρίνει κάθε στοιχείο του B_2 με κάθε στοιχείο της λίστας L χρησιμοποιώντας τεχνολογίες ενίσχυσης της μυστικότητας .
5) Ο διαχειριστής Τ κρατάει μία λίστα A_3 με όλα τα κρυπτογραφημένα στοιχεία του A_2, όπου τα αντίστοιχα στοιχεία του B_2 ταιριάζουν με ένα στοιχείο στη λίστα L. Με αποτέλεσμα όλα τα στοιχεία με άκυρα πιστοποιητικά ψηφοφόρου θα διαγραφούν.
6) Ο διαχειριστής Τ αποκρυπτογραφεί όλα τα στοιχεία στο A_3 και καταμετράει το τελικό αποτέλεσμα.

Αυτό το πρωτόκολλο πετυχαίνει μυστικότητα, ορθότητα, επαληθευσιμότητα και αντίσταση στον εξαναγκασμό όσο οι περισσότερες αρχές δεν διεφθαρμένες. Η μυστικότητα διατηρείται εφόσον τα δίκτυα ανάμιξης λειτουργούν σωστά και οι ψήφοι δεν μπορούν να συνδεθούν με τη λίστα L. Επίσης, αν οι περισσότεροι καταμετρητές είναι διεφθαρμένοι τότε μπορούν να αποκρυπτογραφήσουν τα πάντα από την αρχή της διαδικασίας. Για την ορθότητα και επαληθευσιμότητα οι ψηφοφόροι μπορούν να ελέγξουν τον πίνακα ανακοινώσεων για να επαληθεύσουν αν η ψήφος του μετρήθηκε και το αποτέλεσμα υπολογίστηκε σωστά. Όμως η διεφθαρμένη πλειοψηφία αρχών μπορούν να αποκτήσουν τα πιστοποιητικά των ψηφοφόρων και να καταθέσουν έγκυρους ψήφους προσποιούμενη ότι είναι οι ψηφοφόροι όπου δεν ψήφισαν, έτσι το αποτέλεσμα θα φαίνεται νόμιμο. Η αντίσταση στον εξαναγκασμό επιτυγχάνεται λόγω ότι το πιστοποιητικό του κάθε ψηφοφόρου παραμένει κρυφό σε όλη την εκλογική διαδικασία. Επιπρόσθετα, ο ψηφοφόρος έχει την δυνατότητα να ψηφίσει πολλαπλές φορές και μόνο η ψήφος με το πραγματικό του πιστοποιητικό θα μετρηθεί στο τελικό αποτέλεσμα.

3.4 Helios

Το Helios είναι ένα σύστημα διαδικτυακής ψηφοφορίας μέσω ενός πλοηγού [17]. Δεν απαιτεί κάποιο εξιδεικευμένο υλικό ή λογισμικό και ολόκληρη η εκλογική διαδικασία μπορεί να διεκπεραιωθεί μέσα από ένα συνηθισμένο ηλεκτρονικό υπολογιστή. Επιπλέον, το σύστημα δίνει μεγάλη έμφαση στην επαλήθευση των εκλογών. Όλοι οι ψηφοφόροι μπορούν να ελέγξουν αν η ψήφος τους καταχωρήθηκε, δεν άλλαξε, μετρήθηκε και το τελικό αποτέλεσμα είναι ορθό. Όμως, το σύστημα δεν προσφέρει ιδιαίτερη ασφάλεια σε άτομα με μολυσμένο υπολογιστή. Αν κακόβουλο λογισμικό υπάρχει στον ηλεκτρονικό υπολογιστή του ψηφοφόρου, τότε μπορεί να «ξεγελάσει» τον ψηφοφόρο και να καταχωρήσει την ψήφο του σε άλλο ψηφοφόρο. Αντιθέτως με άλλα συστήματα, το Helios δίνει διάφορες επιλογές στον ψηφοφόρο να επαληθεύσει την ψήφο του, έτσι ο ψηφοφόρος θα ανιχνεύσει την αλλαγή στην ψήφο από το κακόβουλο λογισμικό.

Η διαδικασία ψηφοφορίας του συστήματος είναι πολύ απλή. Αρχικά, όλοι οι πιθανοί ψηφοφόροι λαμβάνουν ένα ηλεκτρονικό μήνυμα, το οποίο τους προσκαλεί να ψηφίσουν. Το μήνυμα περιέχει την περιγραφή της εκλογικής διαδικασίας, τον σύνδεσμο στο θάλαμο ψηφοφορίας, τον μοναδικό αριθμό ψηφοφόρου, τον κωδικό του ψηφοφόρου και τον μοναδικό αριθμό της εκλογής. Ο ψηφοφόρος χρησιμοποιεί τον σύνδεσμο για να φτάσει στην ιστοσελίδα ψηφοφορίας. Στην συνέχεια ο ψηφοφόρος επιλέγει τον υποψήφιο που επιθυμεί, η επιλογή γίνεται με απάντηση ναι ή όχι ερωτήσεων. Όταν τελειώσει με τις επιλογές του, έχει την δυνατότητα ανασκόπησης και αλλαγής των επιλογών του. Εν τω μεταξύ το ψηφοδέλτιο έχει κρυπτογραφηθεί και ο ανιχνευτής του ψηφοδέλτιού είναι διαθέσιμος στον ψηφοφόρο για να το καταγράψει ή τυπώσει. Στο τέλος, ο ψηφοφόρος επιλέγει να καταχωρήσει το ψηφοδέλτιο του. Το σύστημα απαιτεί από το ψηφοφόρο να στείλει το μοναδικό αριθμό και κωδικό του, για να επικυρώσει ότι δικαιούται να ψηφίσει.

Όταν τελειώσει η διαδικασία ψηφοφορίας είναι η στιγμή για την μέτρηση του τελικού αποτελέσματος. Το σύστημα Helios υπολογίζει το κρυπτογραφημένο τελικό αποτέλεσμα, με την χρήση ομομορφικής κρυπτογράφησης, συναθροίζοντας το τελικό ψηφοδελτίου του κάθε εγκύρου ψηφοφόρου. Αυτή η διαδικασία είναι δημόσια και μπορεί να γίνει από οποιοδήποτε άτομο. Στη συνέχεια, τα προκαθορισμένα έμπιστα άτομα προσκαλούνται να αποκρυπτογραφήσουν το τελικό αποτέλεσμα. Κάθε έμπιστο άτομο κατεβάζει το κρυπτογραφημένο τελικό αποτέλεσμα από το σύστημα Helios, ελέγχει αν είναι ορθό, χρησιμοποιεί το ιδιωτικό του κλειδί για μερική αποκρυπτογράφηση και ανεβάζει το αποτέλεσμα πίσω στο σύστημα Helios. Μόνο όταν όλα τα έμπιστα άτομα αποκρυπτογραφήσουν το τελικό αποτέλεσμα, είναι δυνατό να αποκρυπτογραφηθεί το τελικό αποτέλεσμα και να εξαχθεί οποιαδήποτε πληροφορία για αυτό. Μόλις τα έμπιστα άτομα

τελειώσουν με το σκοπό τους, το σύστημα Helios ενώνει όλες τις μερικές αποκρυπτογραφήσεις, υπολογίζει το τελικό αποτέλεσμα και το δημοσιεύει. Η ένωση όλων των μερικών αποκρυπτογραφήσεων είναι δημόσια πράξη. Επιπρόσθετα, μετά την δημοσίευση του τελικού αποτελέσματος τα ιδιωτικά κλειδιά των έμπιστων ατόμων διαγράφονται.

Επίσης, το σύστημα Helios δίνει την ικανότητα σε όλους να προγραμματίσουν ένα σύστημα προετοιμασίας ψηφοδελτίου με στόχο να αυξηθεί η εμπιστοσύνη στο σύστημα. Το σύστημα προετοιμασίας ψηφοδελτίων είναι ο τρόπος που δημιουργεί και καταθέτει ο ψηφοφόρος το ψηφοδέλτιο. Το Helios προσφέρει το δικό του σύστημα, όπου είναι μία απλή ιστοσελίδα, μέσω αυτής ο ψηφοφόρος μπορεί να επιλέξει τους υποψηφίους που επιθυμεί και να καταθέσει την ψήφο του. Επίσης, για περισσότερη ασφάλεια ο χρήστη μπορεί να αποσυνδεθεί από το διαδίκτυο κατά τη διάρκεια ψηφοφορίας. Πιο αναλυτικά, ο χρήστη έχει την δυνατότητα αμέσως μόλις φορτωθεί η ιστοσελίδα να σταματήσει τη σύνδεση του προς το διαδίκτυο, να επιλέξει τις ψήφους τους, να κρυπτογραφηθεί το ψηφοδέλτιο του και να ξανασυνδεθεί στο διαδίκτυο για να καταχωρήσει την ψήφο του. Με αυτό το τρόπο, η επιλογή του δεν θα είναι ποτέ ορατή κατά τη διάρκεια που είναι ενωμένος στο διαδίκτυο.

Το σύστημα Helios χρησιμοποιεί το αλγόριθμο κρυπτογράφησης του ElGamal, του οποίου η ασφάλεια βασίζεται στην δυσκολία της απόφασης του Diffie-Hellman (Decisional Diffie–Hellman) . Η βασική χρήση του είναι η προστασία των ψήφων, ώστε κανένας να μην μπορεί να αναγνωρίσει την ψήφο κάποιου ψηφοφόρου. Στο ψηφοδέλτιο με την λίστα των υποψηφίων, κάθε επιλογή των υποψηφίων αποθηκεύεται σαν «0» ή «1». Το «1» ισούται ότι ο υποψήφιος παίρνει 1 ψήφο και το «0» ότι ο υποψήφιος δεν παίρνει καμία ψήφο. Το «0» και «1» κωδικοποιούνται σαν g^0 και g^1 αντίστοιχα, ώστε η κρυπτογραφημένη ψήφος να είναι ομομορφική. Με την χρήση ομομορφικής κρυπτογραφίας, το σύστημα υπολογίζει το τελικό κρυπτογραφημένο αποτέλεσμα πολλαπλασιάζοντας όλους του κρυπτογραφημένους ψήφους. Με αυτό τον τρόπο δεν αποκρυπτογραφείται ποτέ η ψήφος του χρήστη, άρα παραμένει μυστική. Τα βήματα του ElGamal στο σύστημα Helios είναι τα ακόλουθα:

1) Το μυστικό κλειδί αποκρυπτογράφησης είναι μία τυχαία τιμή x και ανήκει στο Z_q
2) Το δημόσιο κλειδί y υπολογίζεται από το x και είναι το $y=g^x$
3) Το μήνυμα m κρυπτογραφείται με την χρήση ενός τυχαίου r, που ανήκει στο Z_q και υπολογίζεται το κρυπτογραφημένο μήνυμα ως $(c1,c2)=(g^r,my^r)$.
4) Το (c1,c2) μπορεί να αποκρυπτογραφηθεί, με την χρήση του μυστικού κλειδιού αποκρυπτογράφησης x , ως $m = c_2/c_1^x$
5) Για την αποκρυπτογράφηση απαιτείται η συνεργασία κάποιων έμπιστων ατόμων.

6) Για να αποκτήσει το κλειδί του , το έμπιστο άτομο δημιουργεί ένα ζεύγος ElGamal κλειδιών και διατηρεί το x_i μυστικό. $(x_i, y_i = g^{x_i})$.
7) Το δημόσιο κλειδί της εκλογής είναι το $g^x = \Pi g^{x_i}$.
8) Για την αποκρυπτογράφηση του (c1,c2) , κάθε έμπιστο άτομο υπολογίζει και αποκρυπτογραφεί το $d_i = c_1^{x_i}$
9) Στο τέλος το αποτέλεσμα υπολογίζεται ως $c_2/\Pi d_i$.

Στο σύστημα Helios υπάρχει η μυστικότητα της ψήφου και αντίσταση στον εξαναγκασμό ψηφοφορίας. Η μυστικότητα των ψήφων βασίζεται στην ειλικρίνεια τουλάχιστον ενός έμπιστου ατόμου. Για να αποκρυπτογραφηθούν οι ψήφοι και να παραβιαστεί η μυστικότητα της ψήφου, χρειάζονται όλα τα έμπιστα άτομα να χρησιμοποιήσουν το ιδιωτικό τους κλειδί. Όσο τουλάχιστον ένα έμπιστο άτομο παραμένει ειλικρινές και δεν συνεισφέρει στην διαδικασία αποκρυπτογράφησης, τότε καμία πληροφορία δεν μπορεί να εξαχθεί για τους ψηφοφόρους. Η αντίσταση στον εξαναγκασμό ψηφοφορίας προσφέρεται σε αδύναμη μορφή. Όπως σε όλα τα συστήματα ψηφοφορίας χωρίς επίβλεψη, κάποιο κακόβουλο άτομα μπορεί να είναι δίπλα σου όταν ψηφίζεις και να σε αναγκάσεις να ψηφίσεις σύμφωνα με την επιλογή του. Οι ψηφοφόροι έχουν την δυνατότητα να ξαναψηφίσουν σε μία άλλη στιγμή, αλλά το κακόβουλο άτομο μπορεί να αντιληφθεί τη νέα ψήφο μέσω του κέντρου παρακολούθησης της ψηφοφορίας, εκτός αν χρησιμοποιούνται ψευδώνυμα αντί αληθινά ονόματα στο κέντρο παρακολούθησης.

Το σύστημα Helios προσφέρει πλήρης επαλήθευση (end-to-end verification). Η πλήρης επαλήθευση αποτελείται από καταχώρηση όπως προορίζεται (cast-as-intended), καταγραφή όπως καταχωρήθηκε (recorded-as-cast) και καταμέτρηση όπως καταγράφηκε (tallied-as-recorded). Η καταχώρηση όπως προορίζεται είναι δυνατότητα του ψηφοφόρου να αποκτήσει απόδειξη ότι η ψήφος του καταχωρήθηκε στο σύστημα όπως ψήφησε. Η καταγραφή όπως καταχωρήθηκε είναι δυνατότητα του ψηφοφόρου να αποκτήσει απόδειξη ότι η ψήφος καταγράφηκε σωστά στους διακομιστές του συστήματος Helios. Η καταμέτρηση όπως καταγράφηκε επιτρέπει σε οποιοδήποτε άτομο να επικυρώσουν ότι όλοι οι έγκυροι καταγραμμένοι ψήφοι μετρήθηκαν.

Η καταχώρηση όπως προορίζεται επιτυγχάνεται με τον ακόλουθο τρόπο. Κάθε ψηφοδέλτιο έχει ένα ιχνηλάτη και ο ψηφοφόρος μπορεί να χρησιμοποιήσει τον ιχνηλάτη για να ελέγξει αν καταχωρήθηκε η ψήφος του. Όμως, η νομιμότητα του ιχνηλάτη μπορεί να μην ισχύει, έτσι ο ψηφοφόρος έχει την δυνατότητα να το ελέγξει. Το σύστημα Helios δίνει τη δυνατότητα στο χρήστη, μέσω της διαδικασίας που ονομάζεται πρόκληση Benaloh (Benaloh

Challenge), να ελέγξει την νομιμότητα του συστήματος προετοιμασίας ψηφοδελτίων. Αυτό γίνεται όταν τελειώσει όλοι η προετοιμασία του ψηφοδελτίου, αλλά πριν την διαδικασία καταχώρησης του ψηφοδελτίου. Η πρόκληση Benaloh δίνει στο ψηφοφόρο 2 επιλογές: να καταχωρήσει το ψηφοδέλτιο του ή να απαιτήσει έλεγχο του ψηφοδελτίου και να επικυρώσει την κρυπτογράφηση. Αν ο ψηφοφόρος επιλέξει την δεύτερη επιλογή, το σύστημα προετοιμασίας του ψηφοδελτίου δίνει όλα τα δεδομένα που χρησιμοποίησε για να δημιουργήσει το ψηφοδέλτιο, συμπεριλαμβανομένου και τα δεδομένα κρυπτογράφησης. Ο ψηφοφόρος μπορεί να ελέγξει όλα τα δεδομένα του ψηφοδέλτιού με ένα πρόγραμμα επικύρωσης ψηφοδελτίων, για να επικυρώσει ότι το ψηφοδέλτιο του θα καταχωρούσε τη δική του επιλογή, είναι έγκυρο και έχει το σωστό ιχνηλάτη.

Η καταγραφή όπως καταχωρήθηκε επιτυγχάνεται με τον ακόλουθο τρόπο. Ο ψηφοφόρος συνδέεται στην ιστοσελίδα παρακολούθησης ψηφοφορίας του Helios, όπου υπάρχουν όλοι οι ιχνηλάτες όλων των ψήφων όπου θα καταμετρηθούν στο τελικό αποτέλεσμα. Ο ψηφοφόρος επικυρώνει ότι ο ιχνηλάτης της ψήφου του εμφανίζεται και έχει το σωστό μοναδικό αριθμό. Αυτοί η διαδικασία δεν απαιτεί αυθεντικοποίηση από τον ψηφοφόρο, έτσι αν το σύστημα είναι κακόβουλο δεν μπορεί να αλλάξει τη λίστα των ψήφων ανάλογα με τον ψηφοφόρο, ώστε να αποκρύψει ότι άλλαξε κάποιο ψηφοδέλτιο. Επίσης, είναι εύκολο να ανατεθεί αυτός ο έλεγχος σε άλλες οργανώσεις ή ακτιβιστές, ο ψηφοφόρος στέλνει τον μοναδικό αριθμό ιχνηλάτη του ψηφοδελτίου του σε αυτούς για να επικυρώσουν το ψηφοδέλτιο του.

Η καταμέτρηση όπως καταγράφηκε επιτυγχάνεται με τον ακόλουθο τρόπο. Κάθε ενδιαφερόμενος μπορεί να αποκτήσει μία λίστα με τα άτομα που ψήφισαν από την ιστοσελίδα κέντρου παρακολούθησης ψηφοφορίας του Helios, εκτός αν οι αρχές ψηφοφορίας έκρυψαν τα ονόματα με χρήση ψευδώνυμων. Στην συνέχεια επικοινωνεί με αυτά τα άτομα, πιθανόν τυχαία, και τους ζητά να επικυρώσουν τον μοναδικό αριθμό ιχνηλατήσεις του ψηφοδελτίου τους. Όταν όλοι οι μοναδικοί αριθμοί ιχνηλατήσεις επικυρωθούν, το δεύτερο βήμα είναι το κατέβασμα της λίστας με τα κρυπτογραφημένα ψηφοδέλτια από το σύστημα Helios και να ελέγξει αν οι αριθμοί ιχνηλατήσεις ανήκουν στο αναμενόμενο άτομο. Στο τέλος, η ορθότητα του αποκρυπτογραφημένου τελικού αποτελέσματος μπορεί να επικυρωθεί από τις αποδείξεις αποκρυπτογράφησης που παρέχονται από τα έμπιστα άτομα. Η πιο πάνω διαδικασία μπορεί εύκολα να ανατεθεί σε τρίτα άτομα, όπως τους υποψήφιους.

3.5 Voatz

Το Voatz είναι ένα διαδικτυακό σύστημα ψηφοφορίας για τα κινητά τηλέφωνα [7][27]. Ο στόχος του συστήματος είναι η ασφάλεια, η προσβασιμότητα, διαθεσιμότητα και ευκολία στη χρήση. Οι δημιουργοί του ήθελαν να κατασκευάσουν ένα σύστημα το οποίο είναι πρακτικό στον πραγματικό κόσμο και οι ψηφοφόροι μπορούν να το χρησιμοποιήσουν χωρίς πρόβλημα. Το σύστημα συνεχώς εξελίσσεται και βελτιώνεται. Επίσης, αξιολογείται συνεχώς από διάφορους οργανισμούς, με το ποιο σημαντικό να είναι το Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών της Αμερικής.

Η χρήση του Voatz στην εκλογική διαδικασία είναι πολύ απλή. Όλοι οι έγκυροι χρήστες λαμβάνουν ένα ηλεκτρονικό μήνυμα ότι μπορούν να ψηφίσουν με το Voatz. Ο έγκυρος χρήστης κατεβάζει την εφαρμογή του Voatz στο κινητό του και δημιουργεί ένα λογαριασμό. Ο λογαριασμός απαιτεί τον αριθμό κινητού τηλεφώνου, το ηλεκτρονικό ταχυδρομείο και κωδικό ασφαλείας του ψηφοφόρου. Μετά την δημιουργία λογαριασμού, ο ψηφοφόρος πρέπει να επικύρωση την ταυτότητα του μέσω τον κωδικό του, αναγνώριση προσώπου και σάρωση δακτυλικού αποτυπώματος. Μόνο μετά την επιτυχή επικύρωση ταυτότητας ο ψηφοφόρος λαμβάνει το ψηφοδέλτιο του στο κινητό του. Ο ψηφοφόρος επιλέγει τον υποψήφιο που επιθυμεί και στέλνει την ψήφο του μαζί με τα στοιχεία ταυτότητας του. Ο ψηφοφόρος λαμβάνει μία ανώνυμη απόδειξη ψήφου για να επικυρώσει την επιλογή του. Στο τέλος, η δικαιοδοσία εκλογής λαμβάνει το ανώνυμο ψηφοδέλτιο του ψηφοφόρου, το τυπώνει και το σαρώνει για να μετρηθεί το αποτέλεσμα.

Η διαδικασία επικύρωσης ταυτότητας είναι πολύ απλή και συνήθως χρειάζεται λιγότερο από 5 λεπτά. Το σύστημα Voatz ενσωματώνει μια υπηρεσία ελέγχου ταυτότητας από την Jumio, η οποία επαληθεύει την εγκυρότητα της ταυτότητας, μέσω μίας φωτογραφίας της και εκτελεί μια δοκιμή για «ζωτικότητα». Για την εγκυρότητα της ταυτότητας, οι πληροφορίες στην μπροστινή μεριά τις ταυτότητας διαβάζονται μέσω οπτικής αναγνώρισης χαρακτήρων και συγκρίνονται με τις πληροφορίες που είναι κωδικοποιημένες στο γραμμωτό κωδικό (barcode) στην πίσω μεριά της ταυτότητας. Για την δοκιμή «ζωτικότητας» , ο ψηφοφόρος πρέπει να βιντεογραφήσει τον εαυτό του (video selfie) να κινεί να χέρια του, κεφαλή του ή να ανοίγει και κλείνει τα μάτια του. Ο σκοπός της δοκιμή «ζωτικότητας» είναι να επικυρωθεί ότι είναι το ίδιο άτομο στο οποίο ανήκει η ταυτότητα και ότι υπάρχει στον πραγματικό κόσμο. Το τελευταίο στάδιο είναι η σύγκριση του βίντεο με τη φωτογραφία της ταυτότητας. Αυτή η διαδικασία γίνεται αυτόματα ή χειρωνακτικά. Αν γίνει αυτόματα, τότε 2 προγράμματα αναγνώρισης προσώπου πρέπει να βεβαιώσουν ότι το άτομο στο βίντεο είναι το ίδιο άτομο στη φωτογραφία. Αν αυτό αποτύχει τότε ένα άνθρωπος θα προσπαθήσει να βεβαιώσει ότι το άτομο στο βίντεο είναι το ίδιο άτομο στη φωτογραφία. Το τελευταίο στάδιο

τελειώνει με την εισαγωγή του κωδικού και δακτυλικού αποτυπώματος του ψηφοφόρου. Στο τέλος της διαδικασίας διαγράφονται όλα τα δεδομένα του ψηφοφόρου που συλλέχθηκαν σε αυτή την διαδικασία.

Ο ψηφοφόρος έχει την δυνατότητα να επαληθεύσει την ψήφο του, για να είναι σίγουρος ότι η ψήφος του καταχωρήθηκε όπως προοριζόταν. Περίπου 30 δευτερόλεπτα μετά την ψηφοφορίας, ο ψηφοφόρος παίρνει ένα ηλεκτρονικό μήνυμα, όπου είναι προστατευόμενο από τον κωδικό τους, με τις επιλογές τους. Ο ψηφοφόρος ελέγχει τις επιλογές για να είναι σίγουρος ότι η ψήφος του καταχωρήθηκε σωστά.

Το σύστημα ψηφοφορίας Voatz για τους ψηφοφόρους είναι μόνο διαθέσιμο για κινητές συσκευές. Για να διατηρηθεί η ακεραιότητα ολόκληρης της διαδικασίας ψηφοφορίας πρέπει οι κινητές συσκευές να είναι ασφαλείς. Όταν η εφαρμογή εγκατασταθεί στην συσκευή του χρήστη ελέγχει την ασφάλεια της. Αν η εφαρμογή κρίνει ότι η συσκευή δεν είναι ασφαλής, τότε δεν θα επιτρέψει στον χρήστη να ψηφίσει. Κάποιοι βασικοί λόγοι όπου θέτουν σε κίνδυνο την ασφάλειας μιας συσκευής είναι: οι συσκευές με παλιές εκδόσεις λογισμικού, εγκαταστημένες εφαρμογές όπου δεν είναι ψηφιακά υπογραμμένες από Apple ή Google και συσκευές με υψωμένα δικαιώματα (“rooted” , “jaibroken”) όπου θα επίτρεπε το ύπουλο λογισμικό να βλάψει σε μεγάλο βαθμό τη συσκευή. Η αποτροπή ψηφοφόρων να λάβουν μέρος στην εκλογική διαδικασία λόγο μη ασφαλής συσκευών μειώνει την προσβασιμότητα του συστήματος αλλά διατηρεί την ακεραιότητα της εκλογικής διαδικασίας.

Εκτός από την ίδια συσκευή του χρήστη, το δίκτυο μεταφοράς των μηνυμάτων από την συσκευή του χρήστη προς στους διακομιστές του Voatz πρέπει να τηρεί όλες τις απαιτήσεις ασφάλειας. Η επικοινωνία μέσω διαδικτύου γίνεται με την χρήση του πρωτόκολλου ασφάλειας επιπέδου μεταφοράς (TSLv1.2). Επιπλέον, όλα τα μηνύματα από και προς τους διακομιστές είναι κρυπτογραφημένα μέσω αλγόριθμου προηγμένου πρότυπου κρυπτογράφησης που λειτουργεί στη μορφή μετρητή Galois και το μήκος του κλειδιού είναι 256 bits (AES/GCM 256 bits). Επιπρόσθετα, κάθε χρήστης, όταν κατεβάσει την εφαρμογή, δημιουργεί δημόσιο και ιδιωτικό κλειδί κρυπτογράφησης. Το ίδιο συμβαίνει και στον διακομιστή, δημιουργεί δημόσιο και ιδιωτικό κλειδί κρυπτογράφησης για κάθε χρήστη, ώστε να μπορούν να επικυρώσουν ο ένας τον άλλο. Όλα τα κλειδιά που χρησιμοποιούνται από τον ψηφοφόρο αποθηκεύονται σε θήκη (KeyStore) στο υλικό του κινητού. Επίσης, χρησιμοποιούνται διάφοροι μέθοδοι, όπως διαφάνεια πιστοποιητικού (Certificate Transparency) και καρφίτσωμα πιστοποιητικού (Certificate Pinning) για τον έλεγχο της εγκυρότητας του πιστοποιητικού του διακομιστή, που εμφανίζεται κατά την διάρκεια

δημιουργίας μίας διαδικτυακής σύνδεσης με την χρήση του πρωτόκολλου ασφαλής μεταφοράς υπερκειμένου (HTTPS).

Ένα άλλο εξίσου σημαντικό θέμα ασφάλειας είναι η ασφάλειας της μονάδας αποθήκευσης των ψήφων. Το Voatz χρησιμοποιεί αλυσίδα μπλοκ (Blockchain) για την αποθήκευση των κρυπτογραφημένων ψήφων. Σε ένα μπλοκ υπάρχει ο ανώνυμος μοναδικός αριθμό του ψηφοφόρου, ο μοναδικός αριθμός της εκλογής, ο μοναδικός αριθμός της δικαιοδοσίας, ο κρυπτογραφημένος μοναδικός αριθμός του διαγωνισμού και ο κρυπτογραφημένος μοναδικός αριθμός του υποψήφιου που επέλεξε ο ψηφοφόρος. Ο έλεγχος της μονάδας αποθήκευσης θα γίνεται από μία πιστοποιημένη αρχή όπως τον διευθύνων σύμβουλο των εκλογών. Τα βασικά χαρακτηριστικά του δικτύου με τις αλυσίδες μπλοκ (Blockchain) είναι οι κατανεμημένοι διακομιστές, περιττά και αμετάβλητα δεδομένα. Το δικτύου με τις αλυσίδες μπλοκ (Blockchain) περιλαμβάνει τουλάχιστον 32 διακομιστές από Amazon και Microsoft στις Ηνωμένες Πολιτείες της Αμερικής. Κάθε διακομιστής συγχρονίζει τα δεδομένα του με τους υπόλοιπους διακομιστές, άρα κάθε διακομιστής έχει όλους τους ψήφους. Όταν ένας ψήφος έχει προστεθεί στην αλυσίδα με τους υπόλοιπους ψήφους, τότε είναι αδύνατο να μεταβληθεί.

Ο στόχος του Voatz για ασφάλεια, προσβασιμότητα, διαθεσιμότητα και ευκολία χρήσης είναι ελκυστικός, όμως λείπει η διαφάνεια από ολόκληρο το σύστημα [23]. Είναι κατανοητό μία εταιρία να θέλει να προστατέψει το προϊόν της, αλλά για συστήματα ηλεκτρονικής ψηφοφορίας η διαφάνεια είναι απαραίτητη. Οι ιδιοκτήτες του Voatz αρνούνται να συνεργαστούν με ανεξάρτητους ερευνητές και το 2018 κατάγγειλαν ερευνητές του Πανεπιστημίου του Michigan, στο Ομοσπονδιακό Γραφείο Ερευνών των Ηνωμένων Πολιτειών της Αμερικής (FBI), όταν έκανα μία δυναμική ανάλυση του συστήματος. Αντιθέτως, άλλα συστήματα ηλεκτρονικής ψηφοφορίας ήταν διαθέσιμα να συνεργαστούν με ανεξάρτητους ερευνητές και να δημοσιεύσουν το κώδικα του συστήματος. Η έλλειψη διαφάνειας στο Voatz είναι σε τέτοιο βαθμό όπου αποτρέπει την εύρεση πιθανών κινδύνων στο σύστημα, επειδή αποτρέπεται ο έλεγχος του συστήματος και τις ασφάλειας του από άλλα άτομα.

Κεφάλαιο 4

Προδιαγραφές εφαρμογής

4.1 Εισαγωγή στις προδιαγραφές της εφαρμογής

Η ιδέα του συστήματος είναι η μία εφαρμογή ηλεκτρονικής ψηφοφορίας, σε φοιτητικές εκλογές όπως του Πανεπιστημίου Κύπρου, για android κινητά. Η διαδικασία των εκλογών θα γίνεται ηλεκτρονικά, μέσω της κινητής εφαρμογής, αντί να γίνεται με το παραδοσιακό τρόπο, δηλαδή με χαρτί. Πιο συγκεκριμένα, οι διαδικασίες ψηφοφορίας, επαλήθευσης της ψήφου, καταμέτρησης των ψήφων και ανακοίνωσης του τελικού αποτελέσματος θα γίνονται ηλεκτρονικά. Με αυτό τον τρόπο η εκλογική διαδικασία θα είναι πιο εύκολη, βολική, γρήγορη και πιθανό να ελκύσει περισσότερους φοιτητές.

Σε αυτό το κεφάλαιο θα παρουσιαστούν οι προδιαγραφές της εφαρμογής. Πιο συγκεκριμένα θα γίνει ανάλυση των βημάτων κατά την σχεδίαση και υλοποίηση της εφαρμογής. Επίσης θα αναλυθούν οι 3 κατηγορίες απαιτήσεων, οι οποίες είναι οι απαιτήσεις χρηστών, ασφάλειας και ευχρηστίας. Ακόμη, θα γίνει περιγραφή των οντοτήτων, θα αναλυθεί το πρωτόκολλο ψηφοφορίας και στο τέλος θα παρουσιαστούν οι λειτουργίες της εφαρμογής.

4.2 Μέθοδος σχεδίασης και υλοποίησης του συστήματος

Σε αυτό το υποκεφάλαιο θα γίνει αναφορά στη μέθοδο που χρησιμοποιήθηκε στη φάση σχεδίασης και υλοποίησης της εφαρμογής. Η μέθοδος που χρησιμοποιήθηκε είναι παρόμοια με την μεθοδολογία «Λογική διαδραστική σχεδίαση με επίκεντρο τον χρήστη» (LUCID) [10]. Επίσης θα γίνει αναφορά στα βασικά εργαλεία που χρησιμοποιήθηκαν κατά τη διάρκεια σχεδίασης και υλοποίησης του συστήματος.

Αρχικά, έγινε η ανάπτυξη της βασικής ιδέας του συστήματος. Η ιδέα του συστήματος είναι η μία εφαρμογή ηλεκτρονικής ψηφοφορίας, σε φοιτητικές εκλογές όπως του Πανεπιστημίου Κύπρου, για android κινητά. Αυτό έχει ως συνέπεια την ανάγκη για αυστηρές απαιτήσεις ασφάλειας και μυστικότητας στα προσωπικά δεδομένα του χρήστη και στην ψήφο του. Όμως, λόγω ότι η εφαρμογή αφορά φοιτητικές εκλογές δεν απαιτείται το ίδιο επίπεδο ασφάλειας όπως πρέπει να υπάρχει σε κρατικές εκλογές.

Στη συνέχεια έγινε ο προσδιορισμός της τυπικής ομάδας χρηστών. Η τυπική ομάδα των χρηστών του συστήματος είναι οι φοιτητές. Όλοι οι φοιτητές ενός πανεπιστημίου έχουν το δικαίωμα να ψηφίσουν, άρα όλοι οι φοιτητές είναι πιθανοί χρήστες. Από αυτό συμπεραίνουμε ότι οι πιθανοί χρήστες της εφαρμογής έχουν διάφορα χαρακτηριστικά και διαφορετικό επίπεδο γνώσης, αλλά οι πλείστοι έχουν μεγάλη εμπειρία όσο αφορά τη χρήση των κινητών (smartphones). Άρα η εφαρμογή πρέπει να ακολουθεί κάποιους κανόνες ευχρηστίας, ώστε να είναι απλή και κατανοητή για όλους τους χρήστες.

Μετά έγινε η ανάπτυξη του πρωτόκολλου ψηφοφορίας της εφαρμογής. Το πρωτόκολλο παρουσιάζει σε ψηλό επίπεδο τη διαδικασία ψηφοφορίας. Το πρωτόκολλο είναι βασισμένο σε μεγάλο βαθμό στο πρωτόκολλο των Fujioka, Okamoto και Ohta και το πρωτόκολλο των Juels, Catalano και Jakobsson. Αυτά τα δύο πρωτόκολλα έχουν το ίδιο στόχο με το πρωτόκολλο του συστήματος, ο οποίος είναι η μυστικότητα και ασφάλεια του ψηφοφόρου. Το πρωτόκολλο θα αναλυθεί με περισσότερη λεπτομέρεια στο κεφάλαιο 4.7.

Το επόμενο βήμα ήταν ο προσδιορισμός και ανάλυση απαιτήσεων. Στα επόμενα υποκεφάλαια θα παρουσιαστούν οι 3 κατηγορίες απαιτήσεων, οι οποίες είναι οι απαιτήσεις χρηστών, ασφάλειας και ευχρηστίας. Οι απαιτήσεις χρήστη ορίστηκαν με την χρήση διαδικτυακού ερωτηματολόγιου προς τους πιθανούς χρήστες και συνέντευξης με το πρόεδρο του φοιτητικού συμβούλιου του Πανεπιστημίου Κύπρου. Οι απαιτήσεις ευχρηστίας είναι οι 10 κανόνες ευχρηστίας του Jakob Nielsen [13][26]. Οι απαιτήσεις ασφάλειας είναι η μυστικότητα, η ακεραιότητα, η επαλήθευση, η αυθεντικοποίηση, και η διαθεσιμότητα.

Όταν τελείωσε η ανάλυση απαιτήσεων ξεκίνησε η υλοποίηση του συστήματος. Αρχικά δημιουργήθηκε ένα πρωτότυπο με τις βασικές οθόνες του συστήματος. Μετά την αξιολόγηση του πρώτου πρωτότυπου συνέχισε η ανάπτυξη του συστήματος. Το σύστημα αναπτύχθηκε με τη χρήση των εξελικτικών πρωτοτύπων, δηλαδή το σύστημα συνεχώς εξελισσόταν και βελτιώνονταν μέχρι να φτάσει στη τελική του έκδοση. Συνολικά δημιουργήθηκαν 3 πρωτότυπα. Στο πρώτο πρωτότυπο υπήρχαν οι βασικές οθόνες του συστήματος, χωρίς κάποια λειτουργία. Στο δεύτερο πρωτότυπο υπήρχε ολοκληρωμένη η διαδικασία ψηφοφορίας και η διαδικασία επαλήθευσης ψήφου. Στο τρίτο πρωτότυπο υπήρχαν όλες οι λειτουργίες. Κάθε πρωτότυπο αξιολογήθηκε από μία ομάδα πιθανών χρηστών με σκοπό τη βελτίωση του συστήματος.

Η τελευταία φάση είναι η αξιολόγηση του συστήματος. Εκτός από τις αξιολογήσεις των πρωτοτύπων, έγινε μία αξιολόγηση της ευχρηστίας του συστήματος από μία ομάδα πιθανών χρηστών και ένας έλεγχος ασφάλειας του συστήματος. Όλες οι αξιολογήσεις αναλύονται στο πέμπτο κεφάλαιο.

Στη διάρκεια ανάπτυξης του συστήματος χρησιμοποιήθηκαν διάφορα εργαλεία. Το κύριο εργαλείο που χρησιμοποιήθηκε είναι το Android Studio με την χρήση της γλώσσας Kotlin, για την υλοποίηση της android εφαρμογής. Εξίσου σημαντικά εργαλεία είναι το Visual Studio Code για τον προγραμματισμό του διακομιστή ιστού (οντότητες) σε γλώσσα php7.2, phpMyAdmin για την δημιουργία MySQL βάση δεδομένων και apache2 για λογισμικό διακομιστή ιστού όπου φιλοξενεί την βάση δεδομένων και το php7.2 πρόγραμμα. Επιπλέον χρησιμοποιήθηκε HTML5, CSS, JavaScript , php7.2 μέσω του Visual Studio Code, για την υλοποίηση μία βοηθητικής ιστοσελίδας για τις βασικές λειτουργίες των οντοτήτων. Επιπρόσθετα, για βιβλιοθήκες κρυπτογράφησης χρησιμοποιήθηκε στον διακομιστή ιστού η βιβλιοθήκη sodium όπου υπάρχει στο php7.2, η βιβλιοθήκη sodium για JavaScript και για την android εφαρμογή η βιβλιοθήκη lazysodium, όπου είναι η αντίστοιχη της βιβλιοθήκης sodium για android.

4.3 Απαιτήσεις Χρήστη

Σε αυτό το υποκεφάλαιο θα αναφερθούν οι απαιτήσεις από τους μελλοντικούς χρήστες του συστήματος. Αυτές οι απαιτήσεις προέκυψαν από συνέντευξη και ερωτηματολόγια. Η συνέντευξη και τα αποτελέσματα του ερωτηματολογίου υπάρχουν στα παραρτήματα.

Οι πιο κάτω απαιτήσεις αφορούν την εκλογική διαδικασία των φοιτητικών εκλογών και προέκυψαν από συνέντευξη με το πρόεδρο του φοιτητικού συμβουλίου του Πανεπιστημίου Κύπρου. Το φοιτητικό συμβούλιο αποτελείται από 21 μέλη, τα οποία είναι φοιτητές του Πανεπιστημίου. Πρωταρχικά οι ψηφοφόροι ψηφίζουν την παράταξη που επιθυμούν, υπάρχει η δυνατότητα για λευκό ψηφοδέλτιο, και αν θέλουν ψηφίζουν 0-7 μέλη της παράταξής όπου επέλεξαν. Επίσης, οι «ανεξάρτητοι» υποψήφιοι μπορούν να λάβουν μέρος στις εκλογές και αν ο ψηφοφόρος ψηφίσει ένα ανεξάρτητο υποψήφιο τότε δεν μπορεί να ψηφίσει οποιοδήποτε άλλο υποψήφιο ή παράταξη. Όσο αφορά το αποτέλεσμα πρέπει να καταμετρηθούν οι ψήφοι των παρατάξεων και υποψήφιων ξεχωριστά. Πρώτα καταμετρούνται και κατανέμονται οι έδρες σε κάθε παράταξη με αναλογικό τρόπο. Στη συνέχεια καταμετρούνται και κατανέμονται οι έδρες στους υποψήφιους φοιτητές της κάθε παράταξης ανάλογα με πόσες έδρες έχει η κάθε παράταξη και με τον αριθμό των ψήφων του κάθε υποψήφιου.

Στη συνέχεια, θα γίνει αναφορά στις δευτερεύουσες απαιτήσεις, που αφορούν άμεσα τη διαδικασία ψηφοφορίας και προέκυψαν από το ερωτηματολόγιο που δόθηκαν στους πιθανούς χρήστες. Από το ερωτηματολόγιο παρατηρούμε τα περισσότερα άτομα που απάντησαν είναι πολιτικά ενεργοί, αλλά έχουν λίγες γνώσεις για την ηλεκτρονική ψηφοφορία. Σχεδόν όλα τα άτομα που απάντησαν το θεώρησαν πολύ σημαντικό ο ψηφοφόρος να έχει τη δυνατότητα να επαληθεύει την ψήφο του και θεωρήθηκε σημαντικό οι αρχές ή τρίτα άτομα να μπορούν να ελέγξουν ότι μόνο έγκυρα άτομα ψήφισαν. Επίσης, υπάρχει ενδιαφέρον για την δυνατότητα αντικατάστασης της ψήφου. Επιπρόσθετα, τα περισσότερα άτομα δεν θεωρούν απαραίτητο ο ψηφοφόρος να έχει την δυνατότητα να ακυρώσει την ψήφο του, δηλαδή να μην φαίνεται ότι ψήφισε προηγουμένως.

Οι πιο κάτω λειτουργίες δεν αφορούν άμεσα τη διαδικασία ψηφοφορίας, αλλά έχουν βοηθητικό χαρακτήρα και βελτιώνουν την εμπειρία χρήσης της εφαρμογής. Οι πιο κάτω απαιτήσεις προέκυψαν από το ερωτηματολόγιο που δόθηκαν στους πιθανούς χρήστες. Όλα τα άτομα όπου απάντησαν το ερωτηματολόγιο θεωρούν ότι είναι απαραίτητο να υπάρχουν οδηγίες χρήσης της εφαρμογής και οι περισσότεροι από αυτούς απάντησαν ότι ένα απλό παράδειγμα είναι ικανοποιητικό. Επίσης, σχεδόν όλα τα άτομα που απάντησαν θεωρούν σημαντικό να υπάρχει η δυνατότητα για προβολή περισσότερων πληροφοριών για κάποιο υποψήφιο, όπως βασικές προσωπικές πληροφορίες για το υποψήφιο, πληροφορίες φοίτησης και πληροφορίες για την πολιτική του εμπειρία. Επιπρόσθετα, η πλειοψηφία των ατόμων που απάντησαν τους ενδιαφέρει να υπάρχει μία οθόνη όπου θα εμφανίζονται ανακοινώσεις που προσθέτουν οι υποψήφιοι ή ο διαχειριστής της εκλογής ώστε να παραμένουν ενημερωμένοι. Ακόμη, υπάρχει ενδιαφέρον η εφαρμογή να στέλνει ηλεκτρονικά μηνύματα

στους ψηφοφόρους με ενημερώσεις για την εκλογική διαδικασία. Όλες οι απαιτήσεις, εκτός η αποστολή ηλεκτρονικών μηνυμάτων, έχουν υλοποιηθεί.

4.4 Απαιτήσεις Ασφάλειας

Οι βασικές απαιτήσεις ασφάλειας της εφαρμογής είναι οι ίδιες απαιτήσεις όπου έχουν όλες οι εφαρμογές ηλεκτρονικής ψηφοφορίας. Αυτές οι απαιτήσεις είναι η μυστικότητα, η ακεραιότητα, η επαλήθευση, η αυθεντικοποίηση, και η διαθεσιμότητα.

Η μυστικότητα μπορεί να επιτευχθεί με την κρυπτογράφηση της ψήφου. Η ψήφος πρέπει παραμείνει κρυπτογραφημένη μέχρι τη φάση μέτρησης του τελικού αποτελέσματος. Επίσης, μόνο τότε πρέπει να δημιουργηθεί το κλειδί αποκρυπτογράφησης, το οποίο πρέπει να έχει πρόσβαση μόνο ο μετρητής, ο οποίος θα αποκρυπτογραφήσει το ψηφοδέλτια και θα υπολογίσει το τελικό αποτέλεσμα. Το κλειδί αποκρυπτογράφησης και τα αποκρυπτογραφημένα ψηφοδέλτια πρέπει να διαγράφονται στο τέλος της διαδικασίας υπολογισμού του τελικού αποτελέσματος. Επίσης, ο διαχειριστής, ο οποίος γνωρίζει την ταυτότητα του ψηφοφόρου, δεν πρέπει να έχει ποτέ πρόσβαση στην αποκρυπτογραφημένη ψήφο, ούτε να αποθηκεύει την κρυπτογραφημένη ψήφο ώστε να μην μπορεί να δημιουργηθεί σύνδεσμος μεταξύ ψηφοφόρου και ψήφου. Επιπλέον, ο μετρητής και το κοινό δεν πρέπει να έχουν πρόσβαση στην ταυτότητα του ψηφοφόρου.

Η ακεραιότητα της ψήφου και αποτελέσματος μπορεί να εγγυηθεί με τους ακόλουθους τρόπους. Κάθε ψηφοδέλτιο πρέπει να είναι κρυπτογραφημένο σε όλη τη διάρκεια επικοινωνίας για να μην μπορεί να αλλαχθεί και να περιέχει την υπογραφή του ψηφοφόρου ή του διαχειριστή για απόδειξη εγκυρότητας. Επίσης, ο μετρητής οποίος αποθηκεύει τα ψηφοδέλτια και ο διαχειριστής ο οποίος τα υπογράφει, δεν πρέπει να έχουν την δυνατότητα να μεταβάλουν τα ψηφοδέλτια. Επιπλέον, ο μετρητής πρέπει να μετράει όλα τα έγκυρα ψηφοδέλτια και να υπολογίζει σωστά το αποτέλεσμα.

Ο βασικός τρόπος επαλήθευσης είναι ο κωδικός επαλήθευσης. Ο κάθε ψηφοφόρος θα έχει ένα κωδικό επαλήθευσης όπου μπορεί να τον χρησιμοποιεί για να μάθει την κατάσταση του ψηφοδελτίου του. Κάθε κωδικός επαλήθευσης έχει 3 καταστάσεις. Η πρώτη κατάσταση είναι ότι δεν ανήκει σε κάποιο ψηφοδέλτιο στο μετρητή, άρα η ψήφος δεν καταχωρήθηκε ή διαγράφηκε. Η δεύτερη κατάσταση είναι ότι το ψηφοδέλτιο βρίσκεται στο μετρητή, άρα να ανήκει στα ψηφοδέλτια που θα μετρηθούν ή στα παλιά ψηφοδέλτια που έχουν αντικατασταθεί και θα αγνοηθούν. Η τρίτη κατάσταση είναι αν το ψηφοδέλτιο έχει μετρηθεί

ή όχι, όλα τα παλιά ψηφοδέλτια θα θεωρούνται ότι έχουν μετρηθεί παρόλο που δεν μετρήθηκαν. Ο κωδικός επαλήθευσης πρέπει να είναι ανώνυμος και να μην λειτουργεί σαν απόδειξη ψήφου ή αντικατάστασης ψήφου κάποιου υποψήφιου. Επιπλέον, πρέπει να υπάρχει μία λίστα με κάποιες βασικές πληροφορίες της εκλογικής διαδικασίας, ώστε να εκλεχθεί ότι δεν έγινε οτιδήποτε παράνομο. Η λίστα περιέχει τις ακόλουθες πληροφορίες: το σύνολο εμφανίσεων του κάθε ονόματος (first name) των ψηφοφόρων, το σύνολο του κάθε domain του ηλεκτρονικού ταχυδρομείου ("@emaildomain.com") των ψηφοφόρων, το σύνολο των πιθανών ψηφοφόρων, το σύνολο των ατόμων που ψήφισαν, το σύνολο των ψηφοδελτίων, που θα μετρηθούν, και το σύνολο το ψηφοδελτίων που αντικαταστάθηκαν.

Όσο αφορά την αυθεντικοποίηση του ψηφοφόρου, η υπεύθυνη οντότητα είναι ο διαχειριστής. Ο διαχειριστής είναι υπεύθυνος να επιβεβαιώσει ότι ο ψηφοφόρος δικαιούται να λάβει μέρος στις εκλογές και ότι το ψηφοδέλτιο έχει τη ψηφιακή υπογραφή του ψηφοφόρου. Ο διαχειριστής δεν πρέπει να δίνει τη υπογραφή του σε μη έγκυρα άτομα ή να χρησιμοποιεί τα προσωπικά δεδομένα του χρήστη για κάποιο άλλο λόγο. Επίσης, στην είσοδο της εφαρμογής και πριν την καταχώρηση ψήφου πρέπει να υπάρχει αυθεντικοποίηση μέσω ονόματος και κωδικού, ώστε μόνο έγκυρα άτομα να μπορούν να καταχωρήσουν τη ψήφο τους. Πιο συγκεκριμένα ο κωδικός του χρήστη συγκρίνεται με τον κατακερματισμένο κωδικό του στη βάση δεδομένων και αν ταιριάζουν, τότε η αυθεντικοποίηση είναι επιτυχής. Η επιτυχημένη αυθεντικοποίηση είναι απαραίτητη για ένα άτομο να αποκτήσει την υπογραφή του διαχειριστή στο ψηφοδέλτιο του.

Η διαθεσιμότητα υπάρχει όταν το σύστημα είναι προσβάσιμο από όλους του φοιτητές που έχουν το δικαίωμα να ψηφίσουν. Αυτό απαιτεί τη διαδικασία αυθεντικοποίησης να λειτουργά σωστά και να μην απαγορεύει έγκυρους χρήστες να ψηφίζουν. Επιπλέον απαιτεί γρήγορους εξυπηρετητές που μπορούν να ικανοποιούν όλες τις εισερχόμενες αιτήσεις. Επίσης, υπάρχουν μέθοδοι ανάκαμψής, όπως «try/catch block», όταν υπάρχει πρόβλημα με την επικοινωνία, δηλαδή δεν απαντάει ο εξυπηρετητής για κάποιο λόγο.

4.5 Απαιτήσεις Ευχρηστίας

Σε αυτό το υποκεφάλαιο θα αναφερθούν οι απαιτήσεις ευχρηστίας του συστήματος. Αυτές οι απαιτήσεις είναι οι 10 κανόνες του Jakob Nielsen [13,22]. Ο στόχος τους είναι η αύξηση της ευχρηστίας ενός συστήματος, δηλαδή η αποδοτική, αποτελεσματική και ικανοποιητική χρήση του συστήματος από κάθε χρήστη.

Ο πρώτος κανόνας είναι η ορατότητα της κατάστασης του συστήματος. Οι χρήστες πρέπει να είναι ενήμεροι για την κατάσταση του συστήματος μέσα από συνεχή και άμεση ανατροφοδότηση. Για παράδειγμα πρέπει να υπάρχουν μηνύματά που δείχνουν το όνομα της πράξης όπου εκτελείται και πόσο χρόνο χρειάζεται ώστε να ολοκληρωθεί. Επίσης, πρέπει να υπάρχει ενημέρωση σε ποια οθόνη βρίσκεται ο χρήστης.

Ο δεύτερος κανόνας είναι η συμφωνία του συστήματος με τον έξω κόσμο. Η εφαρμογή πρέπει να χρησιμοποιεί μόνο λέξεις και εκφράσεις όπου είναι γνωστές στο χρήστη. Δεν πρέπει να χρησιμοποιεί εξειδικευμένες λέξεις όπου είναι γνωστές μόνο σε άτομα που ασχολούνται με την ηλεκτρονική ψηφοφορία. Επίσης, τα στοιχεία διεπαφής πρέπει να έχουν την αναμενόμενη λειτουργία χρήσης. Για παράδειγμα χρησιμοποιούνται λέξεις όπως: “back”, “next”, “submit” και “exit”, οι οποίες είναι εύκολα κατανοητές.

Ο τρίτος κανόνας είναι ο έλεγχος και ελευθερία του χρήστη. Ο χρήστης πρέπει να την δυνατότητα να σταματήσει μία πράξη που εκτελείται ή να επανέλθει στην προηγούμενη κατάσταση. Για παράδειγμα, στην διαδικασία ψηφοφορίας ο χρήστης μπορεί να αλλάξει την επιλογή του ή να αλλάξει γνώμη και να μην ψηφίσει καθόλου, όσο δεν έχει καταχωρήσει τη ψήφο του.

Ο τέταρτος κανόνας είναι συνοχή και συμμόρφωση έναντι προτύπων. Η εφαρμογή πρέπει να ακολουθεί τα πρότυπα που υπάρχουν στις άλλες ιστοσελίδες και εφαρμογές. Επίσης, πρέπει να υπάρχει συνέπεια μεταξύ των λειτουργιών και εμφάνισης της. Για παράδειγμα, η γραμματοσειρά, το μέγεθος γραμμάτων, τα διαστήματα, το χρώμα γραμμάτων, τα μηνύματα που εμφανίζονται, τα κουμπιά και εικονίδια πρέπει να έχουν μια σταθερή εμφάνιση.

Ο πέμπτος κανόνας είναι η πρόσληψη σφαλμάτων. Η εφαρμογή πρέπει να αποτρέπει τη δημιουργία σφαλμάτων. Για παράδειγμα πρέπει να υπάρχουν προειδοποιητικά μηνύματα για πράξεις που δεν μπορούν να αναιρεθούν, όπως μήνυμα καταχώρησης τελικού ψήφου. Ακόμη, πρέπει να υπάρχουν έλεγχοι ώστε το σύστημα να μην επιτρέπει στο χρήστη να φτάσει σε σφάλμα, για παράδειγμα έλεγχος εγκυρότητας ψηφοδελτίου βάσει των εκλογικών κανόνων, ώστε να μην είναι άκυρη η ψήφος.

Ο έκτος κανόνας είναι αναγνώριση και όχι ανάκληση. Ο χρήστης δεν πρέπει να θυμάται πληροφορία από άλλες οθόνες στο σύστημα, άρα κάθε οθόνη πρέπει να περιέχει σύντομες οδηγίες. Η πληροφορία όπου απαιτείται πρέπει να είναι ορατή και να αποκτάτε εύκολα. Για παράδειγμα, σε κάθε βήμα στη διαδικασία ψηφοφορίας να υπάρχει μία σύντομη οδηγία προς

το χρήστη. Επίσης, ο ψηφοφόρος δεν πρέπει να εισάγει το όνομα της παράταξης ή υποψήφιου που επιθυμεί, υπάρχουν δύο λίστες όπου επιλέγει την παράταξη και το υποψήφιο που θέλει.

Ο έβδομος κανόνας είναι προσαρμοστικότητα και αποδοτικότητα χρήσης. Η εφαρμογή πρέπει να είναι αποδοτική, δηλαδή η χρήση της να είναι γρήγορη και οι πράξεις να είναι απλές και με λίγα βήματα. Η διαδικασία ψηφοφορίας και επαλήθευσης πρέπει να γίνονται σε λιγότερο από 1 λεπτό για έμπειρους χρήστες και λιγότερο από 5 λεπτά για μη έμπειρους χρήστες. Επίσης, η διαδικασία ψηφοφορίας πρέπει να αποτελείται από 5 απλά βήματα. (Επιλογή παράταξής, επιλογή ψηφοφόρου, τελικός έλεγχος ψηφοδελτίου και καταχώρηση κωδικού, επαλήθευση ή έξοδος.) Επιπλέον, το σύστημα προσφέρει 2 επιλογές προσαρμοστικότητας, τη δυνατότητα απόκρυψης του ψευδώνυμου και την δυνατότητα απόκρυψης της ένδειξη ότι έχει ψηφίσει προηγουμένως.

Ο όγδοος κανόνας είναι καλαισθητικός σχεδιασμός. Το περιεχόμενο της πληροφορίας πρέπει να είναι απλό και να εξυπηρετεί το σκοπό του χρήστη. Δεν πρέπει να υπάρχει μη αναγκαία πληροφορία. Επίσης, πρέπει να έχει καλή εμφάνιση.

Ο ένατος κανόνας είναι βοήθεια, αναγνώριση, διάγνωση και ανάκαμψη από λάθη. Τα μηνύματα σφάλματος πρέπει να εκφράζονται σε απλή γλώσσα, να υποδεικνύουν με ακρίβεια το πρόβλημα και να προτείνουν εποικοδομητικά μια λύση. Αν η λύση είναι μεγαλύτερη από μία πρόταση ή δεν υπάρχει λύση, τότε ο χρήστης πρέπει να έχει την δυνατότητα να μιλήσει με την τεχνική υποστήριξη. Για παράδειγμα, αν ο χρήστης εισάγει λάθος κωδικό ή ψηφίσει περισσότερους υποψήφιους από το όριο, θα εμφανιστεί η κατάλληλη οδηγία για ανάκαμψη από το λάθος.

Ο δέκατος κανόνας είναι βοήθεια και εγχειρίδια. Πρέπει να υπάρχει εγχειρίδιο με οδηγίες για να βοηθήσει τους χρήστες να ολοκληρώσουν το στόχο τους. Οι οδηγίες πρέπει να εξηγούν ολόκληρη την διαδικασία ψηφοφορίας με απλό και κατανοητό τρόπο. Για παράδειγμα, υπάρχει μία οθόνη στην εφαρμογή που περιέχει τις οδηγίες της διαδικασίας ψηφοφορίας.

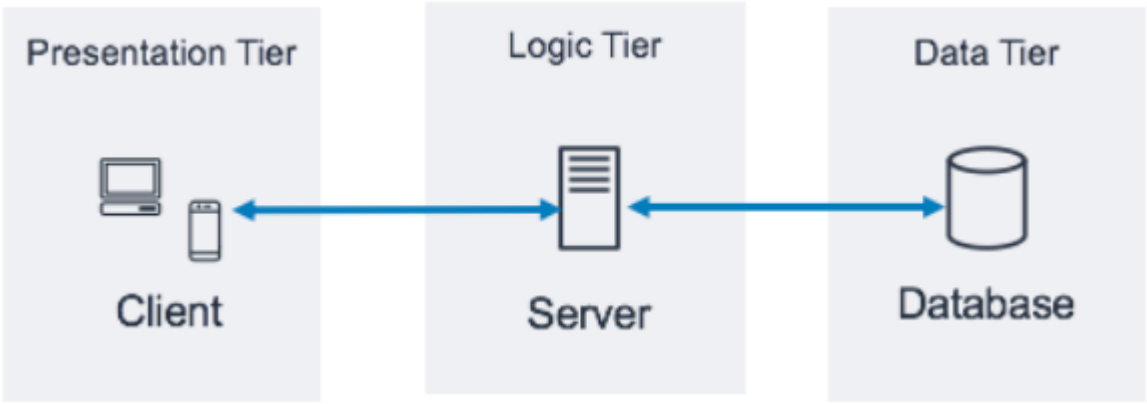
4.6 Οντότητες (Βάσεις δεδομένων)

Το πρωτόκολλο αυτό αποτελείται από 5 οντότητες. Τα έμπιστα άτομα, το ψηφοφόρο, το διαχειριστή, το μετρητή και το κοινό. Μόνο ο διαχειριστής, ο μετρητής και το κοινό έχουν

βάση δεδομένων. Σε αυτό το κεφάλαιο θα αναλυθεί η κάθε οντότητα και αν υπάρχει, η βάση δεδομένων της.

Αρχικά θα αναφερθούν οι δύο οντότητες όπου δεν έχουν βάση δεδομένων. Τα έμπιστα άτομα είναι ένα σύνολο φυσικών ατόμων που ο καθένας γνωρίζει ένα διαφορετικό κομμάτι του κωδικό για να δημιουργηθούν τα κλειδιά κρυπτογράφησης. Μόνο με όλους του κωδικούς μπορεί να δημιουργηθεί το κλειδί κρυπτογράφησης και αποκρυπτογράφησης. Ο ψηφοφόρος είναι το άτομο που χρησιμοποιεί την εφαρμογή για να ψηφίσει. Οι λειτουργίες του ψηφοφόρου θα αναλυθούν στο κεφάλαιο 4.8.

Στη συνέχεια θα αναλυθούν οι οντότητες όπου έχουν βάση δεδομένων, δηλαδή ο διαχειριστής, μετρητής και το κοινό. Η επικοινωνία με τη βάση δεδομένων γίνεται με την αρχιτεκτονική των 3 επιπέδων (3-tier architecture) [31][33]. Το πρώτο επίπεδο είναι το επίπεδο παρουσίασης (presentation tier). Ο βασικός του σκοπός είναι να παρουσιάζει και να συλλέγει πληροφορία από το χρήστη. Το δεύτερο επίπεδο είναι το επίπεδο λογικής (logic tier). Ο βασικός του σκοπός είναι η επεξεργασία πληροφορίας που συλλέχθηκε από το επίπεδο παρουσίας, σε κάποιες περιπτώσεις γίνεται χρήση της πληροφορίας που βρίσκεται στο επίπεδο δεδομένων κατά τη διάρκεια επεξεργασίας. Το τρίτο επίπεδο είναι το επίπεδο είναι το επίπεδο δεδομένων (data tier). Ο βασικός του σκοπός είναι η αποθήκευση και διαχείριση δεδομένων. Όλοι η επικοινωνία περνάει από το δεύτερο επίπεδο, το πρώτο και τρίτο επίπεδό δεν επικοινωνούν απευθείας μεταξύ τους. Για παράδειγμα, αν ο ψηφοφόρος θέλει να λάβει κάποια πληροφορία από τη βάση δεδομένων του μετρητή, τότε επικοινωνεί με το php πρόγραμμα του μετρητή, ακολούθως το php πρόγραμμα του μετρητή επικοινωνεί με την βάση δεδομένων του μετρητή. Στη συνέχεια, το php πρόγραμμα του μετρητή λαμβάνει τη πληροφορία από τη βάση δεδομένων του και στέλνει τη πληροφορία στο ψηφοφόρο. Το php πρόγραμμα μεταφράζει την αίτηση του του ψηφοφόρου (JSON αντικείμενο) στη κατάλληλη διαδικασία (procedure) και το php πρόγραμμα μεταφράζει το αποτέλεσμα της διαδικασίας (procedure) της βάσης δεδομένων σε JSON αντικείμενο, πριν να το στείλει στο ψηφοφόρο. Ο σκοπός της χρήσης της αρχιτεκτονική των 3 επιπέδων είναι η ασφάλεια των δεδομένων, αφού ο χρήστης δεν έχει απευθείας πρόσβαση σε αυτά.



Εικόνα 4.1 Η αρχιτεκτονική των 3 επιπέδων.

Ο διαχειριστής είναι η μόνη οντότητα όπου γνωρίζει στοιχεία για τον ψηφοφόρο. Η βασική του λειτουργία είναι η αυθεντικοποίηση του ψηφοφόρου και η υπογραφή των έγκυρων ψηφοδελτίων.

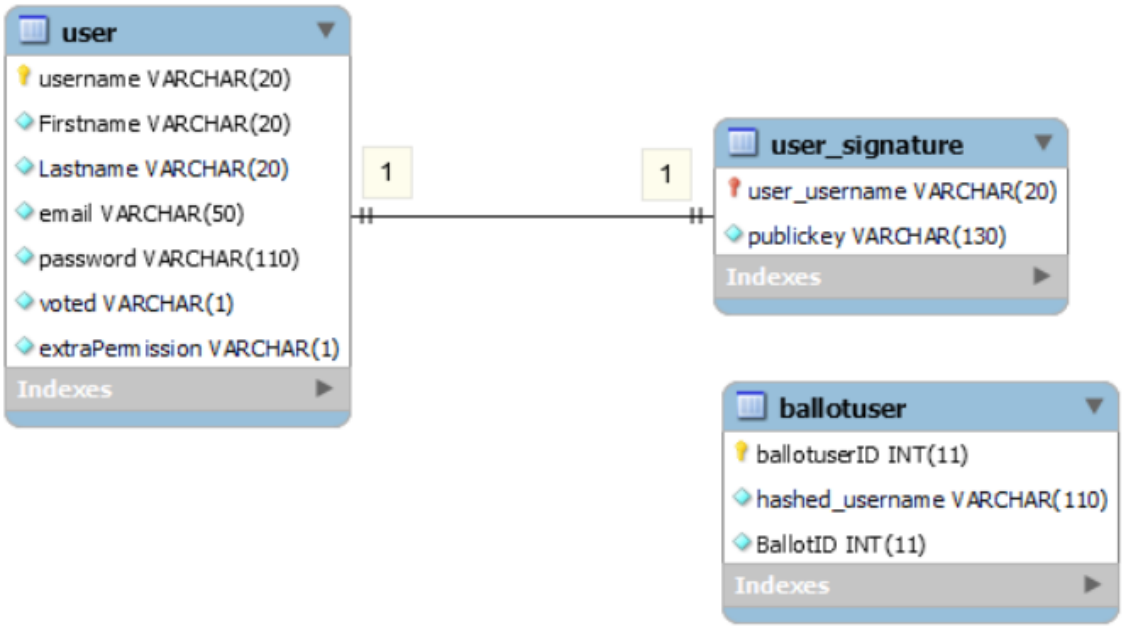
Οι πίνακες που υπάρχουν στη βάση δεδομένων του διαχειριστή είναι:

- ballotuser: Περιέχει τη σχέση κατακερματισμένου ψευδώνυμου και αναγνωριστικό ψηφοδελτίου.
- user: Περιέχει το ψευδώνυμο, όνομα, επίθετο, ηλεκτρονικό ταχυδρομείο, κατακερματισμένο κωδικό, αν ψήφισε και αν έχει επιπλέον δικαιώματα ο χρήστης.
- user_signature: Περιέχει τη σχέση ψευδώνυμου και δημόσιο κλειδί.

Οι λειτουργίες (procedures) της βάσης δεδομένων του διαχειριστή είναι:

- addBallotUser: Προσθήκη σχέσης κατακερματισμένου ψευδώνυμου και αναγνωριστικό ψηφοδελτίου στο πίνακα ballotuser.
- addPassword2Username: Προσθήκη νέας εγγραφής στο πίνακα user ή αν το ψευδώνυμο υπάρχει τότε αντικαθιστά μόνο τον κατακερματισμένο κωδικό.
- addPublicKey: Προσθήκη νέας εγγραφής στο πίνακα user_signature ή αν το ψευδώνυμο υπάρχει τότε αντικαθιστά μόνο το δημόσιο κλειδί.
- deleteBallotUser: διαγραφή μίας εγγραφής στο ballotuser
- getPassword: Επιστρέφει τον κατακερματισμένο κωδικό ενός χρήστη.
- getTotalUserVoted: Επιστρέφει τον αριθμό των χρηστών όπου ψήφισαν τουλάχιστο μία φορά.
- existsKey: Επιστέφει αν υπάρχει ή όχι το δημόσιο κλειδί του χρήστη.
- getBallotUser: Επιστρέφει όλες τις εγγραφές του πίνακα ballotUser
- getUserBasicInfo: Επιστρέφει το όνομα και ηλεκτρονικό ταχυδρομείο ενός χρήστη.

- getUserFullname: Επιστρέφει το όνομα και επίθετο ενός χρήστη.
- getUserKey: Επιστρέφει το δημόσιο κλειδί ενός χρήστη.
- getUsernames: Επιστρέφει όλα τα ψευδώνυμα από το πίνακα user.
- getUserPermision: Επιστρέφει «Y» ή «N» , αν ο χρήστης έχει επιπλέον δικαιώματα.
- getVoted: Επιστρέφει «Y» ή «N» , αν ο χρήστης ψήφησε τουλάχιστον 1 φορά.
- setUserPermission: Θέτει αν ο χρήστης έχει επιπλέον δικαιώματα.
- setVotedNo: Θέτει ότι ο χρήστης δεν έχει ψηφίσει
- setVotedYes: Θέτει ότι ο χρήστης έχει ψηφίσει



Εικόνα 4.2 Μοντέλο οντότητας–συσχετίσεων (Entity-Relation Diagram) της βάσης δεδομένων του διαχειριστή.

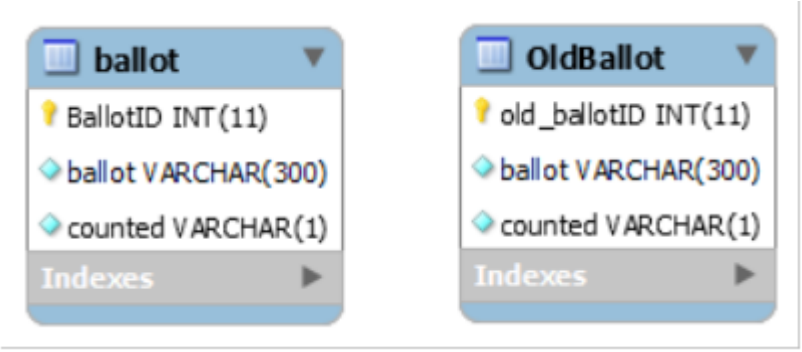
Στη συνέχεια θα αναφερθεί ο μετρητής. Ο μετρητής είναι η μόνη οντότητα που αποθηκεύει το κρυπτογραφημένο ψηφοδέλτιο του χρήστη. Ο μετρητής, με τη χρήση του κωδικού επαλήθευσης του ψηφοφόρου, ενημερώνει το ψηφοφόρο για την κατάσταση του ψηφοδελτίου του. Επίσης, ο μετρητής υπολογίζει το τελικό αποτέλεσμα.

Οι πίνακες που υπάρχουν στη βάση δεδομένων του μετρητή είναι:

- ballot: περιέχει το αναγνωριστικό, περιεχόμενο του ψηφοδελτίου και αν έχει μετρηθεί.
- oldBallot: περιέχει το αναγνωριστικό, περιεχόμενο και αν έχει μετρηθεί. (Σε αυτό το πίνακα αποθηκεύονται τα ψηφοδέλτια που έχουν αντικατασταθεί, άρα δεν θα μετρηθούν στην πραγματικότητα.)

Οι λειτουργίες (procedures) της βάσης δεδομένων του μετρητή είναι:

- addBallot: προσθήκη νέου ψηφοδελτίου στο πίνακα Ballot.
- getBallots: Επιστρέφει τις εγγραφές του πίνακα ballot
- getBothBallotTables: Επιστρέφει τις εγγραφές του πίνακα ballot και oldBallot.
- getTotalBallots: Επιστρέφει το πλήθος των εγγραφών στον πίνακα ballot.
- getTotalOldBallots: Επιστρέφει το πλήθος των εγγραφών στον πίνακα oldBallot.
- replaceBallotFromID: Αντικατάσταση ψηφοδελτίου στο πίνακα ballot και προσθήκη του προηγούμενο ψηφοδελτίου στο πίνακα oldBallot.
- setCounted: Θέτει ότι έχει μετρηθεί το ψηφοδέλτιο στο πίνακα ballot.
- UpdateOldBallotCounted: Θέτει ότι έχουν μετρηθεί όλα τα ψηφοδέλτια στο πίνακα oldBallot .



Εικόνα 4.3 Μοντέλο οντότητας–συσχετίσεων (Entity-Relation Diagram) της βάσης δεδομένων του μετρητή.

Στο τέλος θα αναφερθεί το κοινό. Το κοινό δεν αποθηκεύει κρίσιμες πληροφορίες όπως τα δεδομένα του ψηφοφόρου ή κρυπτογραφημένα ψηφοδέλτια. Οι πληροφορίες που έχει μπορούν να είναι δημοσίως γνωστές. Στο κοινό υπάρχουν τα δεδομένα των ανακοινώσεων, υποψήφιων, παρατάξεων και το αποτέλεσμα. Ο σκοπός του είναι να μειωθεί η επικοινωνία του ψηφοφόρου με το μετρητή και διαχειριστή.

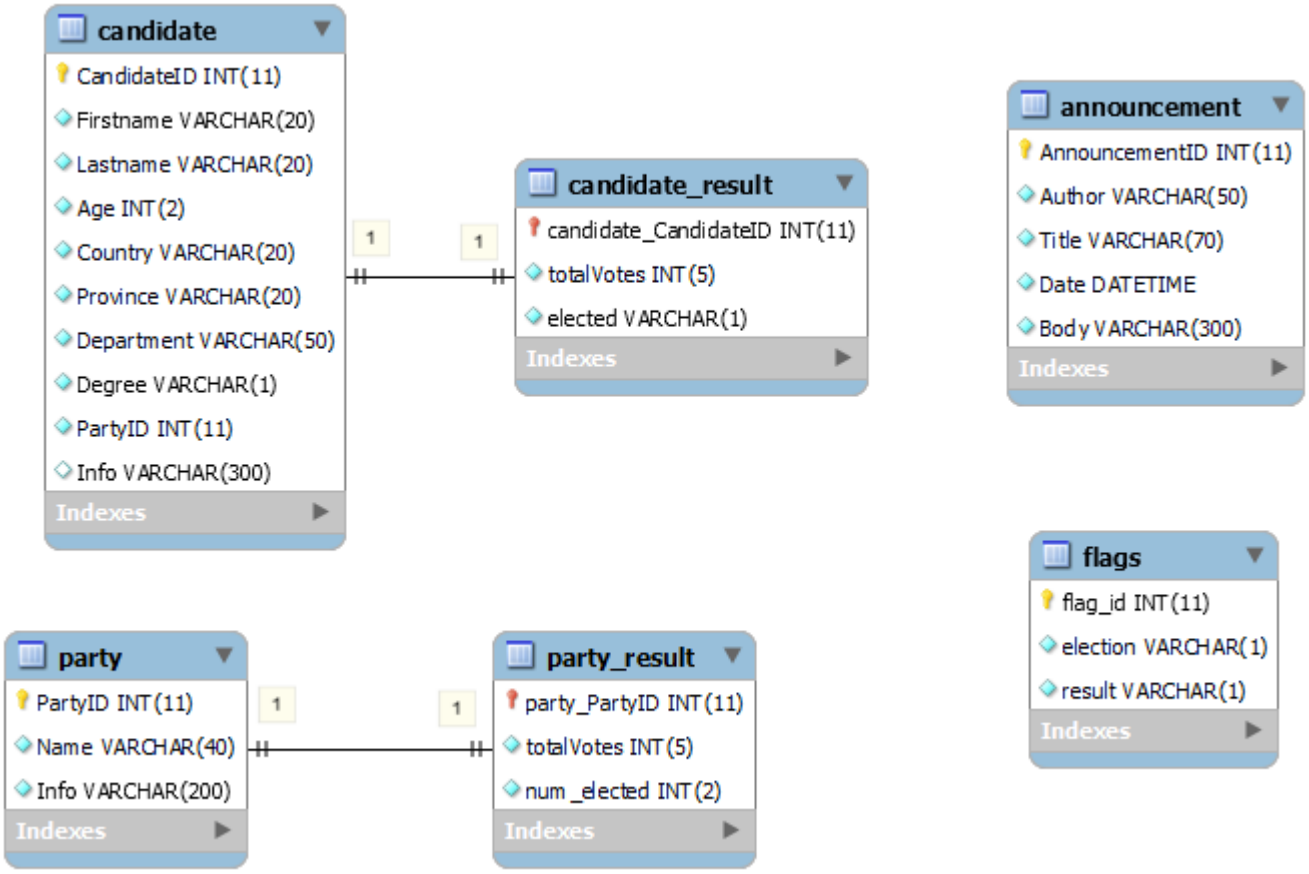
Οι πίνακες που υπάρχουν στη βάση δεδομένων του κοινού είναι:

- announcement: Περιέχει το αναγνωριστικό της ανακοίνωσης, το όνομα του συγγραφέα, τον τίτλο, ημερομηνία και το σώμα της ανακοίνωσης.
- candidate: Περιέχει το αναγνωριστικό του υποψήφιου, το όνομα, επίθετο, ηλικία, χώρα, επαρχία, τμήμα σπουδών, είδος σπουδής (προπτυχιακή, master, Ph. D), αναγνωριστικό της παράταξης που ανήκει, λίγες πληροφορίες για αυτό.

- candidate_result: Περιέχει το αναγνωριστικό του υποψηφίου, τις συνολικές ψήφους που έλαβε και αν εκλέχθηκε.
- flags: Περιέχει πληροφορίες αν ξεκίνησε η εκλογική διαδικασία και αν ανακοινώθηκε το αποτέλεσμα.
- party: Περιέχει το αναγνωριστικό της παράταξης, το όνομα της παράταξης και λίγες πληροφορίες για αυτή.
- party_result: Περιέχει το αναγνωριστικό της παράταξης, τους συνολικούς ψήφους και το αριθμό μελών που εκλέχθηκαν.

Οι λειτουργίες (procedures) της βάσης δεδομένων του κοινού είναι:

- addAnnouncement: προσθήκη εγγραφής στον πίνακα announcement.
- addCandidateResult: προσθήκη εγγραφής στον πίνακα candidate_result.
- addPartyResult: προσθήκη εγγραφής στον πίνακα party_result.
- getAnnouncements: Επιστρέφει τις εγγραφές του πίνακα announcement.
- getCandidateBasic: Επιστρέφει τις εγγραφές του πίνακα candidate και το όνομα της παράταξης που ανήκει ο κάθε υποψήφιος από το πίνακα party.
- getCandidateResult: Επιστρέφει τις εγγραφές του πίνακα candidate και candidate_result.
- getCandidatesIDwithPartyID: Επιστρέφει όλα τα ζευγάρια αναγνωριστικών ενός υποψήφιου και το αναγνωριστικό της παράταξης που ανήκουν.
- getFlagElection: Επιστρέφει «1» ή «0», αν ξεκίνησαν οι εκλογές.
- getFlagResult: Επιστρέφει «1» ή «0», αν ανακοινώθηκε το τελικό αποτέλεσμα.
- getPartyData: Επιστρέφει τις εγγραφές του πίνακα party.
- getPartyIDs: Επιστρέφει όλα τα αναγνωριστικά των παρατάξεων του πίνακα party.
- getPartyResult: Επιστρέφει τις εγγραφές του πίνακα party και party_result.
- setFlagElection: Θέτει την εκλογική διαδικασία σε ενεργή (ξεκίνησε) ή όχι.
- setFlagResult: Θέτει ότι το τελικό αποτέλεσμα ανακοινώθηκε ή όχι.
- getCandidateFull: : Επιστρέφει όλες τις πληροφορίες για ένα υποψήφιο από το πίνακα candidate και το όνομα της παράταξης που ανήκει ο κάθε υποψήφιος από το πίνακα party.



Εικόνα 4.4 Μοντέλο οντότητας–συσχετίσεων (Entity-Relation Diagram) της βάσης δεδομένων του κοινού.

4.7 Πρωτόκολλο ψηφοφορίας του συστήματος ηλεκτρονικής ψηφοφορίας.

Σε αυτό το υποκεφάλαιο θα εξηγηθεί το πρωτόκολλο που θα χρησιμοποιηθεί στο σύστημα ηλεκτρονικής ψηφοφορίας. Πιο συγκεκριμένα θα επεξηγηθούν οι οντότητες και θα αναλυθούν τα στάδια του πρωτοκόλλου. Το πρωτόκολλο είναι βασισμένο σε μεγάλο βαθμό στο πρωτόκολλο των Fujioka, Okamoto και Ohta και το πρωτόκολλο των Juels, Catalano και Jakobsson. Επίσης, είναι βασισμένο σε μικρό βαθμό στο σύστημα ηλεκτρονικής ψηφοφορίας Helios.

Το πρώτο στάδιο είναι το στάδιο δημιουργίας του κλειδιού κρυπτογράφησης.

1) Το κάθε έμπιστο άτομο έχει ένα μυστικό κωδικό που μόνο αυτός το γνωρίζει.
2) Με την χρήση όλων των κωδικών των έμπιστων ατόμων δημιουργείται μόνο το κλειδί κρυπτογράφησης των ψηφοδελτίων.
3) Ο μετρητής αποθηκεύει το κλειδί κρυπτογράφησης των ψηφοδελτίων.

Το δεύτερο στάδιο είναι το στάδιο της ψηφοφορίας.

1) Ο ψηφοφόρος δημιουργεί το ψηφοδέλτιο του.
2) Ο ψηφοφόρος λαμβάνει το κλειδί κρυπτογράφησης από το μετρητή και το χρησιμοποιεί για να κρυπτογραφήσει το ψηφοδέλτιο του.
3) Ο ψηφοφόρος χρησιμοποιεί το κρυπτογραφημένο ψηφοδέλτιο για να δημιουργήσει το κωδικό επαλήθευσης.
4) Ο ψηφοφόρος υπογράφει το κρυπτογραφημένο ψηφοδέλτιο με το ιδιωτικό του κλειδί.
5) Ο ψηφοφόρος στέλνει στον διαχειριστή την υπογραμμένη το κρυπτογραφημένο ψηφοδέλτιο και την ταυτότητα του.

Το τρίτο στάδιο είναι το στάδιο της αυθεντικοποιήσης του ψηφοφόρου.

1) Ο διαχειριστής ελέγχει αν ο ψηφοφόρος έχει το δικαίωμα να ψηφίσει βάση την ταυτότητα του και αν είναι έγκυρή η υπογραφή του, δηλαδή είναι το άτομο που ισχυρίζεται.
2) Αν ναι τότε αφαιρεί την υπογραφή του ψηφοφόρου, υπογράφει το κρυπτογραφημένο ψηφοδέλτιο και το στέλνει στο ψηφοφόρο.
3) Αν όχι, τότε ο διαχειριστής απορρίπτει την ψήφο.

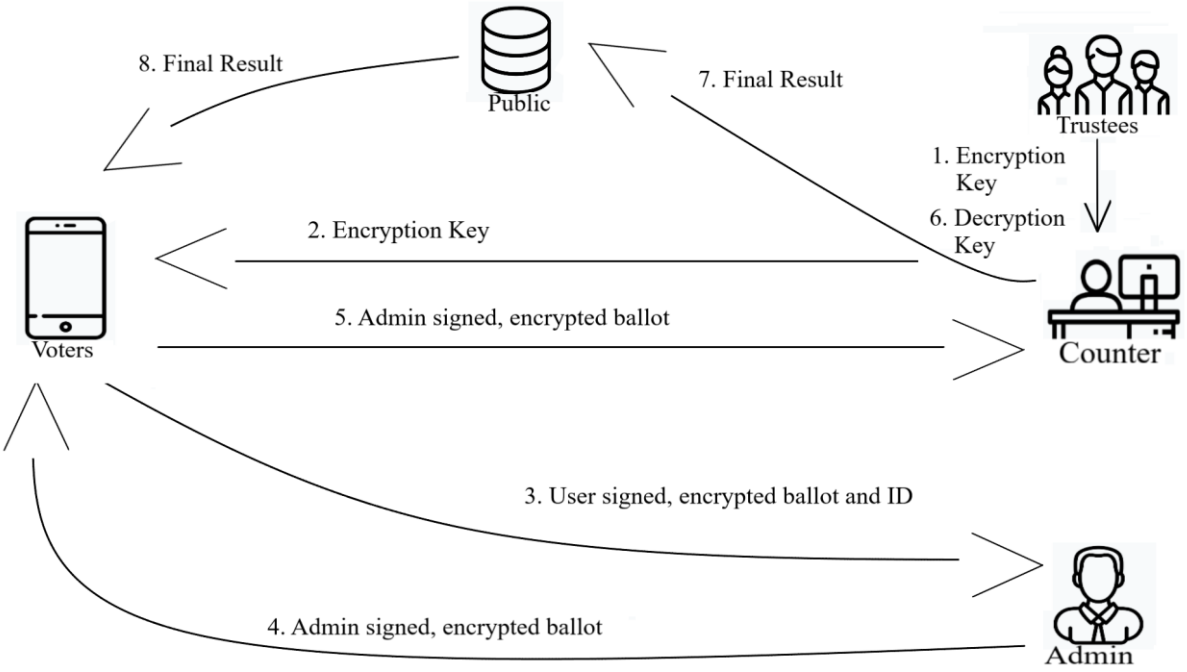
Το τέταρτο στάδιο είναι το στάδιο καταχώρησης της ψήφου.

1) Ο ψηφοφόρος ελέγχει αν το κρυπτογραφημένο ψηφοδέλτιο έχει τη υπογραφή του διαχειριστή. Αν όχι, τότε δεν μπορεί να συνεχίσει τη διαδικασία ψηφοφορίας.
2) Ο ψηφοφόρος στέλνει το κρυπτογραφημένο ψηφοδέλτιο με την υπογραφή του διαχειριστή στο μετρητή.
3) Ο μετρητής ελέγχει την υπογραφή του ψηφοδελτίου (υπογραφή διαχειριστή). Αν ο έλεγχος είναι επιτυχής, τότε αφαιρεί την υπογραφή του διαχειριστή και προσθέτει το ψηφοδέλτιο στη λίστα με τα ψηφοδέλτια.
4) Αν ο ψηφοφόρος έχει είδη ψηφίσει, τότε ο μετρητής μεταφέρει την παλιά ψήφο στο πίνακα με τις αντικατεστημένες ψήφους.
5) Ο ψηφοφόρος μπορεί να χρησιμοποιήσει το κωδικό επαλήθευσης του που έχει δημιουργήσει για να ελέγξει την κατάσταση της ψήφος του.

Το πέμπτο στάδιο είναι το στάδιο της καταμέτρησης της ψήφου.

1) Τα έμπιστα άτομα χρησιμοποιούν τον κωδικό τους για να δημιουργήσουν το κλειδί αποκρυπτογράφησης.

2) Ο μετρητής αποκρυπτογραφεί τις ψήφους και υπολογίζει το τελικό αποτέλεσμα. (Το κλειδί αποκρυπτογράφησης και αποκρυπτογραφημένα ψηφοδέλτια δεν αποθηκεύονται.)
3) Ο μετρητής στέλνει το τελικό αποτέλεσμα στο κοινό. Οι ψηφοφόροι μπορούν να λάβουν το τελικό αποτέλεσμα από το κοινό.



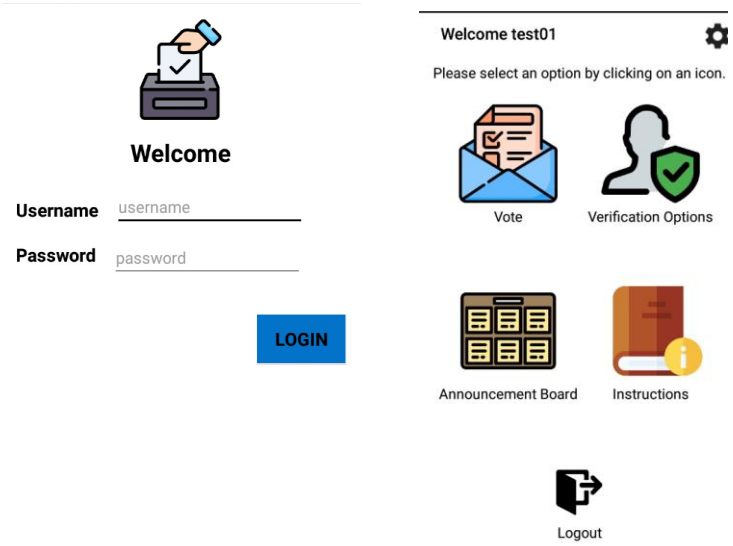
Εικόνα 4.5 Πρωτόκολλο ψηφοφορίας της εφαρμογής. Παρουσιάζει τη ροή σημαντικών δεδομένων στη διαδικασία ψηφοφορίας.

4.8 Εμφάνιση και βασικές λειτουργίες της εφαρμογής

Σε αυτό το υποκεφάλαιο θα αναλυθούν οι βασικές λειτουργίες της android εφαρμογής. Μαζί με την αναφορά των λειτουργιών θα παρουσιαστούν εικόνες που δείχνουν την εμφάνιση αυτών των λειτουργιών. Αυτό το υποκεφάλαιο θα επικεντρωθεί στην android εφαρμογή, δηλαδή οι λειτουργίες θα παρουσιαστούν με επίκεντρο τον χρήστη. Πριν να μπορεί ο χρήστης να χρησιμοποιήσει την εφαρμογή οι οντότητες πρέπει να προσθέσουν στις βάσεις δεδομένων του τις κατάλληλες πληροφορίες για την τρέχον εκλογή και να δημιουργήσουν τα κλειδιά κρυπτογράφησης. Περισσότερες πληροφορίες για την εγκατάσταση της εφαρμογής στο Παράρτημα Δ. Οι πιο κάτω πληροφορίες που φαίνονται αποτελούνται από ψεύτικα δεδομένα.

Η πρώτη οθόνη όπου έρχεται σε επαφή ο χρήστης είναι η οθόνη σύνδεσης. Αρχικά, στο παρασκήνιο γίνεται ανταλλαγή κλειδιών μεταξύ ψηφοφόρου και του διαχειριστή, μετρητή

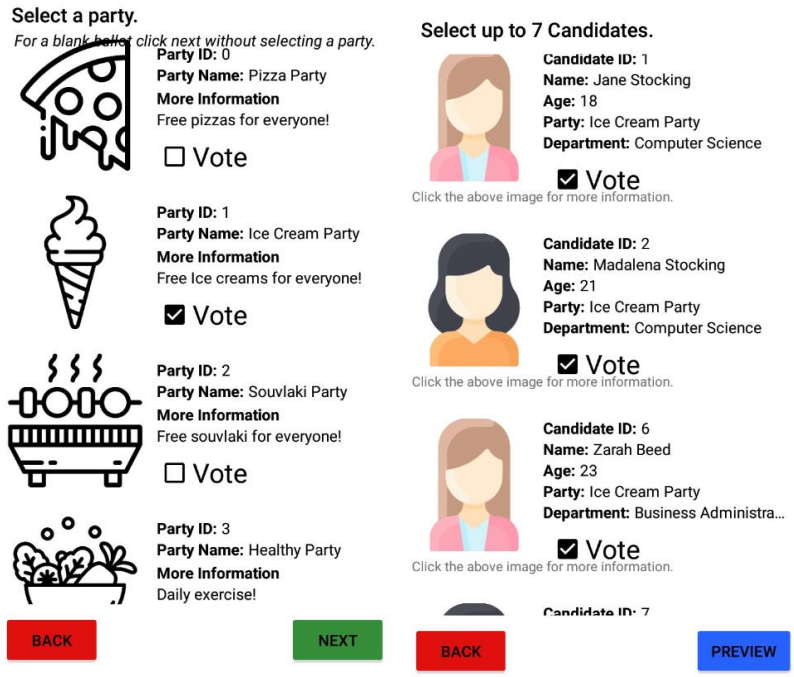
και κοινού, ώστε να υπάρχει κρυπτογραφημένη επικοινωνία μεταξύ τους. Ο ψηφοφόρος πρέπει να εισάγει το όνομα και το κωδικό του, τα οποία στέλνονται στο διαχειριστή για την αυθεντικοποιήση. Ο διαχειριστής χρησιμοποιεί το όνομα του χρήστη για να ανακτήσει το κατακερματισμένο κωδικό του χρήστη. Στη συνέχεια κατακερματίζει το κωδικό που στάλθηκε και ελέγχει αν είναι οι ίδιοι με αυτό στη βάση δεδομένων. Μόνο αν είναι ίδιοι τότε ο χρήστης μπορεί να συνεχίσει. Επίσης, σε αυτό το στάδιο ο ψηφοφόρος στέλνει το δημόσιο του κλειδί στο διαχειριστή.



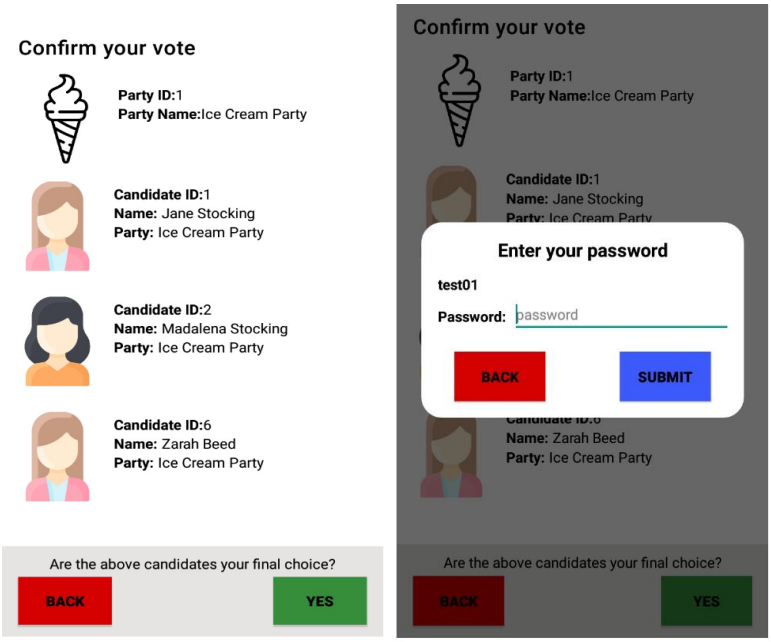
Σχήμα 4.6 Αριστερά είναι η αρχική οθόνη και δεξιά το κύριο μενού.

Η επόμενη λειτουργία που θα αναλυθεί είναι η διαδικασία ψηφοφορίας. Αρχικά ο ψηφοφόρος επιλέγει την πολιτική παράταξη που επιθυμεί και μετά 0 ως 7 υποψήφιους ή 1 υποψήφιο αν ψηφίζει ανεξάρτητο ψηφοφόρο. Αν θέλει να καταχωρήσει λευκό ψηφοδέλτιο, τότε μπορεί να πατήσει “Next” χωρίς να επιλέξει μία πολιτική παράταξη. Ο ψηφοφόρος έχει την ικανότητα να προεπισκοπήσει το ψηφοδέλτιο του. Στο τέλος ο χρήστης εισάγει το κωδικό του για αυθεντικοποίηση. Όταν ο ψηφοφόρος πατήσει το κουμπί καταχώρηση (submit), εκτελούνται 4 βήματα στο παρασκήνιο. Το πρώτο βήμα η λήψη του κλειδιού κρυπτογράφησης από το μετρητή. Το δεύτερο βήμα είναι η κρυπτογράφηση του ψηφοδελτίου. Το τρίτο βήμα είναι η δημιουργία του κωδικού επαλήθευσης, με το κατακερματισμό του κρυπτογραφημένου ψηφοδελτίου. Το τέταρτο βήμα είναι η υπογραφή του ψηφοδελτίου. Ο ψηφοφόρος στέλνει το κρυπτογραφημένο ψηφοδέλτιο υπογραμμένο από το ίδιο, το όνομα και το κωδικό του στο διαχειριστή. Ο διαχειριστής χρησιμοποιεί το όνομα και το κωδικό του ψηφοφόρου για να ελέγξει αν δικαιούται να ψηφίσει και το δημόσιο κλειδί του ψηφοφόρου για να ελέγξει την υπογραφή στο ψηφοδέλτιο. Αν δεν υπάρχει κάποιο λάθος, ο διαχειριστή υπογράφει το κρυπτογραφημένο ψηφοδέλτιο και το στέλνει στο ψηφοφόρο,

όπου ο ψηφοφόρος το στέλνει στο μετρητή. Ο μετρητής ελέγχει την υπογραφεί του διαχειριστή και αν είναι έγκυρη το προσθέτει στη λίστα με τα ψηφοδέλτια. Αν υπάρξει κάποιο σφάλμα, τότε ο ψηφοφόρος ενημερώνεται με το κατάλληλο μήνυμα.



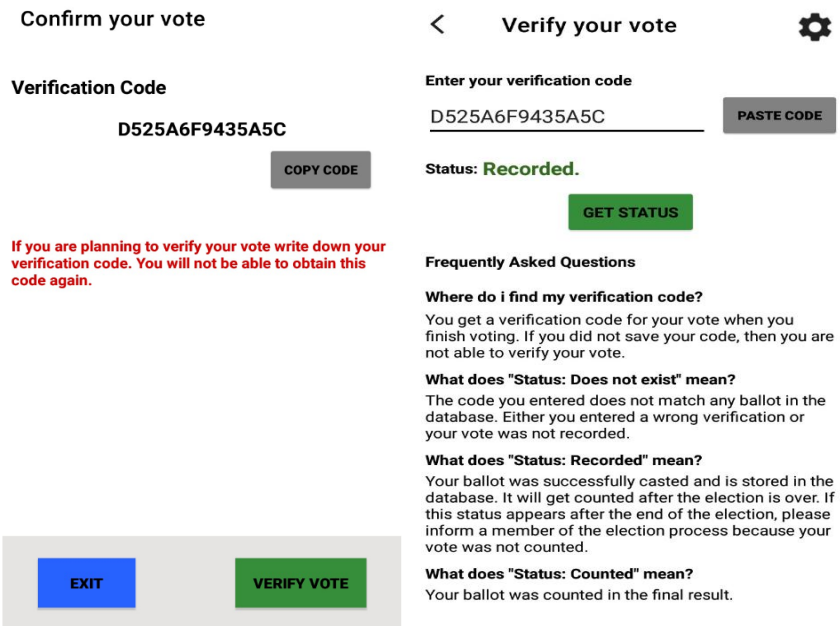
Σχήμα 4.7 Αριστερά είναι η επιλογή παράταξης και δεξιά η επιλογή υποψηφίου της συγκεκριμένης παράταξης.



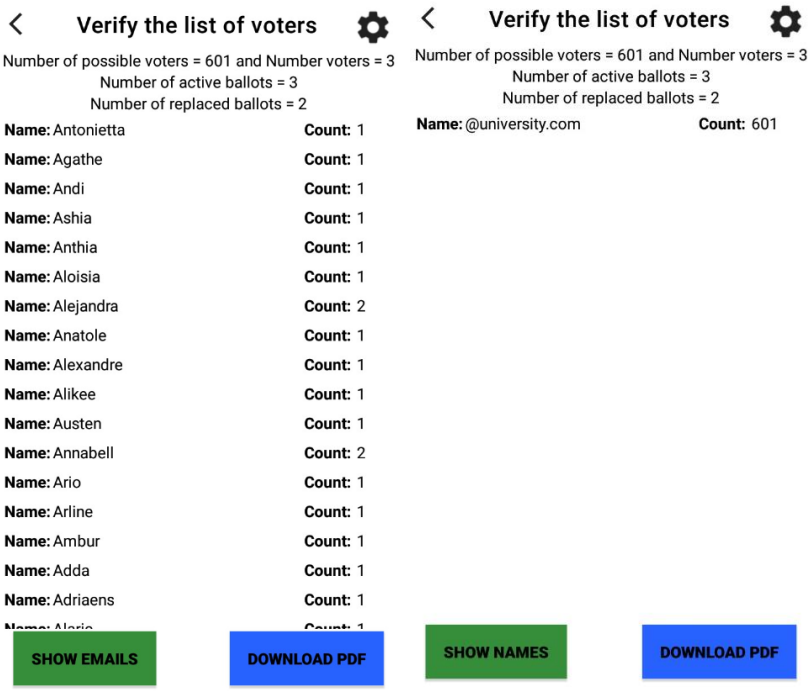
Σχήμα 4.8 Αριστερά είναι η προεπισκόπηση του ψηφοδελτίου και δεξιά η εισαγωγή κωδικού.

Όταν ο ψηφοφόρος τελειώσει με επιτυχία τη διαδικασία ψηφοφορίας, τότε βλέπει το κωδικό επαλήθευσης του. Ο κωδικός επαλήθευσης δημιουργείται από τον ίδιο το ψηφοφόρο, άρα

μόνο ο ίδιος γνωρίζει τον κωδικό αυτό, με αποτέλεσμα αν δεν αποθηκευτεί, τότε δεν μπορεί να το ξανά αποκτήσει. Ο ψηφοφόρος έχει την επιλογή να αποθηκεύσει το κωδικό επαλήθευσης στο clipboard με το πάτημα ενός κουμπιού, ώστε εύκολα να το επικολλήσει σε κάποιο αρχείο για να το αποθηκεύσει. Επίσης έχει την επιλογή για άμεση επαληθεύσει της ψήφου του ή να το πράξει αργότερα. Με την επαλήθευσης της ψήφου, ο κωδικός στέλνεται στο μετρητή, γίνεται έλεγχος αν υπάρχει το ψηφοδέλτιο στη βάση δεδομένων του μετρητή και αν το ψηφοδέλτιο έχει μετρηθεί. Ο μετρητής απαντάει με το κατάλληλο μήνυμα στο ψηφοφόρο. Επιπλέον, κάποια εξουσιοδοτημένα άτομα έχουν την δυνατότητα να ελέγξουν κάποιες πληροφορίες για τους ψηφοφόρους και την εκλογή, ώστε να επιβεβαιώσουν την ακεραιότητα του αποτελέσματος.

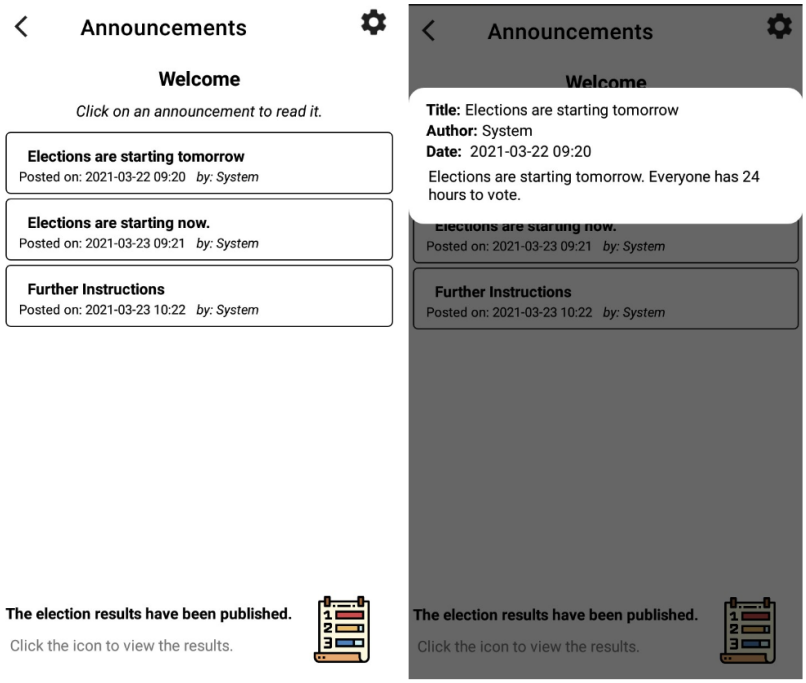


Σχήμα 4.9 Αριστερά είναι η οθόνη λήψης του κωδικού επαλήθευσης και δεξιά είναι η οθόνη επαλήθευσης της ψήφου.

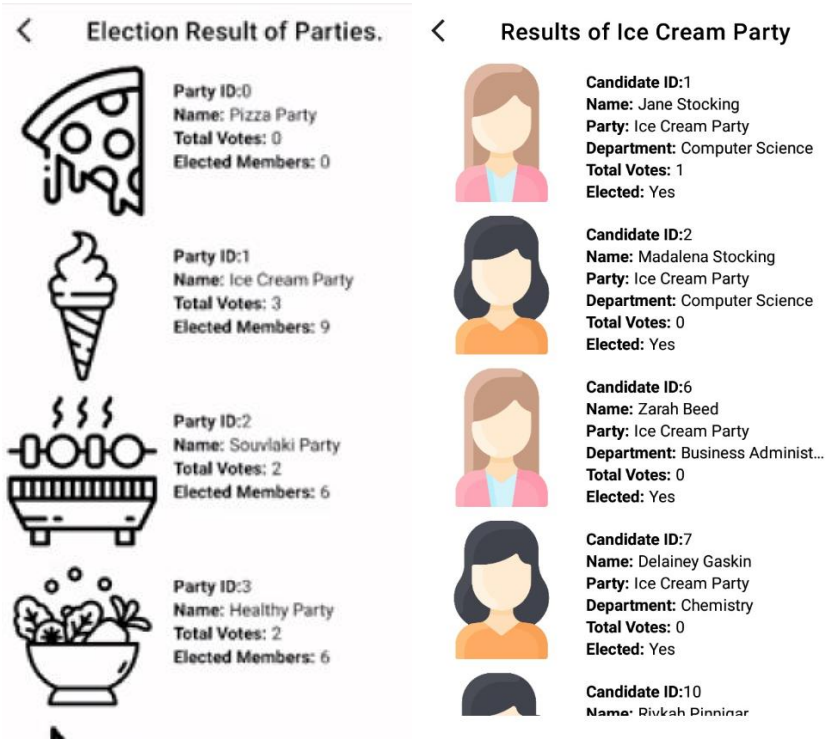


Σχήμα 4.10 Αριστερά είναι η οθόνη με τις μετρήσεις των ονομάτων των ψηφοφόρων και δεξιά είναι η οθόνη με τις μετρήσεις των ηλεκτρονικών ταχυδρομείων.

Ο ψηφοφόρος μπορεί να μεταβεί στην οθόνη των ανακοινώσεων για να ενημερωθεί σε θέματα όπου αφορούν την εκλογή. Αρχικά βλέπει μία λίστα με τις ανακοινώσεις και μπορεί να πατήσει πάνω σε μία ανακοίνωση για να διαβάσει περισσότερες πληροφορίες. Όταν υπολογιστεί το τελικό αποτέλεσμα, θα υπάρχει η ενημέρωση στο κάτω μέρος της σελίδας και ο ψηφοφόρος θα μπορεί να το διαβάσει. Πατώντας το εικονίδιο κάτω αριστερά μπορεί να μεταβεί για να διαβάσει το τελικό αποτέλεσμα. Στην αρχή βλέπει τις ψήφους και των αριθμών εκλεγμένων υποψηφίων για κάθε πολιτική παράταξη και στη συνέχεια μπορεί να πατήσει σε μία παράταξη για να δει τα αποτελέσματα για κάθε υποψήφιους της.



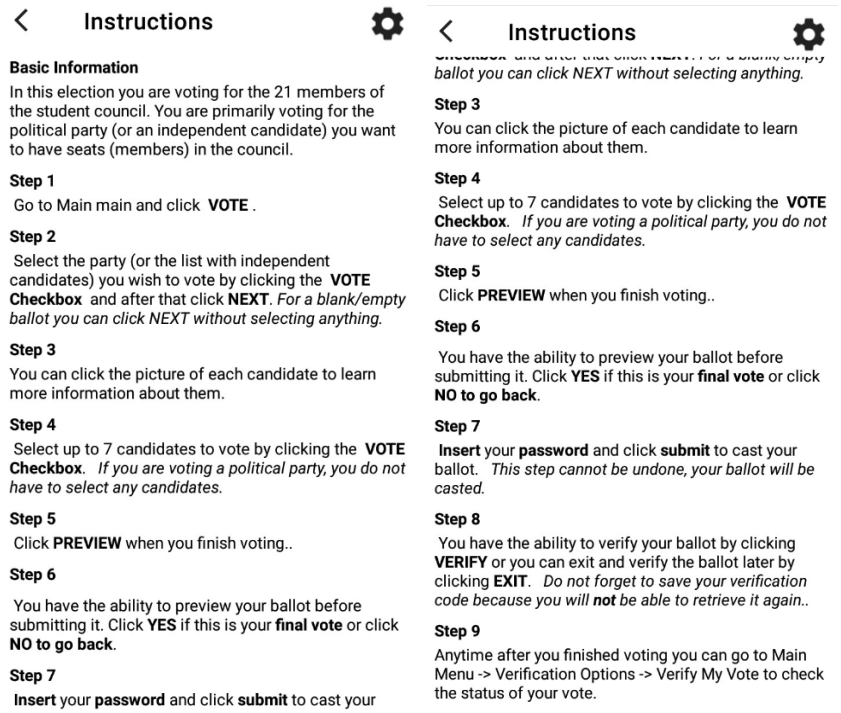
Σχήμα 4.11 Αριστερά είναι η οθόνη με τις ανακοινώσεις και δεξιά περισσότερες πληροφορίες για την πρώτη ανακοίνωση.



Σχήμα 4.12 Αριστερά είναι η οθόνη με τα αποτελέσματα για κάθε παράταξη και δεξιά είναι η οθόνη με τα αποτελέσματα των υποψηφίων μίας συγκεκριμένης παράταξης.

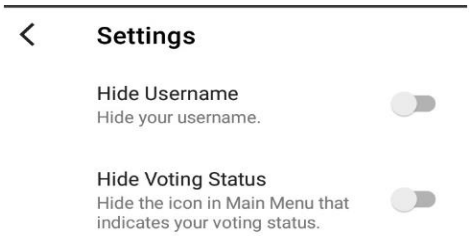
Μία από τις πιο σημαντικές οθόνες είναι η οθόνη με οδηγίες για την εκλογική διαδικασία. Στην αρχή της οθόνης υπάρχουν γενικές πληροφορίες για το σκοπό της εκλογής. Στη συνέχεια υπάρχουν 9 λεπτομερής βήματα που αφορούν την διαδικασία εκλογών και

επαλήθευσης ψηφοδελτίου. Ο ψηφοφόρος δεν είναι ανάγκη να θυμάται τα βήματα επειδή υπάρχουν οδηγίες σε όλοι τη διαδικασία ψηφοφορίας, αλλά είναι πολύ βοηθητικά.

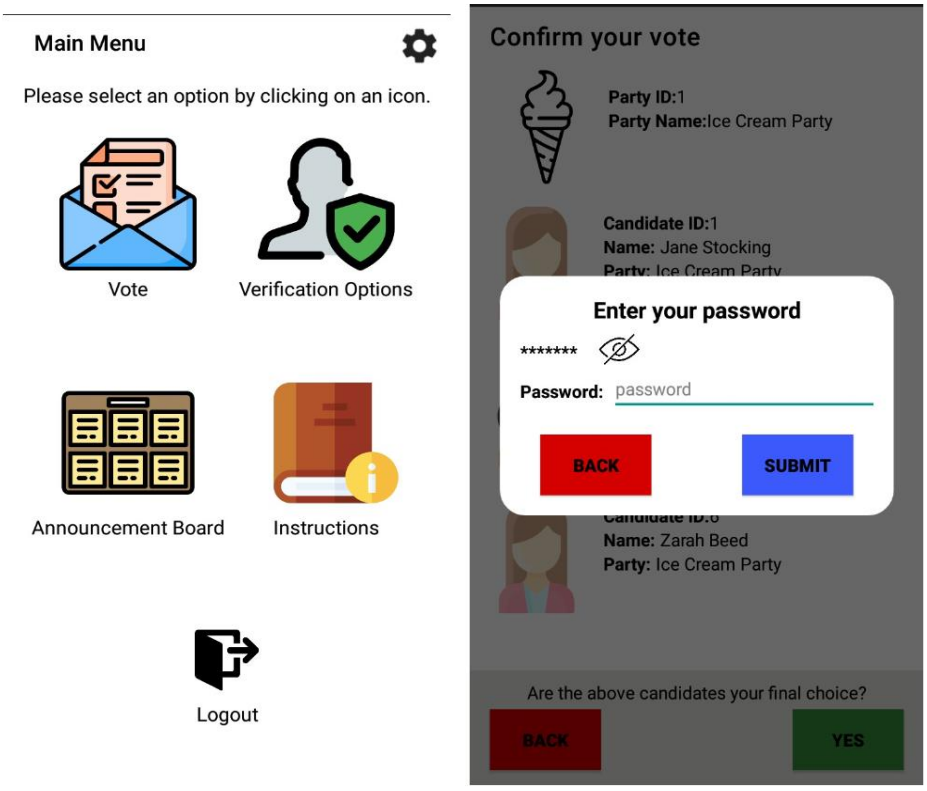


Σχήμα 4.13 Αριστερά και δεξιά είναι οι οθόνες με τις οδηγίες ψηφοφορίας.

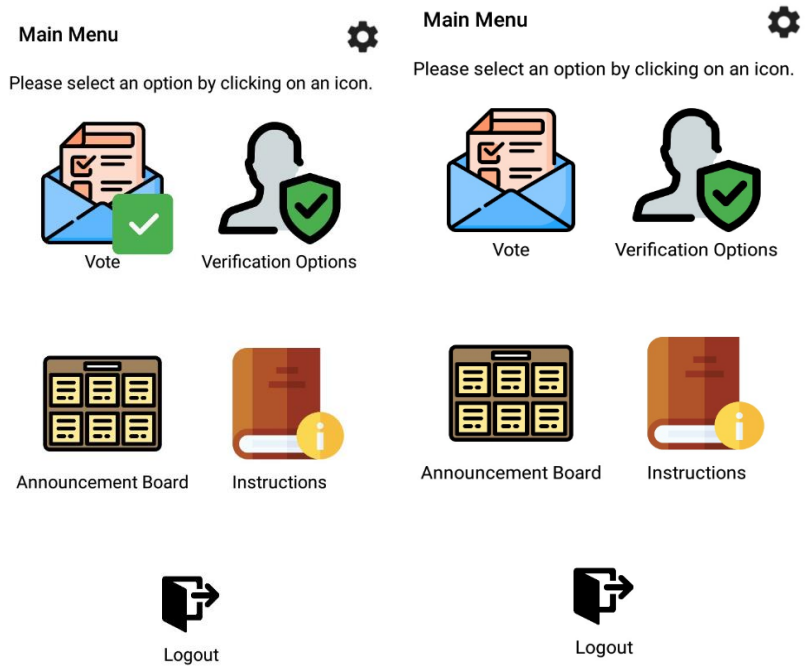
Η τελευταία λειτουργία που έχει μείνει να αναλυθεί είναι οι ρυθμίσεις που προσφέρει η εφαρμογή. Η εφαρμογή προσφέρει μόνο 2 ρυθμίσεις όπου αφορούν την μυστικότητα του χρήστη. Η πρώτη ρύθμιση είναι το κρύψιμο του ονόματος (username) του χρήστη σε όλες τις οθόνες, δηλαδή στο κύριο μενού και διαδικασία ψηφοφορίας. Η δεύτερη ρύθμιση είναι το κρύψιμο της υπόδειξης ότι έχει ψηφίσει ο ψηφοφόρος στο κύριο μενού.



Σχήμα 4.14 Η οθόνη των ρυθμίσεων.



Σχήμα 4.15 Η οθόνη του κυρίως μενού και εισαγωγή κωδικού στη διαδικασία ψηφοφορία όταν η ρύθμιση για κρύψιμο ονόματος είναι ενεργή.



Σχήμα 4.16 Αριστερά είναι το κύριος μενού όταν το κρύψιμο της υπόδειξης ψηφοφορίας είναι ανενεργή και δεξιά είναι όταν είναι ενεργή.

Κεφάλαιο 5

Αξιολόγηση του συστήματος

5.1 Εισαγωγή στην αξιολόγηση του συστήματος

Σε αυτό το κεφάλαιο θα γίνει αναφορά στις αξιολογήσεις που έγιναν στο σύστημα ηλεκτρονικής ψηφοφορίας κατά τη διάρκεια υλοποίησης του. Η αξιολόγηση του συστήματος έγινε με την βοήθεια μιας ομάδας από 5 πιθανούς χρήστες, οι οποίοι είναι όλοι φοιτητές του τμήματος πληροφορικής. Η εφαρμογή δόθηκε στου χρήστες με απλές οδηγίες που αφορούν το σκοπό αξιολόγηση. Κατά τη διάρκεια της αλληλεπίδρασης των χρηστών με την εφαρμογή γινόταν συλλογή των ανατροφοδοτήσεων τους. Μετά από την συλλογή ανατροφοδότησης, γινόταν επεξεργασία σε αυτά τα δεδομένα για εξαγωγή των πιθανών αλλαγών που πρέπει να πραγματοποιηθούν. Οι αλλαγές γίνονται μόνο αν συνεισφέρουν στην βελτίωση των απαιτήσεων του συστήματος.

Κατά τη φάση υλοποίησης του συστήματος υλοποιήθηκαν τρεις αξιολογήσεις, μία αξιολόγηση σε κάθε πρωτότυπο. Το πρώτο πρωτότυπο δημιουργήθηκε στην αρχή της υλοποίησης του συστήματος, περιείχε μόνο την διεπαφή χρήστη και ο σκοπός του ήταν να αξιολογηθεί η διεπαφή χρήστη και το μοντέλο πλοήγησης μεταξύ των οθονών. Στο δεύτερο πρωτότυπο υπήρχε ολοκληρωμένη η διαδικασία ψηφοφορίας και η διαδικασία επαλήθευσης ψήφου. Ο σκοπός του δεύτερου πρωτοτύπου ήταν να αξιολογηθεί κυρίως η διαδικασία ψηφοφορίας και επαλήθευσης, αλλά υπήρχε ανατροφοδότηση για ολόκληρη την εφαρμογή. Το τρίτο πρωτότυπο δημιουργήθηκε στο τέλος της φάσης υλοποίησης, περιείχε όλες τις

λειτουργίες της εφαρμογής και ο σκοπός του ήταν να αξιολογηθούν οι αλλαγές που έγιναν στις προηγούμενες αξιολογήσεις και να βρεθούν οποιαδήποτε λάθη, ατέλειες υπάρχουν. Η τελική αξιολόγηση έγινε στο τελικό σύστημα, δηλαδή μετά την διαδικασία της τρίτης αξιολόγησης και ο σκοπός της είναι να εξεταστεί αν το σύστημα ικανοποιεί της απαιτήσεις ασφάλειας των συστημάτων ηλεκτρονικής ψηφοφορίας. Επιπλέον πραγματοποιήθηκε μία αξιολόγηση των απαιτήσεων ευχρηστίας, δηλαδή των 10 κανόνων του Jakob Nielsen. Επίσης, υπάρχει μία σύγκριση του συστήματος που έχει υλοποιηθεί με το σύστημα διαδικτυακής ψηφοφορίας της Εσθονίας.

5.2 Πρώτη αξιολόγηση, πρωτότυπο

Σε αυτό το υποκεφάλαιο θα γίνει αναφορά στις στην πρώτη αξιολόγηση, δηλαδή την αξιολόγηση του πρώτου πρωτότυπου. Ο σκοπός της αξιολόγησης είναι ο έλεγχος της διεπαφής χρήστης, ώστε να βελτιωθεί και να γίνει πιο φιλική προς τους χρήστες. Το πρωτότυπο που δόθηκε για έλεγχο είχε ολοκληρωμένη την διεπαφή χρήστη και κάποιες βασικές λειτουργίες όπου την αφορούν, όπως η πλοήγηση μεταξύ οθονών και εμφάνιση πληροφοριών από την βάση δεδομένων. Οι διαδικασίες όπου αφορούν την εκλογή δεν ολοκληρώθηκαν, αλλά χρησιμοποιήθηκαν ψεύτικα δεδομένα, ώστε να βοηθήσουν τους χρήστες να αξιολογήσουν την εφαρμογή. Στην συνέχεια θα αναφερθούν οι 5 πιο σημαντικές παρατηρήσεις.

Η πρώτη παρατήρηση αφορά την διάταξη των οθονών στην διαδικασία ψηφοφορίας και προβολή των τελικών αποτελεσμάτων. Στο κάτω μέρος της οθόνης υπάρχει ένα μενού όπου ο χρήστης επιλέγει την φοιτητική παράταξη που θέλει και στη συνέχεια εμφανίζονται οι υποψήφιοι αυτής της παράταξης. Με αυτό τον τρόπο δεν υπάρχουν πληροφορίες για την φοιτητική παράταξη, το οποίο είναι αναγκαίο επειδή ο ψηφοφόρος ψηφίζει και την παράταξη που επιθυμεί, όχι μόνο τους υποψήφιους της. Η εισήγηση για λύση είναι το μενού με τις παρατάξεις να μεταφερθεί στη δική του οθόνη, πριν από την εμφάνιση των υποψήφιων. Σε αυτή την οθόνη, θα εμφανίζονται πληροφορίες για τις παρατάξεις και επιλέγοντας μια φοιτητική παράταξη θα εμφανίζονται πληροφορίες για τους υποψήφιους της. Αυτή η εισήγηση υλοποιήθηκε.

Η δεύτερη παρατήρηση αφορά τον κωδικό επαλήθευσης. Στην οθόνη που εμφανίζεται ο κωδικός επαλήθευσης, στο τέλος της διαδικασίας ψηφοφορίας, ο χρήστης πρέπει να σημειώσει σε μία κόλλα τον κωδικό επαλήθευσης για να τον θυμάται, ώστε να μπορεί να τον πληκτρολογήσει στην οθόνη επαλήθευσης της ψήφου. Η εισήγηση για λύση είναι ένα

κουμπί, στη οθόνη που εμφανίζεται ο κωδικός επαλήθευσης, όπου θα φυλάει το κωδικό στο πρόχειρο (clipboard). Επίσης, άλλο ένα κουμπί, στην οθόνη επαλήθευσης της ψήφου, δηλαδή στην οθόνη όπου πρέπει να πληκτρολογηθεί ο κωδικός επαλήθευσης, που θα επικολλάει τον κωδικό επαλήθευσης. Αυτή η εισήγηση υλοποιήθηκε αφού κάνει πιο εύχρηστη και εύκολη τη διαδικασία επαλήθευσης.

Η τρίτη παρατήρηση αφορά την γενική εμφάνιση των οθονών. Υπάρχουν κάποιες οθόνες όπου τα στοιχεία τους είναι συγκεντρωμένα στο πάνω μέρος της οθόνης, ενώ υπάρχει αρκετός ελεύθερος χώρος στην υπόλοιπη οθόνη. Επίσης, υπάρχουν άλλες περιπτώσεις όπου τα στοιχεία είναι πολύ αραιά και σπαταλούν αρκετό χώρο στην οθόνη. Επιπρόσθετα, υπάρχουν περιπτώσεις όπου η πληροφορία έχει μικρό μέγεθος και πρέπει να είναι μεγαλύτερη ώστε να είναι πιο εύκολα ορατή. Η εισήγηση για λύση είναι η αναδιάταξη των στοιχείων ώστε να σπαταλούν τον κατάλληλο χώρο, να έχουν το σωστό μέγεθος και να υπάρχει περισσότερη συνοχή στην εμφάνιση. Αυτή η εισήγηση υλοποιήθηκε.

Η τέταρτη παρατήρηση είναι τα χρώματα και εικονίδια που εμφανίζονται στην οθόνη. Κάποια άτομα προτιμούν να υπάρχουν περισσότερα χρώματα π.χ. γαλάζιο φόντο. Επίσης, κάποια εικονίδια χαρακτηρίστηκαν ως παιδικά το οποίο δεν ταιριάζει σε μία εφαρμογή ηλεκτρονικής ψηφοφορίας. Η εισήγηση για λύση είναι η χρήση κάποιων χρωμάτων όπως μπλε, γαλάζιο και διαφορετικά εικονίδια. Οι αλλαγές δεν χαρακτηρίστηκαν σημαντικές από τους χρήστες, έτσι έγιναν μόνο κάποιες αλλαγές σε εικονίδια όπου δεν ταίριαζα στην εφαρμογή.

Η πέμπτη παρατήρηση αφορά την πρόσβαση στην οθόνη των αποτελεσμάτων. Η οθόνη των αποτελεσμάτων είναι προσβάσιμη μόνο μέσω της οθόνης των ανακοινώσεων και όχι από την οθόνη του κυρίως μενού. Η εισήγηση είναι να υπάρχει κουμπί για πρόσβαση της οθόνη των αποτελεσμάτων από το κυρίως μενού. Ο λόγος που έγινε αυτή η εισήγηση είναι επειδή το κουμπί για την πρόσβαση στην οθόνη των αποτελεσμάτων δεν ήταν εύκολα ορατή. Αυτό που υλοποιήθηκε είναι το εξής. Το κουμπί για την πλοηγήσει στην οθόνη των αποτελεσμάτων θα είναι στο κάτω μέρος της οθόνης μαζί με το μήνυμα αν τα αποτελέσματα ανακοινώθηκαν ή όχι. Αν ανακοινώθηκαν τα αποτελέσματα ο χρήστης θα πατάει το κουμπί για να τα διαβάσει, αλλιώς δεν θα είναι ορατό το κουμπί αφού δεν υπάρχουν αποτελέσματα για να τα διαβάσει.

5.3 Δεύτερη αξιολόγηση, πρωτότυπο

Σε αυτό το υποκεφάλαιο θα γίνει αναφορά στις στην δεύτερη αξιολόγηση, δηλαδή την αξιολόγηση του δεύτερου πρωτότυπου. Στο δεύτερο πρωτότυπο υπήρχε ολοκληρωμένη η διαδικασία ψηφοφορίας και επαλήθευσης. Ο σκοπός αυτής της αξιολόγησης ήταν συλλογή ανατροφοδότησης για την η διαδικασία ψηφοφορίας και επαλήθευσης, αλλά υπήρχε ανατροφοδότηση για ολόκληρη την εφαρμογή. Οι περισσότερες παρατηρήσεις ήταν θετικές, η διαδικασία ψηφοφορίας, με εξαίρεση κάποιων μικρών προβλημάτων, λειτούργησε όπως αναμενόταν. Στην συνέχεια θα αναφερθούν οι 5 πιο σημαντικές παρατηρήσεις.

Η πρώτη παρατήρηση αφορά την εμφάνιση τη διεπαφής του χρήστη. Έγιναν διάφορες εισηγήσεις για να αλλαχθεί η διάταξη των οθονών και της πληροφορίας που υπάρχει στις οθόνες, ώστε να ταυτίζεται περισσότερο με το νοητικό μοντέλο πλοήγησης του χρήστη. Επίσης, έγιναν εισηγήσεις για χρήση χρωμάτων στο κείμενο ή έντονου φόντου για να επισημανθεί η σημαντική πληροφορία και να είναι ευκολότερα ορατή. Επιπρόσθετα, έγιναν παρατηρήσεις για την χρήση διαφορετικού μεγέθους γραμμάτων, είδος κουμπιών και χρωμάτων χωρίς να υπάρχει λόγος. Οι εισηγήσεις ήταν εύστοχες με αποτέλεσμα να υλοποιηθούν.

Η δεύτερη παρατήρηση αφορά τις οδηγίες που εμφανίζονται στην οθόνη. Παρόλο που υπάρχει οθόνη με οδηγίες, οι χρήστες το θεωρούν απαραίτητο να υπάρχουν σύντομες οδηγίες στη διαδικασία ψηφοφορίας. Για παράδειγμα το μέγιστο αριθμό ψηφοφόρων δικαιούνται να ψηφίσουν, τη δυνατότητα για κενό ψηφοδέλτιο και τη δυνατότητα να αντικαταστήσουν την ψήφο τους. Επίσης, υπήρχαν περιπτώσεις όπου οι χρήστες δεν ήταν σίγουροι ποια είναι η επόμενη κίνηση για να πλοηγηθούν στην επόμενη οθόνη ή αγνοούσαν λειτουργίες στην παρόν οθόνη. Τα προβλήματα που αναφέρουν αυτές οι εισηγήσεις είναι σοβαρά αφού μειώνουν την ευχρηστία της εφαρμογής σε μεγάλο βαθμό, με αποτέλεσμα να προστεθούν σύντομες οδηγίες για να βοηθούν τους χρήστες.

Η τρίτη παρατήρηση αφορά την πλοήγηση μεταξύ οθονών. Υπήρχαν λίγες περιπτώσεις όπου ο χρήστης παγιδευόταν σε μία οθόνη, αφού δεν μπορούσε να πάει στην προηγούμενη οθόνη για λόγους ασφάλειας. Έγιναν αλλαγές σε όλες στις οθόνες, ώστε ο χρήστης να μπορεί πάντα να πηγαίνει στην οθόνη του κυρίου μενού, με λίγα βήματα, από οποιαδήποτε οθόνη.

Η τέταρτη παρατήρηση αφορά την ανίχνευση λαθών στη διαδικασία εκλογών. Το πρώτο μεγάλο λάθος είναι ότι το λευκό ψηφοδέλτιο δεν λειτουργούσε, ο χρήστης ήταν αναγκασμένος να ψηφίσει μία παράταξη. Το δεύτερο μεγάλο λάθος είναι ότι ο χρήστης μπορούσε να επιλέξει πολλαπλές φοιτητικές παρατάξεις να ψηφήσει, ενώ το όριο είναι μόνο

μία. Αυτά τα δύο λάθη είναι αντίθετα σε σχέση με τις απαιτήσεις του συστήματος με αποτέλεσμα να διορθωθούν ώστε να λειτουργούν όπως αναμένεται.

Η πέμπτη παρατήρηση αφορά την επίδοση του συστήματος. Η αξιολόγηση της εφαρμογής έγινε με μεγάλο αριθμό δεδομένων τα οποία, παρόλο που είναι ψεύτικα, μοιάζουν αρκετά με τα αληθινά. Αυτό είχε ως αποτέλεσμα να εμφανιστούν περιπτώσεις στη διαδικασία ψηφοφορίας όπου ο χρήστης πρέπει να περιμένει αρκετά δευτερόλεπτα για το επόμενο βήμα. Η εισήγηση των χρηστών ήταν να μειωθεί ο χρόνος αναμονής όπου είναι δυνατός. Έγινε έλεγχος στο σύστημα και ανακαλύφθηκε ότι οι μέθοδοι κρυπτογράφησης μείωναν την επίδοση. Υπήρχαν κάποιες περιπτώσεις, για παράδειγμα στον κατακερματισμό (hashing) κάποιων δεδομένων, όπου είναι δυνατό να χρησιμοποιηθεί πιο γρήγορος αλγόριθμος, χωρίς να επηρεάζεται σημαντικά η ασφάλεια και η μυστικότητα του χρήστη.

5.4 Τρίτη αξιολόγηση, πρωτότυπο

Σε αυτό το υποκεφάλαιο θα γίνει αναφορά στις στην τρίτη αξιολόγηση, δηλαδή την αξιολόγηση του τρίτου πρωτότυπου. Στο τρίτο πρωτότυπο υπάρχουν όλες οι λειτουργίες και ο σκοπός αξιολόγησης του είναι η ανίχνευσης και διόρθωσης των πιθανών λαθών. Αυτό είναι το τελικό πρωτότυπο και μετά από την διόρθωση των λαθών θα παραχθεί το τελικό σύστημα. Στην συνέχεια θα αναφερθούν οι 5 πιο σημαντικές παρατηρήσεις.

Η πρώτη παρατήρηση αφορά το κωδικό επαλήθευσης της ψήφου. Ο σκοπός του κωδικού επαλήθευσης είναι να ενημερώσει το χρήστη για την κατάσταση της ψήφου του. Υπάρχουν 3 πιθανές καταστάσεις, ο κωδικός δεν ανήκει σε κάποια ψήφο στη βάση δεδομένων, ο κωδικός ανήκει σε κάποια ψήφο στη βάση δεδομένων και ο κωδικός ανήκει σε κάποια ψήφο που μετρήθηκε στη βάση δεδομένων. Όταν ο χρήστης αντικαθιστούσε την ψήφο του, η παλιά ψήφος διαγραφόταν από την βάση δεδομένων, έτσι ο παλιός κωδικός επαλήθευσης επιστρέφει ότι η ψήφος δεν υπάρχει στη βάση δεδομένων. Αυτό είναι πρόβλημα γιατί ο κάτοχος του παλιού κωδικού επαλήθευσης γνωρίζει αν ο ψηφοφόρος αντικατάστησε τη ψήφο του. Με αποτέλεσμα ένα ύπουλο άτομο να έχει την δυνατότητα να αναγκάσει το ψηφοφόρο να ψηφίσει ένα συγκεκριμένο υποψήφιο και το ύπουλο άτομο να γνωρίζει αν ο υποψήφιος άλλαξε τη ψήφο του. Ο τρόπος αντιμετώπισης είναι η δημιουργία ενός δεύτερου πίνακα στη βάση δεδομένων με τις παλιές ψήφους. Αυτές οι ψήφοι θα φαίνονται ότι ανήκουν στη βάση δεδομένων μαζί με τις έγκυρες ψήφους, αλλά θα αγνοηθούν στη διαδικασία μέτρησης. Με αυτή την αλλαγή ένα ύπουλο άτομο δεν θα γνωρίζει αν ο ψηφοφόρος

αντικατάστησε τη ψήφο του ή όχι, έτσι ο ψηφοφόρος θα μπορεί να αλλάξει τη ψήφο του χωρίς φόβο.

Η δεύτερη παρατήρηση αφορά την αντικατάσταση της ψήφου. Ο χρήστης είχε την επιλογή να επιλέξει αν θέλει ο ίδιος να έχει την δυνατότητα να αντικαταστήσει τη ψήφο του ή όχι. Η επιλογή του ήταν τελειωτική, άρα αν επίλεγε «όχι» και καταχωρούσε τη ψήφο του, δεν θα μπορούσε να την αντικαταστήσει. Κατά τη διάρκεια της αξιολόγησης οι χρήστες δήλωσαν ότι θα ήταν πιο απλό να είχαν πάντα την επιλογή να αντικαθιστούν την ψήφο τους. Επίσης, η δυνατότητα επιλογής αντικατάστασης ψήφου, αναιρούσε τα πλεονεκτήματα της, δηλαδή την πώληση ψήφου και τον εξαναγκασμό, αφού μπορεί να αποδεχτεί ποια επιλογή προτίμησε ο χρήστης ή και να εξαναγκαστεί να επιλέξει μία επιλογή. Το τελικό σύστημα δεν θα δίνει την επιλογή αντικατάστασης ψήφου, όλοι οι ψηφοφόροι θα έχουν την ικανότητα να αντικαταστήσουν τη ψήφο τους, ώστε να μην μπορούν να πωλήσουν τη ψήφο τους ή να εξαναγκαστούν να ψηφίσουν ένα υποψήφιο.

Η τρίτη παρατήρηση αφορά την εμφάνιση των υποψηφίων και πολιτικών παρατάξεων. Το ψηφοδέλτιο του υποψηφίου περιέχει τα αναγνωριστικά των υποψηφίων και πολιτικών παρατάξεων. Όμως, η εφαρμογή δεν έδειχνε το αναγνωριστικό τους, αλλά χρησιμοποιούσε τα ονόματα, ώστε να γνωρίζει ο ψηφοφόρος ποια επιλογή ψηφίζει. Μαζί με το όνομα του κάθε υποψήφιου ή παράταξης θα εμφανίζεται και το αναγνωριστικό τους, ώστε ο χρήστης να γνωρίζει το περιεχόμενο του ψηφοδελτίου του. Αυτό καταπολεμά τυχόν προσπάθεια της οντότητας κοινού να αλλάξει τα αναγνωριστικά της παράταξης ή των υποψηφίων, ώστε να ξεγελάσει τους υποψηφίους να ψηφίσουν κάποια άλλη επιλογή.

Η τέταρτη παρατήρηση αφορά την διαδικασία ψηφοφορίας. Ο ψηφοφόρος είχε τη δυνατότητα να συνεχίζει να ψηφίζει μετά το τέλος της διαδικασίας ψηφοφορίας. Αυτό είναι ξεκάθαρα λάθος, έτσι πρέπει να διορθωθεί. Έγιναν οι απαραίτητες αλλαγές ώστε η εφαρμογή να μην επιτρέπει στον ψηφοφόρο να ψηφίζει και ο μετρητής δεν αποδέχεται ψηφοδέλτια όταν τελειώσει η διαδικασία ψηφοφορίας ή υπολογιστεί το τελικό αποτέλεσμα.

Η πέμπτη παρατήρηση αφορά τις περιπτώσεις όπου μπορεί η εφαρμογή να σταματήσει να λειτουργεί λόγω προβλημάτων στην εκτέλεση του κωδικού. Παρατηρήθηκαν ότι υπήρχε απότομη διακοπή της λειτουργίας της εφαρμογής, ιδιαίτερα σε περιπτώσεις όπου υπάρχει επικοινωνία με τους εξυπηρετητές (server). Σε όλες τις περιοχές που υπάρχει πιθανότητα για την απότομη διακοπή της εκτέλεσης της εφαρμογής (crash), έγινε προσθήκη try/catch block, ώστε να αποτρέψει την διακοπή λειτουργίας. Επίσης, προστέθηκαν διάφορα μηνύματα

λαθών, ώστε ο χρήστης να γνωρίζει ποιο είναι το λάθος του και αν είναι αναγκαίο, ποιες ενέργειες πρέπει να πράξει.

5.5 Αξιολόγηση ευχρηστίας

Σε αυτό το υποκεφάλαιο θα γίνει αξιολόγησης της ευχρηστίας του συστήματος βάση των 10 κανόνων ευχρηστίας του Jakob Nielsen [13][26]. Ο σκοπός της αξιολόγησης είναι να ελεγχθεί ο βαθμό ευχρηστίας της εφαρμογής. Μία ομάδα από 5 πιθανούς χρήστες έλεγξαν την εφαρμογή και αμέσως μετά απάντησαν το ερωτηματολόγιο. Οι απαντήσεις του ερωτηματολογίου δείχνουν το βαθμό ευχρηστίας της εφαρμογής. Στο τέλος του υποκεφάλαιου υπάρχει ένας πίνακας που συνοψίζει το αποτέλεσμα. Το ερωτηματολόγιο υπάρχει στο Παράρτημα Γ.

Ο πρώτος κανόνας είναι η ορατότητα της κατάστασης του συστήματος. Το σύστημα πρέπει να παρέχει συνεχή και άμεση ανατροφοδότηση στο χρήστη. Η ανατροφοδότηση πρέπει να αναφέρει ποια κατάσταση βρίσκεται ο χρήστης, ποιες λειτουργίες εκτελούνται στο παρασκήνιο του συστήματος και πόσο χρόνο χρειάζονται για να τελειώσουν. Το σύστημα ικανοποιεί αυτό τον κανόνα σε πολύ καλό βαθμό.

Ο δεύτερος κανόνας είναι η συμφωνία του συστήματος με τον έξω κόσμο. Η εφαρμογή πρέπει να χρησιμοποιεί λέξεις και εκφράσεις όπου είναι γνωστές στο χρήστη, δεν πρέπει χρησιμοποιεί εξειδικευμένες λέξεις που δεν είναι κατανοητές στους απλούς χρήστες. Επίσης, τα στοιχεία διεπαφής χρήστη πρέπει να έχουν την αναμενόμενη λειτουργία βάση την εμφάνιση τους. Το σύστημα ικανοποιεί πλήρως αυτό τον κανόνα.

Ο τρίτος κανόνας είναι ο έλεγχος και η ελευθερία του χρήστη. Ο χρήστης πρέπει να έχει την δυνατότητα να ακυρώσει ή αναιρέσει μία ανεπιθύμητη πράξει με εύκολο τρόπο, χωρίς να χρειάζεται τη βοήθεια του διαχειριστή ή της τεχνικής υποστήριξης του συστήματος. Το σύστημα ικανοποιεί πλήρως αυτό τον κανόνα.

Ο τέταρτος κανόνας είναι η συνοχή και συμμόρφωση έναντι προτύπων. Η εφαρμογή πρέπει να ακολουθεί τα πρότυπα που υπάρχουν από άλλες εφαρμογές. Επίσης, πρέπει να υπάρχει συνοχή μεταξύ των λειτουργιών της ίδιας εφαρμογής. Στο σύστημα υπάρχει πολύ καλή συνοχή μεταξύ των λειτουργιών της, αλλά υπάρχει μόνο καλή συμμόρφωση και συνοχή μεταξύ των προτύπων από άλλες εφαρμογές.

Ο πέμπτος κανόνας είναι η πρόσληψη σφαλμάτων. Το σύστημα πρέπει να αποτρέπει το χρήστη να φτάσει σε σφάλμα και να υπάρχουν προειδοποιήσεις για τις πράξεις που μπορούν να οδηγήσουν το χρήστη σε σφάλμα. Το σύστημα προειδοποιήσει, σε πλήρη βαθμό, το χρήστη για πράξεις που πιθανό να οδηγήσουν σε σφάλμα. Επίσης υπάρχουν μέθοδοι, σε πολύ καλό βαθμό, όπου απαγορεύουν το χρήστη να φτάσουν σε σφάλμα.

Ο έκτος κανόνας είναι η αναγνώριση και όχι ανάκληση. Το σύστημα δεν πρέπει να αναμένει από το χρήστη να θυμάται κάποια πληροφορία, αλλά η πληροφορία να είναι ορατή ή εύκολα προσβάσιμη και ο χρήστη θα πρέπει μόνο να την αναγνωρίσει. Επιπρόσθετα, το σύστημα πρέπει να παρέχει σύντομες οδηγίες σε κάθε οθόνη, παρόλο που υπάρχει μία οθόνη με πλήρης οδηγίες για την διαδικασία ψηφοφορίας. Το σύστημα ικανοποιεί αυτό τον κανόνα σε πολύ καλό βαθμό.

Ο έβδομος κανόνας είναι η προσαρμοστικότητα και αποδοτικότητα χρήσης. Η εφαρμογή πρέπει να έχει τρόπους προσαρμογής της εμφάνισης και περιεχομένου της. Επίσης πρέπει να είναι αποδοτική, δηλαδή η χρήση της να είναι γρήγορη και οι πράξεις να είναι απλές και με λίγα βήματα. Η εφαρμογή ικανοποιεί και τον κανόνα αποδοτικότητας σε πολύ καλό βαθμό τον κανόνα προσαρμοστικότητας σε καλό βαθμό.

Ο όγδοος κανόνας είναι ο καλαισθητικός σχεδιασμός. Το περιεχόμενο της πληροφορίας της εφαρμογής πρέπει να είναι απλό και να εξυπηρετεί το σκοπό του χρήστη. Επίσης, η εφαρμογή πρέπει να έχει απλό και καλό σχεδιασμό. Η εφαρμογή εμφανίζει όλες τις απαραίτητες πληροφορίες για ολοκλήρωση του στόχου του χρήστη και έχει πολύ καλό σχεδιασμό.

Ο ένατος κανόνας είναι βοήθεια, αναγνώριση, διάγνωση και ανάκαμψη από λάθη. Τα μηνύματα σφάλματος του συστήματος πρέπει να εκφράζονται σε απλή γλώσσα, να υποδεικνύουν με ακρίβεια το πρόβλημα και να προτείνουν εποικοδομητικά μια λύση. Το σύστημα ικανοποιεί αυτό το κανόνα σε πολύ καλό βαθμό.

Ο δέκατος κανόνας είναι βοήθεια και εγχειρίδια. Η εφαρμογή πρέπει να προσφέρει εγχειρίδιο με απλές και κατανοητές οδηγίες για να βοηθήσει τους χρήστες να ολοκληρώσουν το στόχο τους. Η εφαρμογή ικανοποιεί πλήρως αυτό το κανόνα.

Στη συνέχεια θα παρουσιαστεί ένας πίνακας που συνοψίζει τα αποτελέσματα του ερωτηματολογίου. Η βαθμολογία στο ερωτηματολόγια είναι καθόλου, λίγο, μέτριο, καλό και πλήρως. Το πολύ καλό είναι όταν ένας κανόνας έχει βαθμολογία μεταξύ καλό και πλήρως.

Κανόνας	Βαθμολογία
1. Ορατότητα της κατάστασης του συστήματος	Πολύ Καλό βαθμό
2. Συμφωνία του συστήματος με τον έξω κόσμο	Πλήρως
3. Έλεγχος και η ελευθερία του χρήστη	Πλήρως
4. Συνοχή και συμμόρφωση έναντι προτύπων	Καλό Βαθμό
5. Πρόσληψη σφαλμάτων	Πολύ Καλό Βαθμό
6. Αναγνώριση και όχι ανάκληση	Πολύ Καλό Βαθμό
7. Προσαρμοστικότητα και αποδοτικότητα χρήσης	Καλό Βαθμό
8. Καλαισθητικός σχεδιασμός	Πολύ Καλό Βαθμό
9. Βοήθεια, Αναγνώριση, Διάγνωση και Ανάκαμψη από λάθη	Πολύ Καλό Βαθμό
10. Βοήθεια και εγχειρίδια	Πλήρως

Πίνακα 5.1 Τα αποτελέσματα της αξιολόγησης ευχρηστίας που προέκυψαν από το ερωτηματολόγιο.

5.6 Τελική αξιολόγηση συστήματος αναφορικά με την ασφάλεια

Σε αυτό το υποκεφάλαιο θα γίνει αναφορά στην τελική αξιολόγηση, δηλαδή την αξιολόγηση του τελικού συστήματος ως προς τις απαιτήσεις ασφάλειας. Ο σκοπός της αξιολόγησης είναι να ελεγχθεί ολόκληρο το σύστημα, όχι από την μάτια ενός χρήστης, αλλά από τη ματιά ενός προγραμματιστή και γνώστη σε συστήματα ηλεκτρονικής ψηφοφορίας. Ο κύριος στόχος της αξιολόγησης είναι να εξεταστεί αν το σύστημα ικανοποιεί τις απαιτήσεις ασφάλειας των συστημάτων ηλεκτρονικής ψηφοφορίας. Οι απαιτήσεις ασφάλειας είναι η μυστικότητα του χρήστη και ψηφοδελτίου, ακεραιότητα του αποτελέσματος, αυθεντικοποιήση του χρήστη, επαλήθευση της ψήφου και διαθεσιμότητα του συστήματος. Επίσης, θα γίνει αναφορά στου κινδύνους που μπορούν να προκύψουν από τη εσφαλμένη δημιουργία κλειδιών κρυπτογράφησης και θα γίνει μια σύντομη αναφορά στις οντότητες. Στο τέλος του υποκεφάλαιου υπάρχει ένας πίνακας που συνοψίζει το αποτέλεσμα.

Αρχικά θα γίνει αναφορά στη δημιουργία των κλειδιών κρυπτογράφησης των ψηφοδελτίων. Τέσσερα έμπιστα άτομα σκέφτονται ένα μυστικό κωδικό, δηλαδή μία λέξη, οι κωδικοί ενώνονται σε μία τελική φράση (string concatenate), η φράση κατακερματίζεται με χρήση

sha512 και βάση τα πρώτα 32 byte της κατακερματισμένης φράσης θα δημιουργηθεί ο σπόρος (seed) του κλειδιού. Από το σπόρο του κλειδιού δημιουργείται το κλειδί κρυπτογράφησης και αποκρυπτογράφησης. Η είσοδος των κωδικών μπορεί να γίνει ένα-ένα, με οποιαδήποτε σειρά, ώστε να μην αποκαλύπτεται κάποιος κωδικός. Στην πρώτη φάση δημιουργείται και αποθηκεύεται μόνο το κλειδί κρυπτογράφησης και στο τέλος της εκλογικής διαδικασίας δημιουργείται το κλειδί αποκρυπτογράφησης. Απαιτούνται και οι 4 κωδικοί για να δημιουργηθεί το κλειδί αποκρυπτογράφησης, αν κάποιο άτομο γνωρίζει τους 3 από τους 4 κωδικούς, λόγω του κατακερματισμού και τρόπου δημιουργίας του σπόρου των κλειδιών, το κλειδί που θα δημιουργήσει θα είναι εντελώς άσχετο με το πραγματικό. Ο μόνος κίνδυνος που μπορεί να υπάρξει είναι αν ο μετρητής είναι διεφθαρμένος και έχει αλλάξει τη λειτουργία δημιουργίας κλειδιών, ώστε να αποθηκεύεται το κλειδί αποκρυπτογράφησης ενώ κανονικά δεν γίνεται. Αυτό όμως μπορεί να ελεγχθεί από τα έμπιστα άτομα ή κάποιο άλλο άτομο πριν τη διαδικασία εκλογών.

Εκτός από τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης των ψηφοδελτίων είναι σημαντικό να γίνει αναφορά στα κλειδιά κρυπτογράφησης της επικοινωνίας ψηφοφόρου και οντοτήτων (μετρητής, διαχειριστής, κοινό). Τα κλειδιά κρυπτογράφησης της επικοινωνίας ψηφοφόρου και οντοτήτων χρησιμοποιούνται για να κρυπτογραφήσουν τα μηνύματα μεταξύ ενός ψηφοφόρου και μίας οντότητας. Κάθε ψηφοφόρος και οντότητα έχουν ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Για το ψηφοφόρο τα κλειδιά του είναι αποθηκευμένα στο Android Keystore και για τις οντότητες είναι αποθηκευμένα, τοπικά, σε ένα αρχείο. Το ιδιωτικό κλειδί της κάθε οντότητας και του ψηφοφόρου είναι μυστικό και είναι γνωστό μόνο από τον ιδιοκτήτη του. Ο κάθε ψηφοφόρος γνωρίζει το δημόσιο κλειδί των οντοτήτων και οι οντότητες γνωρίζουν το δημόσιο κλειδί των ψηφοφόρων. Ο ψηφοφόρος δημιουργεί το κλειδί κρυπτογράφησης και αποκρυπτογράφησης των μηνυμάτων συνδυάζοντας το ιδιωτικό του κλειδί και το δημόσιο κλειδί της οντότητας που θέλει να επικοινωνήσει. Η οντότητα δημιουργεί το κλειδί κρυπτογράφησης και αποκρυπτογράφησης των μηνυμάτων συνδυάζοντας το ιδιωτικό της κλειδί και το δημόσιο κλειδί του ψηφοφόρου. Χρησιμοποιούνται τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων. Όσο η επικοινωνία παραμένει κρυπτογραφημένη υπάρχει πλήρης μυστικότητα από τρίτα άτομα.

Στη συνέχεια, θα γίνει αναφορά για τις τρεις οντότητες που αποθηκεύουν δεδομένα, το διαχειριστή(admin), τον μετρητή (counter) και το κοινό (public). Κάθε οντότητα αποτελείται από ένα php αρχείο και τη δική της βάση δεδομένων. Κάθε οντότητα μπορεί να τρέχει σε ξεχωριστό υπολογιστή και ξεχωριστή διεύθυνση (IP address). Επιπρόσθετα, ο κώδικας του

php αρχείου και της βάσης δεδομένων μπορεί εύκολα να ελεγχθεί, ώστε να επιβεβαιωθεί ότι λειτουργεί σωστά. Ακόμη, η κάθε οντότητα μπορεί να αποτελείται πάνω από ένα άτομο, ώστε να υπάρχει περισσότερος έλεγχος για την ορθή λειτουργία της. Μία τέταρτη βοηθητική οντότητα είναι η "main", όπου σκοπός της είναι η εύκολη και ασφαλής δημιουργία των κλειδιών κρυπτογράφησης και την αρχή της ψηφοφορίας. Η «main» συνεργάζεται μόνο με το κοινό και μετρητή για τις λειτουργίες της.

Ακολούθως, θα εξηγηθούν οι κίνδυνοι στη μυστικότητα του ψηφοφόρου, δηλαδή αν υπάρχει δυνατότητα να συνδεθεί ο ψηφοφόρος με το ψηφοδέλτιο του. Κανονικά, μόνο ο διαχειριστής γνωρίζει πληροφορίες για τον ψηφοφόρο και το αναγνωριστικό του ψηφοδελτίου, ενώ ο μετρητής γνωρίζει το αναγνωριστικό του ψηφοδελτίου και το κρυπτογραφημένο ψηφοδέλτιο. Η σχέση ψηφοφόρου – αναγνωριστικού ψηφοδελτίου είναι κατακερματισμένη, έτσι υπό κανονικές δεν είναι ορατή από τον διαχειριστή. Αν ο διαχειριστής και ο μετρητής είναι διεφθαρμένοι, τότε μπορούν να μεταβάλουν το πρόγραμμα με σκοπό να υπολογίζουν το κατακερματισμό όνομα του ψηφοφόρου, ώστε να το συνδέσουν με το όνομα του (ψηφοφόρου) και στο τέλος υπολογίσουν τη σύνδεση ονόματος – κατακερματισμένου ονόματος - αναγνωριστικού ψηφοδελτίου - κρυπτογραφημένου ψηφοδελτίου. Ακόμη ένας κίνδυνος προς τη μυστικότητα αφορά τον κώδικα επαλήθευσης του ψηφοδελτίου και το μετρητή. Ο κώδικας επαλήθευσης είναι η κατακερματισμένη κρυπτογραφημένη ψήφος, άρα αν ο μετρητής γνωρίζει που ανήκει ένας κωδικός επαλήθευσης, το οποίο δεν γίνεται σε κανονικές συνθήκες, έχει τη δυνατότητα να ανακαλύψει το κρυπτογραφημένο ψηφοδέλτιο όπου ανήκει. Αυτό μπορεί να συνδέσει ένα ψηφοφόρο με την κρυπτογραφημένη ψήφο του. Επιπρόσθετα, αν τα έμπιστα άτομα δεν είναι πραγματικά έμπιστα, μπορούν να δώσουν το μυστικό κωδικό τους στο μετρητή για να υπολογίσει το κλειδί αποκρυπτογράφησης, με αποτέλεσμα να συνδεθεί ο ψηφοφόρος με την ψήφο του. Η πιθανότητα δημιουργίας σχέσης ψηφοφόρου – κρυπτογραφημένη ψηφοδελτίου είναι πολύ μικρή αφού απαιτεί τουλάχιστον 2 άτομα, όπου ανήκουν στη διαδικασία εκλογών, και την αλλαγή του προγράμματος, ενώ η πιθανότητα δημιουργίας σχέσης ψηφοφόρου – ψηφοδελτίου είναι πολύ πιο μικρή αφού απαιτούνται τουλάχιστον 6 άτομα που ανήκουν στη διαδικασία εκλογών και την αλλαγή του προγράμματος.

Μια δεύτερη πλευρά της μυστικότητας είναι η μυστικότητα στην επικοινωνία του ψηφοφόρου με τις οντότητες. Η επικοινωνία μεταξύ του ψηφοφόρου και τις οντότητες είναι κρυπτογραφημένη, άρα δεν μπορεί κάποιος τρίτος να διαβάσει το περιεχόμενο των μηνυμάτων, εκτός αν γνωρίζει το κρυφό κλειδί. Όμως, δεν υπάρχει ανωνυμία στην επικοινωνία μεταξύ του ψηφοφόρου και τις οντότητες, έτσι ένα τρίτο άτομο μπορεί να

γνωρίζει ποια IP διεύθυνση ή και άτομο, αν γνωρίζει σε ποιο άτομο ανήκει η κάθε διεύθυνση, επικοινωνεί με τις οντότητες και με ποια οντότητα επικοινωνεί. Μόνο στη σύνδεση με την εφαρμογή και στη καταχώρηση της ψήφου ο ψηφοφόρος στέλνει το όνομα του στο διαχειριστή, όμως όσο είναι κρυπτογραφημένη η επικοινωνία, κάποιος τρίτος δεν μπορεί να γνωρίζει ποιο άτομο έστειλε το μήνυμα.

Σε αυτή τη παράγραφο θα αναλυθεί η αντίσταση που προσφέρει το σύστημα προς το εξαναγκασμό και στη πώληση ψήφου. Ο ψηφοφόρος έχει τη δυνατότητα να αντικαταστήσει τη ψήφο του σε όλη τη διάρκεια της φάσης ψηφοφορίας, ψηφίζοντας το άτομο που επιθυμεί και όχι τον υποψήφιο που τον υποχρέωσε κάποιο ύπουλο άτομο. Επίσης, λόγω της δυνατότητας αντικατάστασης της ψήφου, ο αγοραστής δεν γνωρίζει αν ο ψηφοφόρος θα αντικαταστήσει τη ψήφο του στο μέλλον, έτσι δεν υπάρχει λόγος να αγοράζει ψήφους. Επιπλέον, όσο υπάρχει η μυστικότητα στην εκλογική διαδικασία, τότε δεν υπάρχει κίνδυνος να συνδεθεί η ψήφος και ο ψηφοφόρος, άρα δεν μπορεί ένας τρίτος να γνωρίζει την ψήφο ενός ατόμου. Ακόμη, ο κωδικός επαλήθευσης δεν αποτελεί κίνδυνο στη αντίσταση προς το εξαναγκασμό και πώληση ψήφου. Όλοι οι κωδικοί επαλήθευσης συνεχίσουν να συμπεριφέρονται το ίδιο, ασχέτως αν σχετίζονται με ένα ψηφοδέλτιο που έχει αντικατασταθεί, αλλά δεν θα μετρηθούν στο τελικό αποτέλεσμα. Με αποτέλεσμα ο κωδικός επαλήθευσης να μην αποτελεί ένδειξη αν ένας ψηφοφόρος αντικατέστητε τη ψήφο του.

Οι επόμενοι κίνδυνοι όπου θα αναλυθούν είναι οι κίνδυνοι προς την ακεραιότητα του αποτελέσματος. Αν ο διαχειριστής είναι έμπιστος και δίνει τη υπογραφή του μόνο σε άτομα που έχουν το δικαίωμα να ψηφίσουν, τότε μόνο έγκυρα άτομα θα μπορούν να ψηφίσουν μέσα από την εφαρμογή. Αντιθέτως, αν είναι διεφθαρμένος και επιτρέπει σε μη έγκυρα άτομα να ψηφίσουν, για παράδειγμα να προσθέσει μη έγκυρα άτομα στη λίστα ψηφοφόρων, τότε θα υπάρχουν μη έγκυρα ψηφοδέλτια. Επιπρόσθετα, ένας διεφθαρμένος μετρητής μπορεί να δημιουργήσει ένα πρόγραμμα και να προσθέτει ψεύτικους ψήφους. Η προσθήκη ψεύτικων ψήφων μπορεί να ανακαλυφθεί μετρώντας των αριθμών των ψηφοφόρων που ψήφισαν, το μέγιστο έγκυρων ψηφοφόρων και ψηφοδέλτια που υπάρχουν στο σύστημα. Ο σοβαρότερος κίνδυνος είναι η αντικατάσταση ψήφων από διεφθαρμένο μετρητή ή διαχειριστή. Ο κώδικας επαλήθευσης θα δείξει ότι μία ψήφος λείπει μόνο αν διαγράφηκε πλήρως από το σύστημα, αλλιώς αν το ψηφοδέλτιο είναι στο πίνακα με τα αντικατεστημένα ψηφοδέλτια θα δείχνει ότι είναι παρόν. Μπορούν να μετρηθούν τα περιεχόμενα του πίνακα αυτού για να ελεγχθεί αν υπήρχε μεγάλος αριθμός αντικατεστημένων ψηφοδελτίων ή αν χρειάζεται, μπορεί να ελεγχθεί από το μετρητή, όχι όμως σε κανονικές συνθήκες, αν ένας κωδικός επαλήθευσης ανήκει σε αντικατεστημένη ψήφο. Επιπλέον, το κοινό (public), αν

είναι ύπουλο, μπορεί να αλλάξει προσωρινά τα αναγνωριστικά των πολιτικών ομάδων (partyID), σε άλλη ομάδα που θέλει, έτσι στο ψηφοδέλτιο να αναγράφεται η ομάδα που θέλει το κοινό, όχι η ομάδα που επίλεξε ο ψηφοφόρος. Για παράδειγμα όλα τα αναγνωριστικά των πολιτικών ομάδων να είναι «001», με αποτέλεσμα όλοι οι ψήφοι να αντιστοιχούν στην πολιτική ομάδα «001» και όχι σε αυτή που ψήφισε ο ψηφοφόρος. Όμως είναι δύσκολο να ξεγελαστεί ο ψηφοφόρος επειδή θα φαίνεται στη εφαρμογή ότι ψηφίζει λάθος αναγνωριστικό ομάδας και ότι υπάρχουν ομάδες με το ίδιο αναγνωριστικό. Άλλο ένας κίνδυνος είναι από τρίτα ύπουλα άτομα. Ένα τρίτο ύπουλο άτομο που έχει το κλειδί κρυπτογράφησης των ψηφοδελτίων, όλοι οι ψηφοφόροι μπορούν να το αποκτήσουν, και γνωρίζει τη μορφή του ψηφοδελτίου μπορεί να δημιουργήσει ψεύτικα ψηφοδέλτια. Όταν ο ψηφοφόρος επικοινωνεί με τον διαχειριστή ζητώντας την υπογραφή του, το ύπουλο άτομο έχει την ευκαιρία να αντικαταστήσει το αληθινό ψηφοδέλτιο με το ψεύτικο του. Με τελικό αποτέλεσμα να καταχωρηθεί το ψεύτικο ψηφοδέλτιο. Αυτός ο κίνδυνος έχει 2 τρόπους αντιμετώπισης, όλη η επικοινωνία του χρήστη μεταξύ οντοτήτων (διαχειριστής, μετρητής, κοινό) είναι κρυπτογραφημένη άρα είναι δύσκολο να αντικατασταθεί ο αληθινός ψήφος και ο κωδικός επαλήθευσης θα ενημερώσει τον χρήστη αν το ψηφοδέλτιο του δεν καταγράφηκε.

Ακολούθως, θα επεξηγηθούν οι κίνδυνοι που αφορούν την αυθεντικοποίηση του χρήστη. Η αυθεντικοποιήση γίνεται μόνο από τον διαχειριστή, δεν λαμβάνει μέρος άλλη οντότητα. Όπως αναφέρθηκε προηγουμένως, η αυθεντικοποιήση γίνεται μέσω ονόματος και κωδικού. Επίσης, αποθηκεύεται ο κατακερματισμένος κωδικός και όχι ο πραγματικός, με αποτέλεσμα ο διαχειριστής να μην γνωρίζει το πραγματικό κωδικό, έτσι δεν μπορεί να τον χρησιμοποιήσει για να συνδεθεί σαν κάποιο χρήστη. Ακόμη ένας κίνδυνος είναι ένα τρίτο άτομο να κλέψει το όνομα και κωδικό ενός χρήστη στη διάρκεια της φάσης αυθεντικοποιήσης. Αυτό είναι δύσκολο να επιτευχθεί, επειδή η επικοινωνία του χρήστη μεταξύ οντοτήτων (διαχειριστής, μετρητής, κοινό) είναι κρυπτογραφημένη, άρα όσο τα συμμετρικά κλειδιά παραμένουν μυστικά, τότε υπάρχει ασφάλεια. Επίσης, οι κωδικοί πρόσβασης είναι κατακερματισμένοι στη βάση δεδομένων του διαχειριστή, άρα ένα τρίτο άτομο δεν μπορεί να συνδεθεί παράνομα σε αυτή με σκοπό να κλέψει τους κωδικούς.

Στη συνέχεια θα αξιολογηθεί η επαληθευσιμότητα του συστήματος. Ο πρώτος τρόπος είναι με τον κωδικό επαλήθευσης. Ο κάθε ψηφοφόρος θα έχει ένα κωδικό επαλήθευσης όπου μπορεί να τον χρησιμοποιεί για να μάθει την κατάσταση του ψηφοδελτίου του, δηλαδή αν έχει καταγραφεί ή και έχει μετρηθεί. Για λόγους ασφάλειας ο ψηφοφόρος δεν γνωρίζει αν έχει αντικατασταθεί ή όχι η ψήφος του. Αν κάποιος αντικαταστήσει τη ψήφο του, ο ψηφοφόρος δεν θα το γνωρίζει, αφού το ψηφοδέλτιο θα βρίσκεται στο πίνακα με τους

παλιούς ψήφους, έτσι ο κωδικός θα επιστρέφει ότι έχει καταγραφεί. Ο δεύτερος τρόπος είναι με την λίστα που περιέχει πληροφορίας για την κατάσταση της εκλογικής διαδικασίας. Μόνο συγκεκριμένα έμπιστα άτομα θα έχουν πρόσβαση σε αυτή τη λίστα, όπως οι επικεφαλής της κάθε πολιτικής παράταξης. Η λίστα, όπως αναφέρθηκε πιο πάνω, περιέχει τις ακόλουθες πληροφορίες: το σύνολο εμφανίσεων του κάθε ονόματος (first name) των ψηφοφόρων, το σύνολο του κάθε domain του ηλεκτρονικού ταχυδρομείου ("@emaildomain.com") των ψηφοφόρων, το σύνολο των πιθανών ψηφοφόρων, το σύνολο των ατόμων που ψήφισαν, το σύνολο των ψηφοδελτίων, που θα μετρηθούν, και το σύνολο το ψηφοδελτίων που αντικαταστάθηκαν. Με βάση αυτών των πληροφοριών μπορεί να γίνει έλεγχος αν υπάρχει κάποια απροσδόκητη κατάσταση, για παράδειγμα περισσότερες ψήφους από άτομα που ψήφισαν. Όμως, αν τα ύπουλα άτομα είναι έξυπνα μπορούν να αλλάξουν το τελικό αποτέλεσμα, όπως αντικατάσταση μικρό ποσοστού ψήφων, χωρίς να γίνει αντιληπτό.

Στο τέλος θα αναλυθεί η διαθεσιμότητα του συστήματος. Ο κύριος παράγοντας που επηρεάζει την διαθεσιμότητα είναι οι εξυπηρετητές των τριών οντοτήτων. Όσο οι εξυπηρετητές ικανοποιούν όλα τα αιτήματα από τους χρήστες χωρίς καθυστερήσεις ή προβλήματα, τότε υπάρχει ψηλή διαθεσιμότητα. Έγινε ένας έλεγχος με 3 χρήστες όπου έστελνα ταυτόχρονες αιτήσεις στις οντότητες (εξυπηρετητές), για παράδειγμα ταυτόχρονη σύνδεση στη εφαρμογή και κάθε βήμα της διαδικασίας ψηφοφορίας έγινε ταυτόχρονα. Ακόμη, με τη χρήση του Apache JMeter, στάλθηκαν 2 φόρες 10 ταυτόχρονες αιτήσεις για σύνδεση στην εφαρμογή. Οι πιο πάνω δοκιμές έγιναν με επιτυχία, οι οντότητες ικανοποίησαν όλες τις αιτήσεις των χρηστών χωρίς κάποιο πρόβλημα. Επίσης, η εφαρμογή έχει μεθόδους ώστε να ανακάμψει από σφάλματα με την επικοινωνία μεταξύ χρήστη και εξυπηρετητή. Επιπλέον, η εφαρμογή δεν έχει προστασία από DDOS επιθέσεις ή άλλου είδους επιθέσεων όπου έχουν σκοπό να ενοχλήσουν την επικοινωνία χρήστη – οντοτήτων [28].

Στη συνέχεια θα παρουσιαστεί ένας πίνακας που συνοψίζει το βαθμό ικανοποιήσεις μίας απαίτησης ασφαλείας βάσει την τελική αξιολόγηση.

	Μυστικότητα	Ακεραιότητα	Επαληθευσιμότητα	Αυθεντικο-ποίηση	Διαθεσι-μότητα
Διαχειριστής	Πλήρως	Πλήρως	Πλήρως	Πλήρως	Πλήρως
Μετρητής	Πλήρως	Πλήρως	Πλήρως	Πλήρως	Πλήρως
Κοινό	Πλήρως	Πλήρως	Πλήρως	Πλήρως	Πλήρως
Διεφθαρμένος	Μέτρια	Καθόλου	Πλήρως	Πλήρως	Πλήρως

Διαχειριστής					
Διεφθαρμένος Μετρητής	Καθόλου	Καθόλου	Καθόλου	Πλήρως	Πλήρως
Διεφθαρμένο Κοινό	Πλήρως	Πλήρως	Πλήρως	Πλήρως	Πλήρως
Διαχειριστής & Μετρητής	Καθόλου	Καθόλου	Καθόλου	Πλήρως	Πλήρως
Διαχειριστής & Κοινό	Πλήρως	Πλήρως	Πλήρως	Πλήρως	Πλήρως
Μετρητής & Κοινό	Πλήρως	Πλήρως	Πλήρως	Πλήρως	Πλήρως
Τρίτα άτομα	Πλήρως	Πλήρως	Πλήρως	Πλήρως	Καθόλου

Πίνακας 5.2 Σύνοψη της τελικής αξιολόγησης βάσει τις απαιτήσεις ασφάλειας. Στο πίνακα εμφανίζεται κατά πόσο ικανοποιείται μία απαίτηση.

5.7 Σύγκριση με το διαδικτυακό σύστημα ψηφοφορίας της Εσθονίας.

Σε αυτό το υποκεφάλαιο θα γίνει μία σύγκριση του συστήματος που έχω υλοποιήσει με το σύστημα διαδικτυακής ψηφοφορίας της Εσθονίας. Η σύγκριση θα γίνει με αναφορά στα διάφορα μέρη του συστήματος της Εσθονίας και τις διαφορές που υπάρχουν με το σύστημα που έχω υλοποιήσει [32].

Αρχικά θα γίνει αναφορά στις οντότητες που υπάρχουν στο σύστημα της Εσθονίας, οι βασικές οντότητες είναι οι ακόλουθες. Ο Ψηφοφόρος, ο οποίος ψηφίζει μέσω ηλεκτρονικού υπολογιστή. Ο Συλλέκτης όπου δίνει τη λίστα με τους υποψήφιους στο ψηφοφόρο, αποθηκεύει τις ψήφους και είναι υπεύθυνος για την επαλήθευση της ψήφου. Ο Επεξεργαστής, όπου ελέγχει τις ψηφιακές υπογραφές, την εγκυρότητα των ψήφων και διαγράφει τις μη έγκυρες ψήφους. Επίσης, ο Επεξεργαστής ταξινομεί τις ψήφους βάσει εκλογικής περιφέρειας και αναμιγνύει τις ψήφους για να ενισχυθεί η ανωνυμία τους. Ο Διοργανωτής έχει το ιδιωτικό κλειδί, ανοίγει τις ανώνυμες και αναμιγμένες ψήφους και υπολογίζει το τελικό αποτέλεσμα. Στο σύστημα που έχω υλοποιήσει, υπάρχει ο Ψηφοφόρος, αλλά χρησιμοποιεί το κινητό του για να ψηφίσει. Επιπλέον, ο Επεξεργαστής έχει παρόμοια λειτουργία με το Διαχειριστή, δηλαδή την αυθεντικοποίηση του Ψηφοφόρου και την εγκυρότητα της ψήφου, αλλά δεν υπάρχει ανάμιξη των ψηφοδελτίων στο σύστημα που έχω υλοποιήσει. Ακόμη, ο Συλλέκτης και ο Διοργανωτής έχουν παρόμοιες λειτουργίες με το

Μετρητή, δηλαδή την αποθήκευση, επαλήθευση και καταμέτρηση των ψήφων, με κύρια διαφορά ότι η λίστα με τους υποψήφιους υπάρχει στο Κοινό, όχι στο Μετρητή.

Επιπρόσθετα, το σύστημα της Εσθονίας προσφέρει αρκετές υπηρεσίες όπου το σύστημα όπου έχω υλοποιήσει δεν τις προσφέρει. Για παράδειγμα, υπάρχει οντότητα όπου ελέγχει την ακεραιότητα των δεδομένων της εκλογικής διαδικασίας. Επίσης, υπάρχει τεχνική υποστήριξη, όπου βοηθάει το ψηφοφόρο με προβλήματα κατά την διάρκεια της εκλογικής διαδικασίας.

Στην συνέχεια θα γίνει αναφορά στην μέθοδο δημιουργίας των κλειδιών κρυπτογραφίας των ψηφοδελτίων στο σύστημα της Εσθονίας. Αυτή η μέθοδος είναι πολύ παρόμοια με την μέθοδο δημιουργίας των κλειδιών κρυπτογραφίας που χρησιμοποιεί το σύστημα που έχω υλοποιήσει. Υπάρχει ένα δημόσιο κλειδί, όπου είναι το κλειδί κρυπτογράφησης και ένα ιδιωτικό κλειδί όπου είναι το κλειδί αποκρυπτογράφησης. Το κλειδί αποκρυπτογράφησης δημιουργείται από μία ομάδα από έμπιστα άτομα με τη χρήστη ενός κωδικού ή κάρτας chip και διαγράφεται όταν το τελικό αποτέλεσμα έχει ανακοινωθεί.

Ακολούθως, θα γίνει αναφορά στις μεθόδους ταυτοποίησης του ψηφοφόρου στο σύστημα της Εσθονίας. Ο ψηφοφόρος μπορεί να χρησιμοποιήσει, όπως στο σύστημα που έχω υλοποιήσει, ένα ψευδώνυμο και κωδικό για να ταυτοποίηση το εαυτό του και τη ψηφιακή του υπογραφή για να εξασφαλίσει την ακεραιότητα και αυθεντικότητα της ψήφος του. Το σύστημα της Εσθονίας προσφέρει ακόμη ένα πιο ασφαλές τρόπο ταυτοποίησης, τη χρήση μίας φυσικής ένδειξης (token), όπως μία κάρτα sim, και ένα κωδικό.

Στις επόμενες παραγράφους θα αναλυθεί η εκλογική διαδικασία του συστήματος της Εσθονίας. Η πρώτη φάση είναι η διαδικασία ταυτοποίησης. Αρχικά, ο ψηφοφόρος επιλέγει μία μέθοδος ταυτοποίησης και γίνεται ταυτοποίηση του ψηφοφόρου. Αν έχει το δικαίωμα να ψηφίζει, τότε εμφανίζονται οι υποψήφιοι τις εκλογικής του περιφέρειας. Η κύρια διαφορά του συστήματος της Εσθονίας με το σύστημα που έχω υλοποιήσει είναι ότι στο σύστημα που έχω υλοποιήσει η διαδικασία ταυτοποίησης γίνεται στην είσοδο της εφαρμογής και μετά την επιλογή των υποψηφίων.

Η δεύτερη φάση του συστήματος της Εσθονίας είναι η διαδικασία ψηφοφορίας. Ο ψηφοφόρος επιλέγει τους υποψήφιους που επιθυμεί και ένα τυχαίο αριθμό, το οποίο είναι το ψηφοδέλτιο του. Στη συνέχεια κρυπτογραφεί και υπογράφει το ψηφοδέλτιο του. Ο Συλλέκτης λαμβάνει το κρυπτογραφημένο και υπογραμμένο ψηφοδέλτιο, το πιστοποιητικό

του ψηφοφόρου και το χρόνο που καταχωρήθηκε η ψήφος. Ο χρόνος που καταχωρήθηκε η ψήφος χρησιμοποιείται ώστε μόνο το νεότερο ψηφοδέλτιο να καταμετρηθεί. Στο τέλος, αν ο ψηφοφόρος είναι στη λίστα το έγκυρων ψηφοφόρων, τότε στο ψηφοδέλτιο προθέτεται ένα ενδεικτικό εγκυρότητας και ο ψηφοφόρος λαμβάνει ένα QR κωδικό για την επαλήθευση της ψήφου του. Οι κύριες διαφορές του συστήματος της Εσθονίας με το σύστημα που έχω υλοποιήσει είναι ότι στο σύστημα που έχω υλοποιήσει τα ψηφοδέλτια αποθηκεύονται στο χωρίς τη ψηφιακή υπογραφή του ψηφοφόρου, δεν υπάρχει ο χρόνος καταχώρησης του ψηφοδελτίου αφού το προηγούμενο ψηφοδέλτιο θα μεταφερθεί στο πίνακα με τα παλιά ψηφοδέλτια και ο κωδικός επαλήθευσης αποτελείται από αριθμούς και γράμματα.

Η τρίτη φάση του συστήματος της Εσθονίας είναι η διαδικασία επαλήθευσης. Η διαδικασία επαλήθευσης δεν γίνεται από τον υπολογιστή του ψηφοφόρου, αλλά από μία κινητή συσκευή, η οποία έχει εγκατεστημένο το πρόγραμμα επαλήθευσης. Ο ψηφοφόρος σαρώνει το QR κωδικό με την κινητή του συσκευή. Η συσκευή, μαζί με το δημόσιο κλειδί του ψηφοφόρου και το τυχαίο αριθμό, επιστρέφει το όνομα του ψηφοφόρου που έχει ψηφίσει. Οι κύριες διαφορές του συστήματος της Εσθονίας με το σύστημα που έχω υλοποιήσει είναι ότι στο σύστημα που έχω υλοποιήσει όλες οι φάσεις μπορούν να γίνουν στη κινητή συσκευή του ψηφοφόρου και ότι η μέθοδος επαλήθευσης δεν επιστρέφει τους υποψήφιου που επίλεξε ο ψηφοφόρος, αλλά επιστρέφει αν καταχωρήθηκε ή καταμετρήθηκε η ψήφος.

Η τέταρτη φάση είναι του συστήματος της Εσθονίας είναι η διαδικασία καταμέτρησης. Αρχικά γίνεται έλεγχος της εγκυρότητα των ψηφοδελτίων μέσω της ψηφιακής τους υπογραφής. Μετά αφαιρούνται οι πολλαπλές ψήφοι ενός ψηφοφόρου αφήνοντας μόνο την πιο πρόσφατη και αν ένας ψηφοφόρος έχει ψηφίσει με χάρτινο ψηφοδέλτιο τότε αφαιρούνται οι διαδικτυακοί ψήφου του. Στη συνέχεια αφαιρούνται οι ψηφιακές υπογραφές από τα ψηφοδέλτια ή άλλες προσωπικές πληροφορίες και ενεργοποιείται το κλειδί αποκρυπτογράφησης από μία ομάδα από έμπιστα άτομα. Στο τέλος υπολογίζεται το τελικό αποτέλεσμα, δημιουργούνται απόδειξης ορθότητας του τελικού αποτελέσματος και απενεργοποιείται το κλειδί αποκρυπτογράφησης. Οι κύριες διαφορές του συστήματος της Εσθονίας με το σύστημα που έχω υλοποιήσει είναι ότι στο σύστημα που έχω υλοποιήσει δεν προσφέρεται απόδειξη ορθότητας του τελικού αποτελέσματος και δεν δίνει την δυνατότητα για ταυτόχρονη παραδοσιακή και διαδικτυακή ψηφοφορία.

Κεφάλαιο 6

Συμπεράσματα

6.1 Συμπεράσματα

Η ηλεκτρονική ψηφοφορία είναι ένα ενδιαφέρον θέμα. Τα πλεονεκτήματα που προσφέρει, ιδιαίτερα η διαδικτυακή ψηφοφορία, είναι απαραίτητα σε ένα μοντέρνο δημοκρατικό κόσμο. Η αύξηση της προσέλευσης των ψηφοφόρων λόγω της ευκολίας ψηφοφορίας, η ακεραιότητα του τελικού αποτελέσματος που επικυρώνεται από τις μεθόδους επαλήθευσης και το χαμηλότερο κόστος είναι πολύ σημαντικά στη διαδικασία εκλογών. Όμως υπάρχουν αρκετά εμπόδια που πρέπει να αντιμετωπιστούν πριν η ηλεκτρονική ψηφοφορία να αντικαταστήσει τους παραδοσιακούς τρόπους ψηφοφορίας. Ένα από τα πιο σημαντικά εμπόδια είναι η αντίληψη του κοινού, δηλαδή η δημιουργία εμπιστοσύνης, προς την διαδικασία ηλεκτρονικής ψηφοφορίας. Χωρίς την θετική αντίληψη προς τα συστήματα ψηφοφορίας, τότε δεν θα μπορούν ποτέ να αντικαταστήσουν τα παραδοσιακά συστήματα.

Η διπλωματική αυτή εργασία μου έχει δώσει την ευκαιρία να ασχοληθώ με τις διάφορες φάσεις δημιουργίας ενός συστήματος ηλεκτρονικής ψηφοφορίας για android κινητά. Η αρχική μελέτη για τα συστήματα ηλεκτρονικής ψηφοφορίας με βοήθησε να καταλάβω ότι είναι ένα περίπλοκο θέμα. Επίσης, με την μελέτη των διάφορων πρωτοκόλλων και των υφιστάμενων συστημάτων έγινε κατανοητό πως μπορεί να εφαρμοστεί ένα σύστημα στην πράξη και τις διάφορες μεθόδους που χρησιμοποιούνται για την ικανοποίηση των απαιτήσεων του. Επιπλέον, η μελέτη των διάφορων πρωτοκόλλων και συστημάτων με βοήθησε να δημιουργήσω το δικό μου πρωτόκολλο, το οποίο βασίζεται στο πρωτόκολλο του Fujioka, Okamoto και Ohta και το πρωτόκολλο του Juels, Catalano και Jakobsson. Αυτό το πρωτόκολλο είναι η βάση του συστήματος ηλεκτρονικής ψηφοφορίας που έχω δημιουργήσει. Λόγω ότι είναι πρώτη φορά που αναπτύσσω μία android εφαρμογή, και ένα ολόκληρο

σύστημα, με ψηλές απαιτήσεις ασφάλειας, έκανα αρκετά λάθη αλλά στη πάροδο του χρόνου απόκτησα αρκετή γνώση για την ανάπτυξη μελλοντικών συστημάτων. Οι 3 αξιολογήσεις όπου έγιναν κατά τη δημιουργία του συστήματος εντόπισαν αρκετά λάθη και η λύση τους βελτίωσε σημαντικά το σύστημα. Αυτό επίσης με βοήθησε να κατανοήσω πόσο εύκολο ήταν να γίνουν τα λάθη και πόσο απαραίτητο είναι η διαδικασία της ανίχνευσης και διόρθωσης λαθών.

Ίσως η πιο σημαντική γνώση που έχω αντιληφθεί μέσω αυτής της διπλωματικής εργασίας είναι το γεγονός ότι οι απαιτήσεις ασφάλειας ενός συστήματος ηλεκτρονική ψηφοφορίας είναι δύσκολο να επιτευχθούν. Αυτές οι απαιτήσεις πρέπει να βρίσκονται πάντα στην σκέψη του δημιουργού, αλλιώς εύκολα μπορούν να παραβιαστούν. Επίσης, οι απαιτήσεις ασφάλειας μπορεί να έρχονται σε αντίθεση μεταξύ τους και η εύρεση του σωστού τρόπου υλοποίησης τους να μην είναι εύκολο. Στη δική μου υλοποίηση θεώρησα ότι οι οντότητες (μετρητής, διαχειριστής και κοινό) είναι έμπιστες, έτσι δεν υπάρχει μεγάλη προστασία σε κακόβουλες ενέργειες από αυτές, αλλά υπάρχει περισσότερη ασφάλεια από τρίτα ύπουλα άτομα. Επιπλέον, υπήρχε προτεραιότητα στη μυστικότητα του ψηφοφόρου, αντίσταση στο εξαναγκασμό και ακεραιότητα του αποτελέσματος, με αποτέλεσμα να πληγεί η δυνατότητα επαλήθευσης. Για παράδειγμα, η ψήφος ενός ψηφοφόρος μπορεί να αντικατασταθεί από το διεφθαρμένο μετρητή, αλλά ο κωδικός επαλήθευσης δεν θα το αναγνωρίσει. Αυτό έγινε με σκοπό να προστατέψει το ψηφοφόρο από τον εξαναγκασμό στην εκλογική διαδικασία.

Είναι γνωστό ότι η υλοποίηση ενός συστήματος ηλεκτρονικής ψηφοφορίας είναι δύσκολο κατόρθωμα. Αρκετές χώρες προσπάθησαν αλλά απέτυχαν, όμως αρκετές χώρες συνεχίσουν να προσπαθούν. Επίσης, συνειδητοποίησα τη δυσκολία του προβλήματος μέσα από την ανάπτυξη του δικού μου συστήματος. Πιστεύω όμως ότι τα προβλήματα που υπάρχουν μπορούν να αντιμετωπιστούν. Υπάρχουν διάφοροι μέθοδοι κρυπτογράφησης, όπως τυφλές υπογραφές ή ομομορφική κρυπτογράφηση, όπου μπορούν να ικανοποιήσουν τις απαιτήσεις των συστημάτων ηλεκτρονικής ψηφοφορίας. Το πιο δύσκολο εμπόδιο είναι η αντίληψη της κοινωνίας προς τη τεχνολογία και τα συστήματα ηλεκτρονικής τεχνολογίας.

6.2 Εισηγήσεις για μελλοντικές επεκτάσεις

Το σύστημα που έχω υλοποιήσει ικανοποιεί της απαιτήσεις από τους μελλοντικούς χρήστες και τις απαιτήσεις ασφαλείας. Είναι ένα ολοκληρωμένο σύστημα που μπορεί να χρησιμοποιηθεί σε φοιτητικές εκλογές. Παρόλα αυτά υπάρχουν τομείς του συστήματος που μπορούν να βελτιωθούν με σκοπό να αυξηθεί η ασφάλεια που προσφέρει.

Μία απαίτηση του συστήματος που θα μπορούσε να βελτιωθεί περισσότερο είναι η επαλήθευση. Ένα παράδειγμα είναι να δίνεται η δυνατότητα επαλήθευσης του τελικού αποτελέσματος από τρίτους. Τα μη κρυπτογραφημένα ψηφοδέλτια και κάποιες οδηγίες χρήσης θα μπορούσαν να δίνονται σε έμπιστα τρίτα άτομα ώστε να υπολογίσουν το τελικό αποτέλεσμα. Αυτός ο τρόπος επαλήθευσης υπάρχει στο σύστημα Helios με χρήση ομομορφικής κρυπτογράφησης. Αυτό θα αυξήσει την εμπιστοσύνη του κοινό προς το τελικό αποτέλεσμα. Ένα δεύτερο παράδειγμα είναι ο κωδικός επαλήθευσης να ενημερώνει το χρήστη αν αντικαταστάθηκε η ψήφος του ή και αν μετρήθηκε στο τελικό αποτέλεσμα, χωρίς όμως να υπάρχει κίνδυνος στη μυστικότητα του χρήστη, στην αντίσταση για εξαναγκασμό στην ψηφοφορία ή πώληση ψήφου.

Ακόμη μία απαίτηση όπου μπορεί να βελτιωθεί είναι η μυστικότητα του συστήματος ώστε να είναι πιο δύσκολο να δημιουργηθεί η σχέση μεταξύ ψηφοφόρου και ψηφοδελτίου. Για παράδειγμα το αναγνωριστικό κάθε ψηφοδελτίου να είναι εντελώς τυχαίο, π.χ. ένα καθολικό μοναδικό αναγνωριστικό (UUID), ώστε να μην είναι εμφανής η σειρά ψηφοφορίας. Επίσης η σχέση του ονόματος χρήστη και το αναγνωριστικό ψηφοδελτίου που του αντιστοιχεί να είναι δυσκολότερο να ανακαλυφθεί, ίσως με την κρυπτογράφηση της από ένα κλειδί του χρήστη που βασίζεται στο κωδικό του.

Μία ακόμη πιθανή μελλοντική επέκταση του συστήματος είναι η αυθεντικοποίηση του χρήστη να γίνεται μέσω βιομετρικών στοιχείων. Ο χρήστης εκτός από το όνομα και κωδικό του θα μπορούσε να δίνει το δακτυλικό του αποτύπωμα ή να γίνεται αναγνώριση της ίριδας του ματιού. Με αυτό το τρόπο μόνο ο ίδιος ο ψηφοφόρος θα μπορεί να συνδεθεί στο λογαριασμό του στην εφαρμογή. Η χρήση βιομετρικών στοιχείων απαιτεί μια βάση δεδομένων με την αποθήκευση αυτών το στοιχείων, το οποίο θα πρέπει να υλοποιηθεί πολύ προσεκτικά ώστε να μην κλαπούν. Μία πρόκληση για τη χρήση βιομετρικών δεδομένων είναι ότι αποτελούν προσωπικά δεδομένων και προστατεύονται από νόμους επεξεργασίας και αποθήκευσης προσωπικών δεδομένων (GDPR) [5]. Μία δεύτερη πρόκληση είναι η απαίτηση από το χρήστη να κατέχει σύγχρονο κινητό. Ο χρήστης πρέπει να έχει κινητό που υποστηρίζει τη σάρωση δακτυλικού αποτυπώματος ή και την αναγνώριση ίριδας, το οποίο μπορεί να είναι αδύνατο για κάποιους ψηφοφόρους, έτσι θα αποκλείονταν από την εκλογική διαδικασία.

Επίσης, μία εισήγηση επέκτασης για βελτίωση της διαθεσιμότητας είναι χρήση πολλαπλών εξυπηρετητών για κάθε οντότητα. Θα υπάρχει ένας κεντρικός εξυπηρετητής όπου θα

μοιράζει τις αιτήσεις, δηλαδή την εισερχόμενη επικοινωνία από το χρήστη, στους εξυπηρετητές και κάθε εξυπηρετητής να διαθέτει πολλαπλά νήματα. Με χρήση παραλληλισμού δεν θα υπάρχουν καθυστερήσεις στην επικοινωνία μεταξύ του ψηφοφόρου και των οντοτήτων. Επιπρόσθετα, θα μπορούσε να υπάρχει κάποιο είδος ασφάλειας από DDOS επιθέσεις, όπου έχουν σκοπό να διακόψουν την επικοινωνία μεταξύ χρήστη και οντοτήτων [28].

Επιπλέον, μία πιθανή επέκταση είναι η προστασία από ύπουλα άτομα. Θα μπορούσε να υπάρχει ένας εξυπηρετητής όπου δειγματοληπτικά, θα ελέγχει την επικοινωνία προς και από των οντοτήτων. Ο έλεγχος αυτός θα έχει σκοπό να ανιχνεύσει άτυπες συμπεριφορές, όπου πιθανό να είναι μία προσπάθεια απάτης. Θα μπορούσε να ανακαλύψει ποιο άτομο ή οντότητα κάνει την απάτη, να την σταματήσει ή να ενημερώσει τα κατάλληλα άτομα. Αυτός ο έλεγχος θα συνεισφέρει σημαντικά στην επικύρωση της ακεραιότητας του τελικού αποτελέσματος, αλλά η υλοποίηση του πρέπει να έχει βασικό σκοπό την διατήρηση της μυστικότητας του ψηφοφόρου.

Επιπρόσθετα, μία μελλοντική επέκταση είναι μια ιστοσελίδα ή άλλο είδος διεπαφής χρήστη για την κάθε οντότητα. Στο παρόν σύστημα οι οντότητες δεν έχουν κάποια διεπαφή για να επικοινωνούν με την βάση δεδομένων τους, εκτός μέσω από την οντότητα “main” όπου προσφέρει μόνο βασικές λειτουργίες. Αν χρειάζεται να γίνει κάποια αλλαγή στη βάση δεδομένων ή έλεγχος κάποιας πληροφορίας γίνεται απευθείας από την βάση δεδομένων. Η απευθείας πρόσβαση στη βάση δεδομένων είναι επικίνδυνη, επειδή είναι εύκολο μια κακόβουλη οντότητα να παραβιάσει την ασφάλεια του συστήματος. Η διεπαφή χρήστη θα επιτρέπει στην οντότητα να έχει περιορισμένη πρόσβαση στην βάση δεδομένων, ώστε να μην τίθεται σε κίνδυνο η ασφάλεια του συστήματος.

Βιβλιογραφία

[1] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology (ASIACRYPT '92). Springer-Verlag, Berlin, Heidelberg, 244–251, 1992.

[2] "Estonian Internet Voting." CEF Digital, 29 July 2019, 14:03, ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/07/29/Estonian+Internet+voting

[3] FCh, Swiss Federal Chancellery. "E-Voting." Bundeskanzlei - Startseite, www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html.

[4] FCh, Swiss Federal Chancellery. e-Voting: Dialogue with Experts on Redesigning the Trial Phase, www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-79556.html.

[5] "GDPR Update - Biometric Data." Dentons - GDPR Update, Dentons, 22 Dec. 2020, www.dentons.com/en/insights/alerts/2020/december/22/gdpr-update-biometric-data.

[6] Gharadaghy, Rojan, and Melanie Volkamer. "Verifiability in Electronic Voting Explanations for Non Security Experts." Center for Advanced Security Research.

[7] "How It Works - Voatz How Voatz Works for Voters and Administrators." Voatz, 9 Sept. 2020, voatz.com/how-it-works/.

[8] "i-Voting - e-Estonia." i-Voting, 24 July 2019, e-estonia.com/solutions/e-governance/i-voting/.

[9] i-Voting – the Future of Elections? - e-Estonia." i-Voting – the Future of Elections?, 25 Sept. 2019, e-estonia.com/i-voting-the-future-of-elections/.

[10] Kreitzberg, Charles B. The LUCID Framework, Cognetics Corporation, 1 Jan. 2008, static1.squarespace.com/static/5492005de4b07708508198e8/t/54d86349e4b0964b00da4952/1423467337513/Lucid-Paper-v2.pdf.

[11] Lin, Gloria, and Nicole Espinoza. Electronic Voting - Arguments in Favor, 2007, cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index_files/page0001.html.

[12] Lin, Gloria, and Nicole Espinoza. Electronic Voting - Arguments Against, 2007, cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index_files/page0002.html.

[13] Nielsen, Jakob. "10 Usability Heuristics for User Interface Design." Nielsen Norman Group, 15 Nov. 2020, www.nngroup.com/articles/ten-usability-heuristics/.

[14] Pan, Haijun. "A Novel e-Voting System with Diverse Security Features." New Jersey Institute of Technology, 2017, https://digitalcommons.njit.edu/cgi/viewcontent.cgi?article=1007&context=dissertations.

[15] Panda, Samanvaya. "ElGamal Encryption Algorithm." GeeksforGeeks, 16 Nov. 2018, www.geeksforgeeks.org/elgamal-encryption-algorithm/.

[16] Pauli, Sebastian. "MAT 112 Ancient and Contemporary Mathematics." ElGamal Encryption System, mathstats.uncg.edu/sites/pauli/112/HTML/secelgamal.html.

[17] Pereira, Olivier. "Internet Voting with Helios ∗." (2016).

[18] Reorienting EVoting and Ensuring Stable Trial Operation, www.egovernment.ch/en/umsetzung/schwerpunktplan/vote-electronique/.

[19] Rønne, Peter B., Atashpendar, A., Gjøsteen, K. and Ryan, P. "Coercion-Resistant Voting in Linear Time via Fully Homomorphic Encryption." Springer, 2019.

[20] Riera, Andreu. Scytl, 2002, Comments on the Report "e-Voting Security Study" Written by the Communications-Electronics Security Group, www.scytl.com/wp-content/uploads/2013/05/Comments_on_the_report_e-Voting_Security_Study_UK.pdf.

[21] Seberry, Jennifer, and Yuliang Zheng. Advances in Cryptology-AUSCRYPT '92: Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992, Proceedings. Vol. 718, Springer-Verlag, 1993.

[22] Shimkiv, Y. M. “Blind Signature and Its Applications.” CryptoWiki, 24 Dec. 2015, cryptowiki.net/index.php?title=Blind_signature_and_its_applications.

[23] Specter, Michael A., et al. “The Ballot Is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections.” Internet Policy Research Initiative - MIT, internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf.

[24] Stone, Casey. “What Is Homomorphic Encryption?” What Is Homomorphic Encryption? - Hashed Out by The SSL Store™, 20 June 2019, www.thesslstore.com/blog/what-is-homomorphic-encryption/.

[25] Trechsel, Alexander, et al. “POTENTIAL AND CHALLENGES OF E-VOTING IN THE EUROPEAN UNION.” European Parliament, European Parliament's Committee on Constitutional Affairs, May 2016, www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf.

[26] Valdellon, Lionel. Heuristic Evaluation for Improving App UX, CleverTap, 6 June 2019, clevertap.com/blog/heuristic-evaluation/.

[27] “Voatz Mobile Voting Platform An Overview: Security, Identity, Auditability.” Voatz, Voatz, Inc., 2020, new.voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf.

[28] “What Is a DDoS Attack?” What Is a Distributed Denial-of-Service (DDoS) Attack ? | Cloudfare, Cloudfare, www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[29] “What Is GDPR, the EU's New Data Protection Law?” Edited by Ben Wolford, GDPR.eu, 13 Feb. 2019, gdpr.eu/what-is-gdpr/.

[30] Wolf, Peter, and Rushdi Nackerdien. Introducing Electronic Voting: Essential Considerations. International IDEA, 2011.

[31] AWS Serverless Multi-Tier Architectures with Amazon API Gateway and AWS Lambda. Amazon Web Services, Sept. 2019, docs.aws.amazon.com/whitepapers/latest/serverless-multi-tier-architectures-api-gateway-lambda/three-tier-architecture-overview.html.

[32] General Framework of Electronic Voting and Implementation Thereof at National Elections in Estonia. State Electoral Service of Estonia, June 2017, www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf.

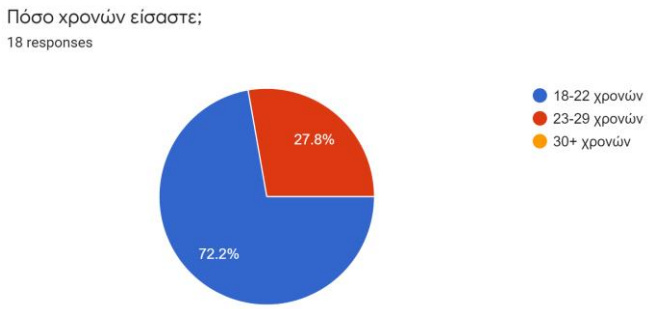
[33] IBM Cloud Education. “Three-Tier Architecture.” What Is Three-Tier Architecture | IBM, 28 Oct. 2020, https://www.ibm.com/cloud/learn/three-tier-architecture.

Παράρτημα Α

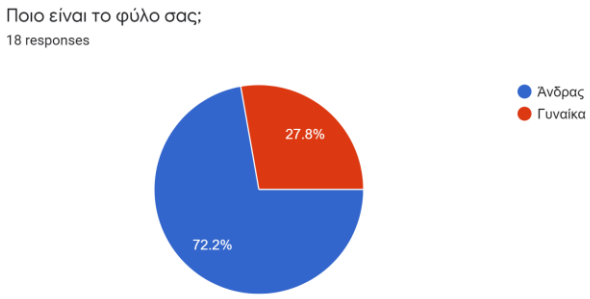
Ερωτηματολόγιο για το προσδιορισμό των απαιτήσεων της εφαρμογής.

Στη συνέχεια θα παρουσιαστούν τα αποτελέσματα του ερωτηματολογίου που χρησιμοποιήθηκε για το προσδιορισμό των απαιτήσεων. Δημιουργήθηκαν δύο ερωτηματολόγια. Το ένα δόθηκε σε πιθανούς χρήστες που ανήκουν στο Τμήμα της Πληροφορικής και το δεύτερο σε άτομα που ανήκουν στο φοιτητικό συμβούλιο.

Αρχικά θα παρουσιαστεί το ερωτηματολόγιο για του πιθανούς χρήστες. Ο σύνδεσμος είναι: https://forms.gle/uCYYQFq6upFN7DVQ6



Σχήμα Α.1 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 1



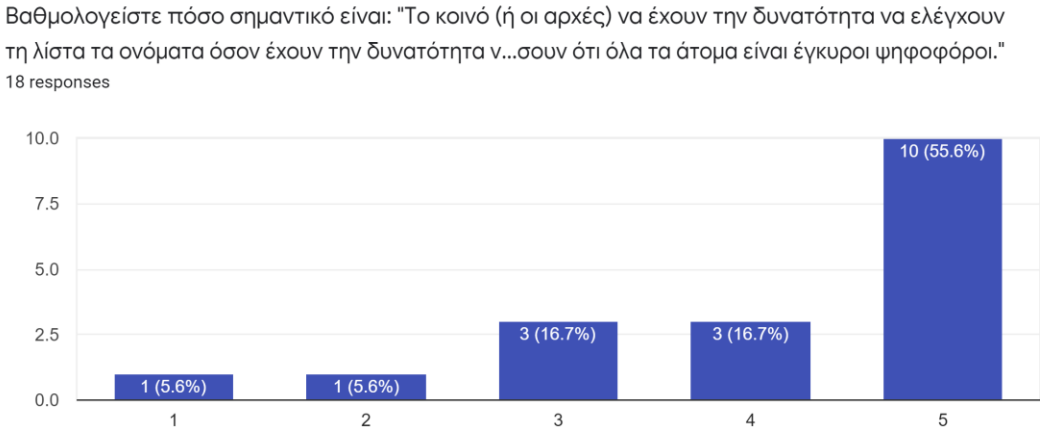
Σχήμα Α.2 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 2

Σχήμα Α.3 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 3

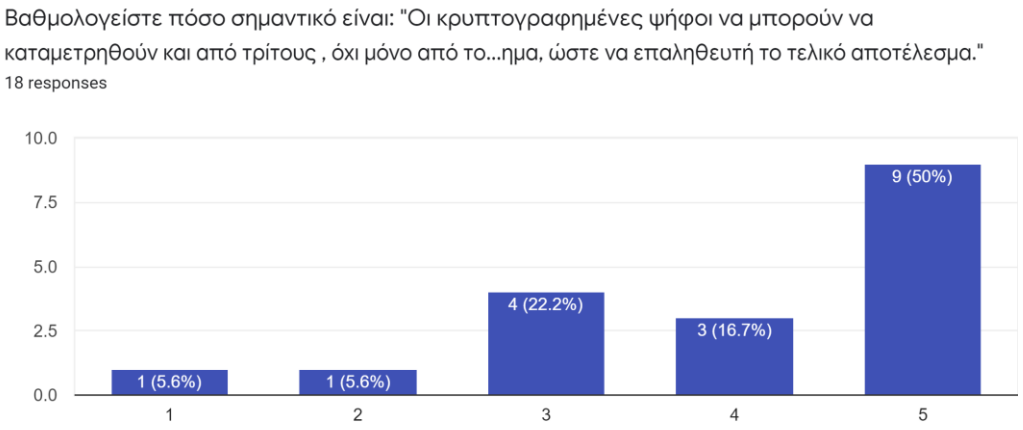
Σχήμα Α.4 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 4

Σχήμα Α.5 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 5

Σχήμα Α.6 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 6

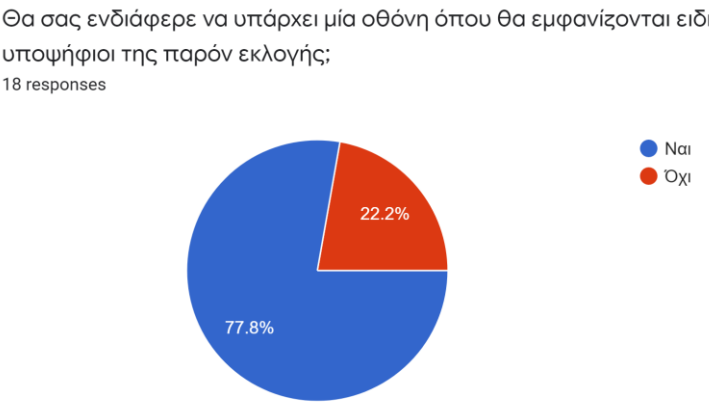


Σχήμα Α.7 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 7

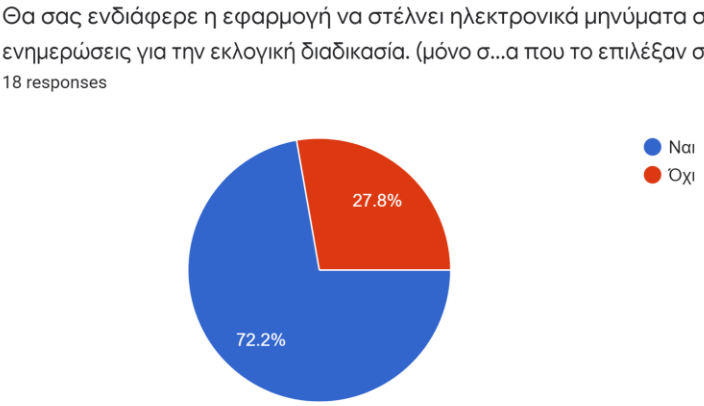


Σχήμα Α.8 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 8

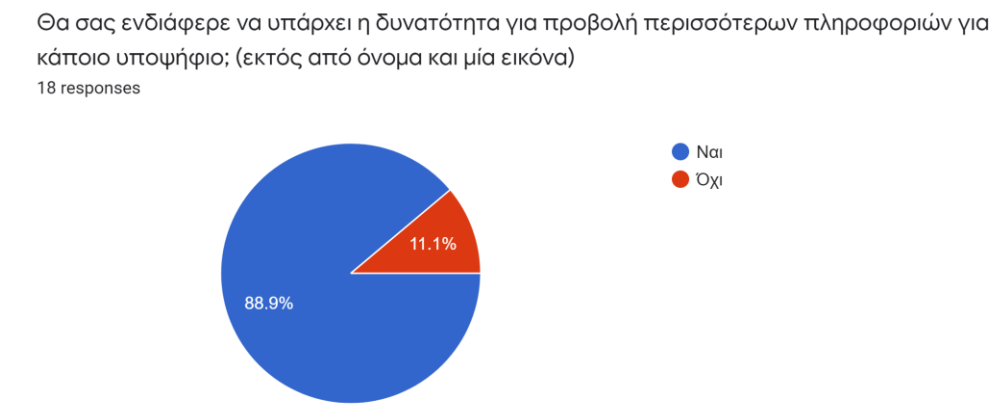
Σχήμα Α.9 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 9



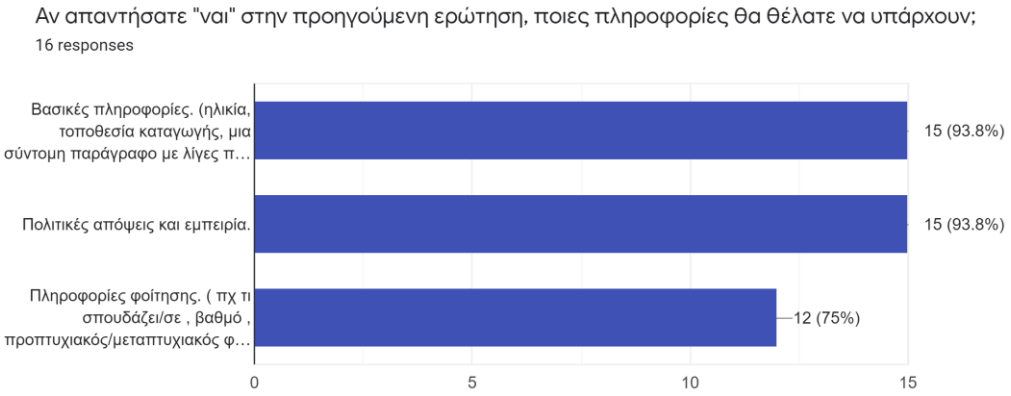
Σχήμα Α.10 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 10



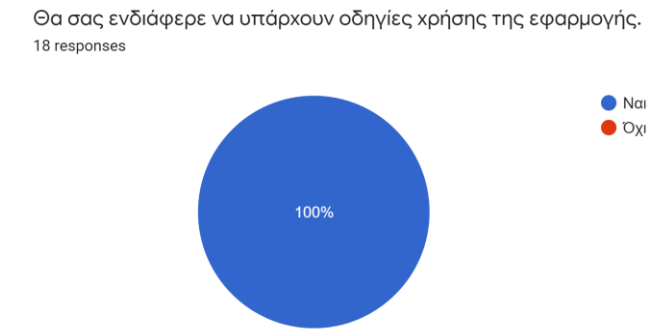
Σχήμα Α.11 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 11



Σχήμα Α.12 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 12



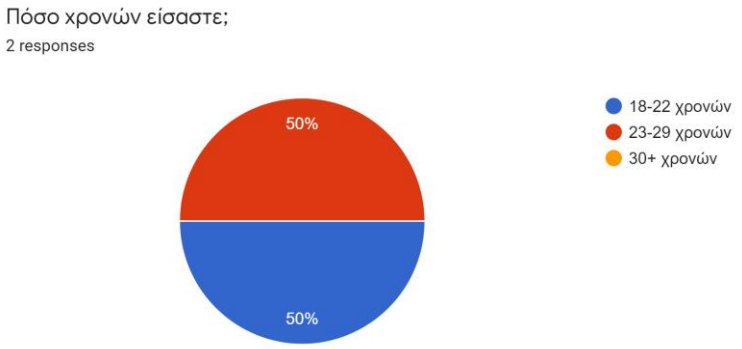
Σχήμα Α.13 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 13



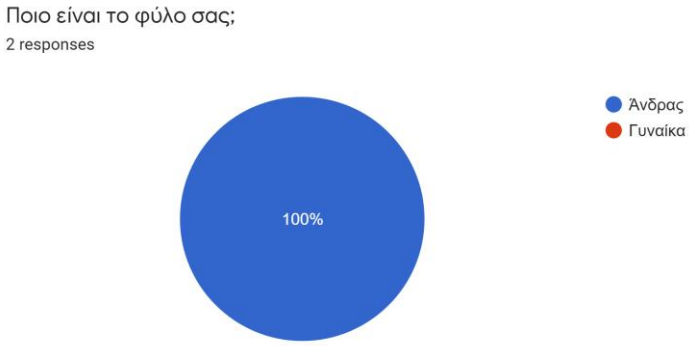
Σχήμα Α.14 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 14

Σχήμα Α.15 Ερωτηματολόγιο για πιθανούς χρήστες - Ερώτηση 15

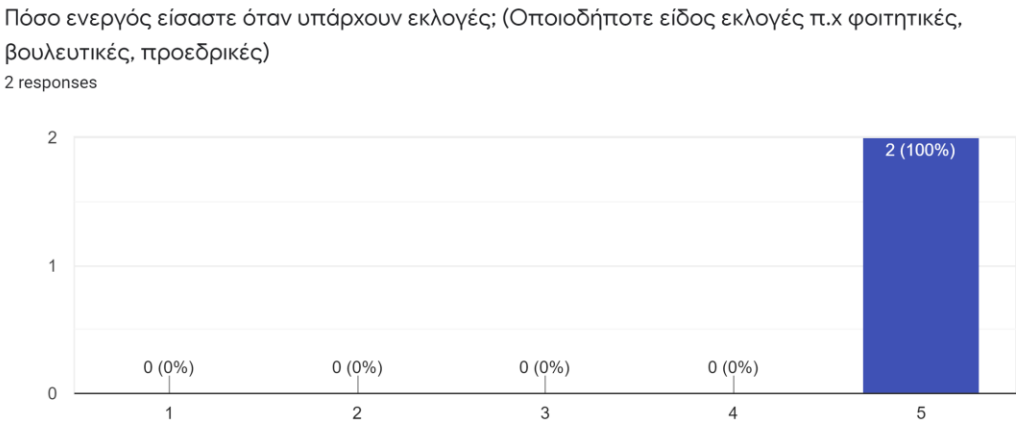
Στην συνέχεια θα παρουσιαστεί το ερωτηματολόγιο που δόθηκε στα μέλη του φοιτητικού συμβουλίου. Μόνο 2 άτομα το απάντησαν αλλά λόγω ότι είχαν κοινές απόψεις μπορούμε να εξάγουμε κάποια συμπεράσματα. Ο σύνδεσμος είναι: https://forms.gle/r6HCirkw7LYffWMSA



Σχήμα Α.16 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 1

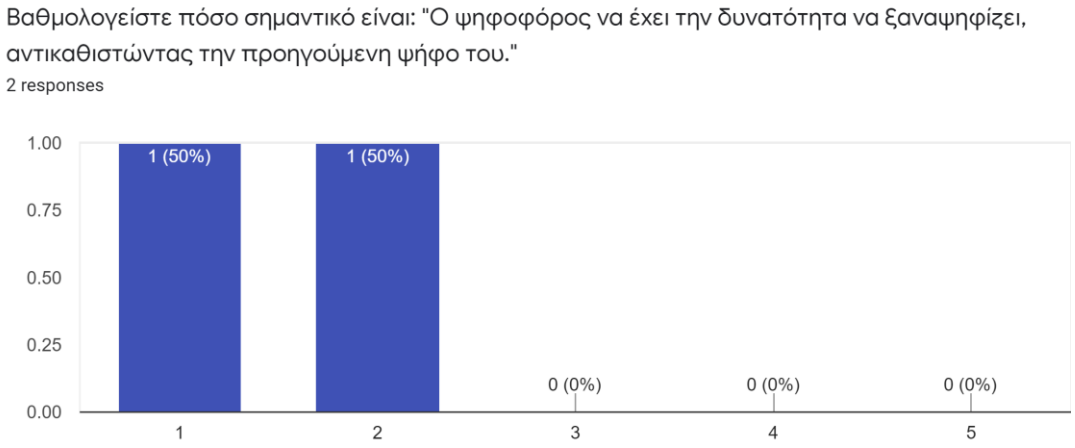


Σχήμα Α.17 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 2

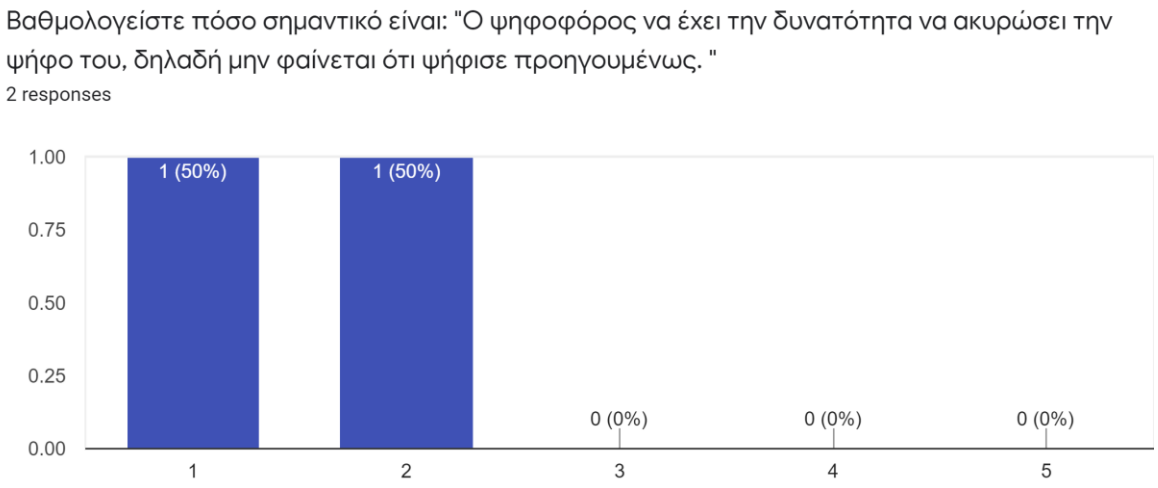


Σχήμα Α.18 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 3

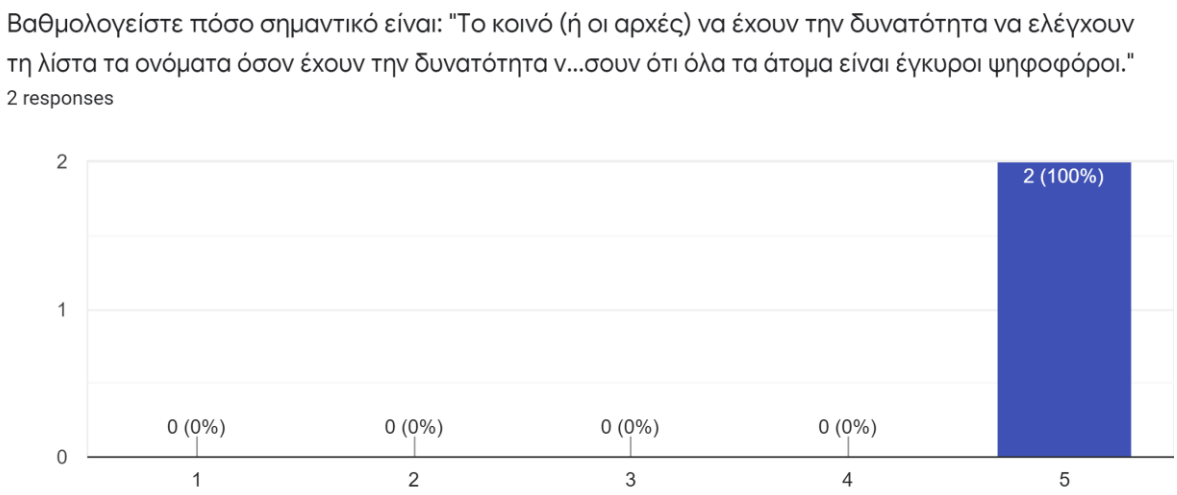
Σχήμα Α.19 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 4



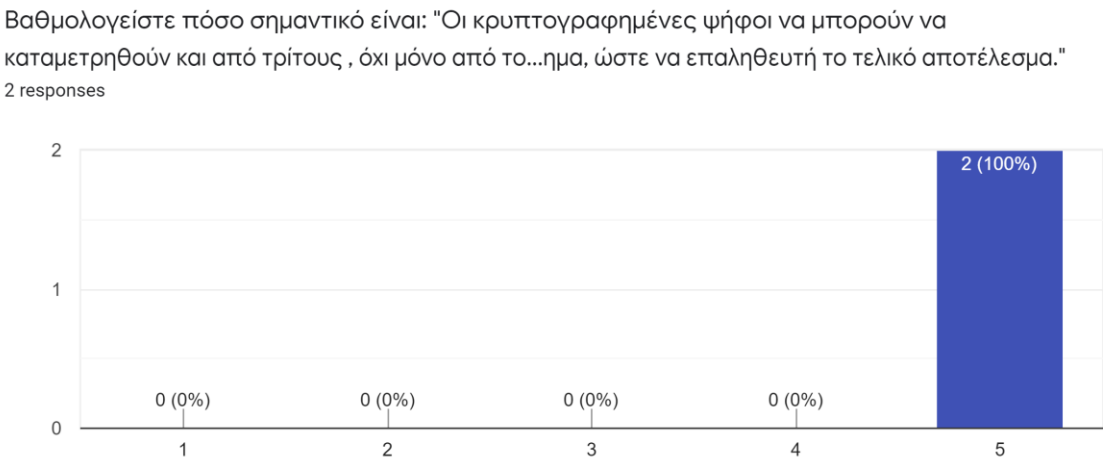
Σχήμα Α.20 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 5



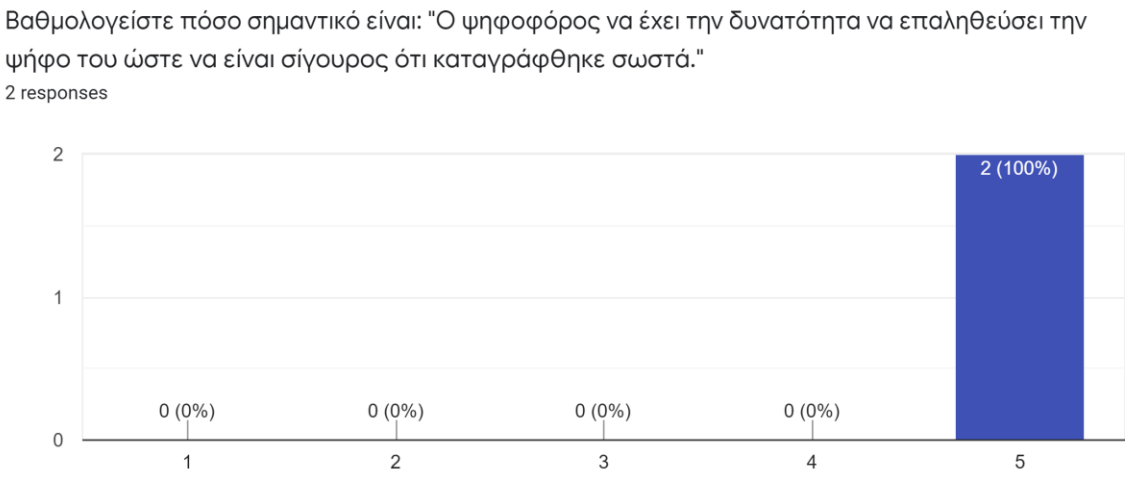
Σχήμα Α.21 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 6



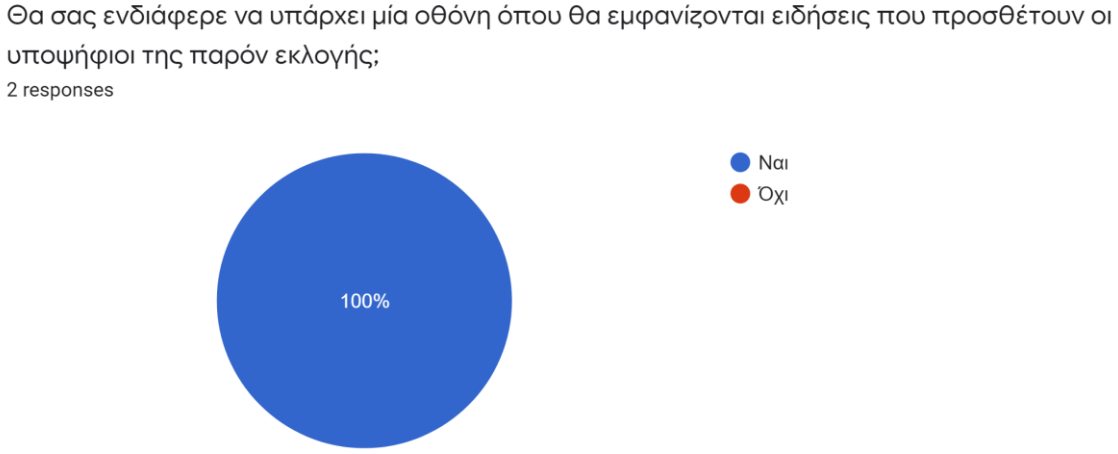
Σχήμα Α.22 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 7



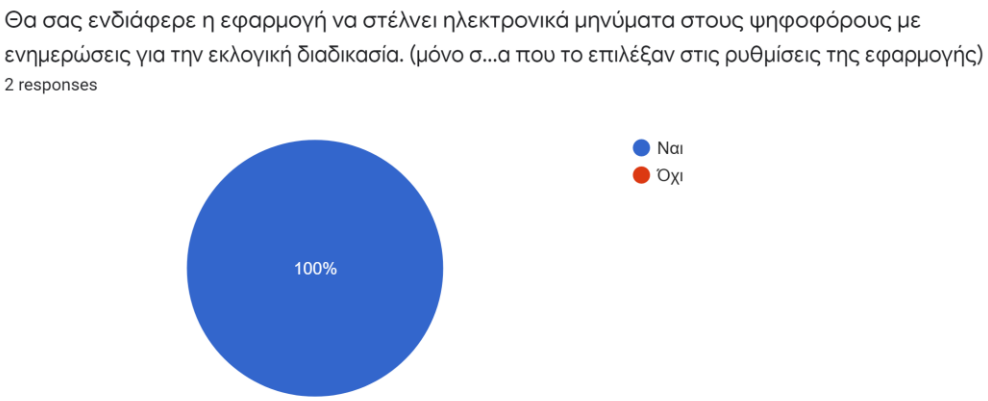
Σχήμα Α.23 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 8



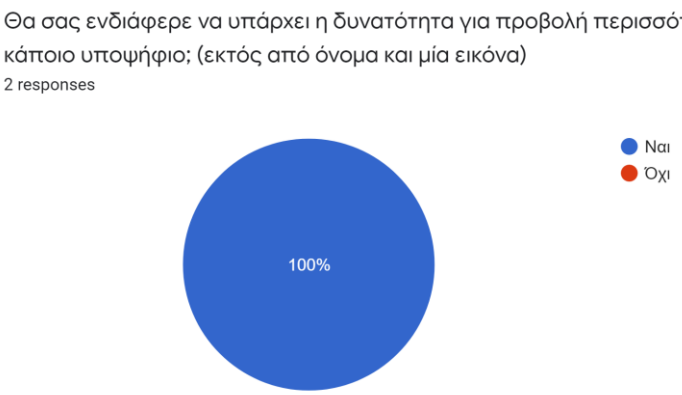
Σχήμα Α.24 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 9



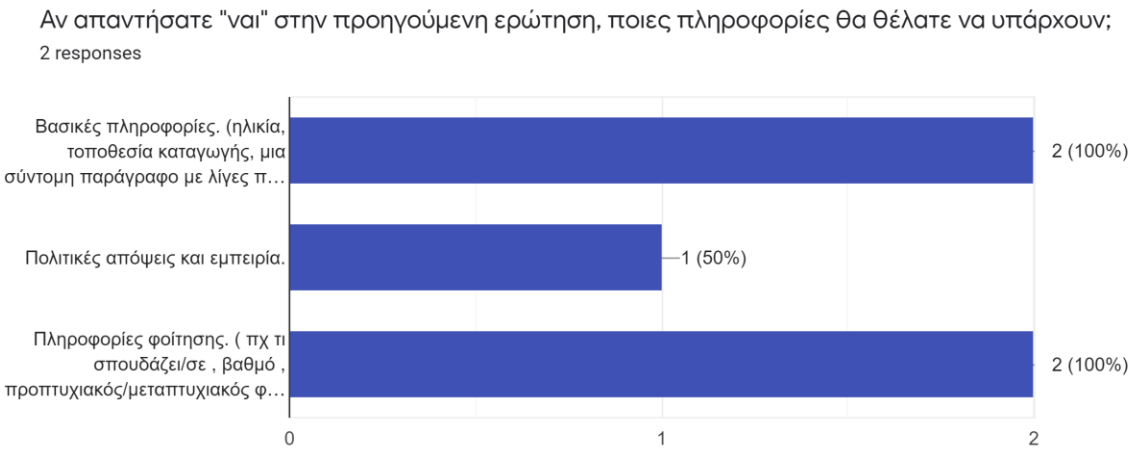
Σχήμα Α.25 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 10



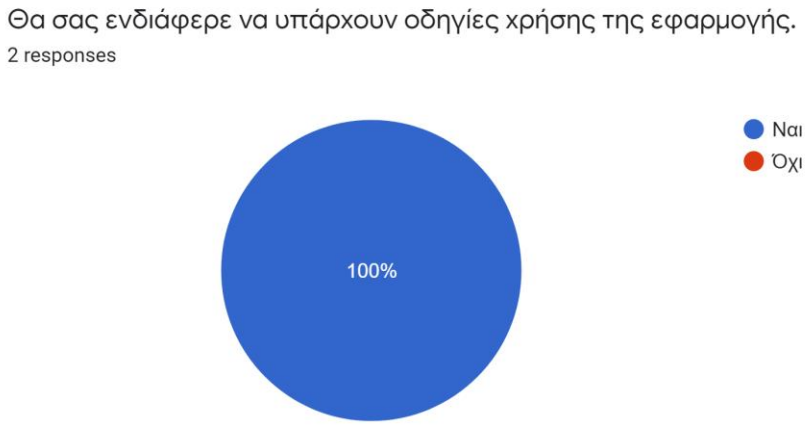
Σχήμα Α.26 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 11



Σχήμα Α.27 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 12



Σχήμα Α.28 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 13



Σχήμα Α.29 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 14

Σχήμα Α.30 Ερωτηματολόγιο για μέλη φοιτητικού συμβουλίου - Ερώτηση 15

Παράρτημα Β

Συνέντευξη για προσδιορισμό απαιτήσεων της εκλογικής διαδικασίας.

Η συνέντευξη έγινε με το πρόεδρο του φοιτητικού συμβουλίου του Πανεπιστημίου Κύπρου. Ο σκοπός της ήταν να μάθω πληροφορίες για την εκλογική διαδικασία στο Πανεπιστήμιο Κύπρου. Η εφαρμογή υλοποιήθηκε ώστε να υπακούει σε αυτούς τους κανόνες. Η συνέντευξη έγινε τηλεφωνικά. Οι απαντήσεις που θα παρουσιαστούν είναι παράφραση των απαντήσεων που έλαβα, αλλά διατηρούν την ίδια σημασία.

Ερώτησης 1: Τι ψηφίζει ουσιαστικά κάθε άτομο;
Απάντηση 1: Κάθε άτομο ψηφίζει την παράταξη που επιθυμεί. Ο ψήφος στην παράταξης «μετρά περισσότερο» από την ψήφο σε κάποιο μέλος.

Ερώτηση 2: Σε τι χρησιμεύει η ψήφος σε κάποιο υποψήφιο;
Απάντηση 2: Όταν μοιραστούν οι θέσεις στις παρατάξεις ανάλογα με τις ψήφους, τότε (σε κανονικές συνθήκες), οι πιο δημοφιλής υποψήφιοι της κάθε παράταξής, παίρνουν τις διαθέσιμες θέσεις της παράταξης που ανήκουν.

Ερώτηση 3: Πόσες παρατάξεις ψηφίζει ένα άτομο;
Απάντηση 3: Κάθε άτομο 0-1 παράταξη ή ένα ανεξάρτητο ψηφοφόρο..

Ερώτηση 4: Πόσα άτομα ψηφίζει κάθε άτομο;
Απάντηση 4: Από 0 – 7 άτομα της ίδιας παράταξης. Κάθε ανεξάρτητος ψηφοφόρος θεωρείται δική του παράταξη, όχι άτομο, άρα το μέγιστο 1 ανεξάρτητο υποψήφιο.

Ερώτηση 5: Ποια άτομα μπορούν να δηλώσουν υποψηφιότητα;
Απάντηση 5: Όλοι οι φοιτητές, ασχέτου αν είναι μέλος σε παράταξη ή όχι .

Ερώτηση 6: Πόσα μέλη εκλέγονται στο συμβούλιο;
Απάντηση 6: 21 μέλη.

Ερώτηση 7: Υπάρχει μέγιστος αριθμός υποψηφίων;
Απάντηση 7: Δεν υπάρχει.

Ερώτηση 8: Πως υπολογίζεται το αποτέλεσμα;

Απάντηση 8:

Ν- σύνολο ψήφων.

Ψ(Χ)- ψήφοι της Χ παράταξης.

έδρες(Χ) = (Ψ(Χ)/Ν) *21 (στρογγυλεύω προς τα κάτω, το υπόλοιπο φυλάγεται και χρησιμοποιείται πιο κάτω).

Έδρες (Χ) – Είναι οι έδρες στο συμβούλιο που απόκτησε η Χ παράταξη.

Η παράταξη με το μεγαλύτερο υπόλοιπο παίρνει την έδρα που έμεινε.

Ερώτηση 9: Ποια είναι η διαδικασία κατανομής των εδρών;

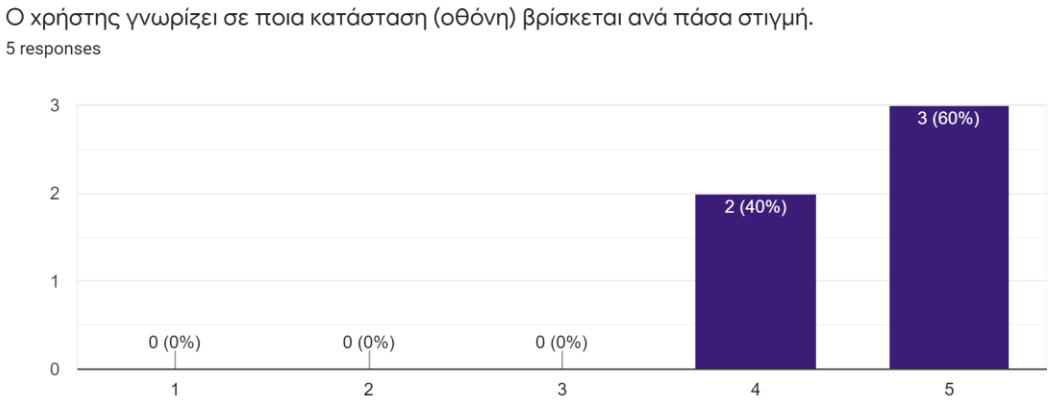
Απάντηση 9: Αρχικά, σύμφωνα με το πιο πάνω, κατανέμονται οι έδρες σε κάθε παράταξη. Στην συνέχεια η κάθε παράταξη μετρά πόσους ψήφους πήρε ο κάθε υποψήφιος της. Βάση των ψήφων, συνήθως τα άτομα με τους περισσότερους ψήφους, οι παρατάξεις αποφασίζουν σε ποια άτομα της παράταξης τους θα κατανέμουν τις έδρες της παράταξής τους.

Παράρτημα Γ

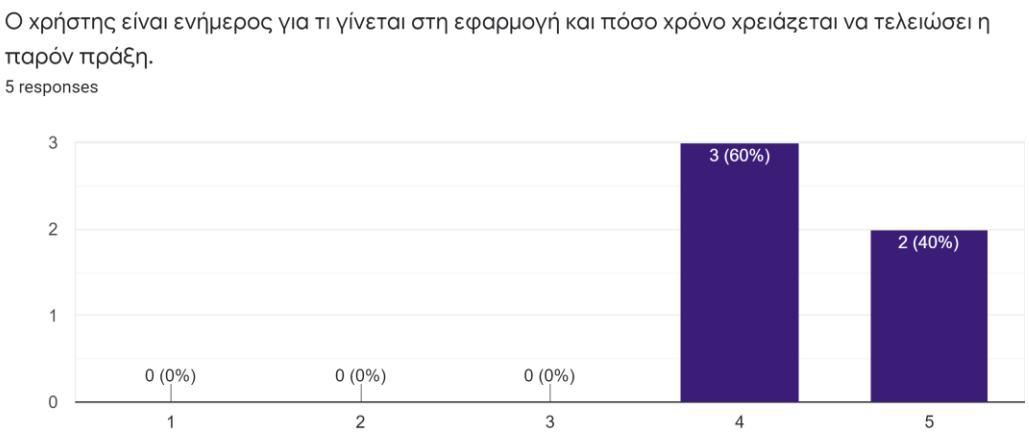
Ερωτηματολόγιο για αξιολόγησης της εφαρμογής βάσηει κανόνων ευχρηστίας.

Στη συνέχεια θα παρουσιαστεί το ερωτηματολόγιο ευχρηστίας. Το ερωτηματολόγιο δόθηκε σε μία ομάδα πιθανών χρηστών μαζί με την τελική εφαρμογή. Μετά τον έλεγχο της εφαρμογής, οι χρήστες απάντησαν το ερωτηματολόγιο. Ο σύνδεσμος του ερωτηματολογίου είναι: https://forms.gle/UgKEa5X8W4s5bqBD7. Πιο κάτω είναι οι απαντήσεις του ερωτηματολογίου.

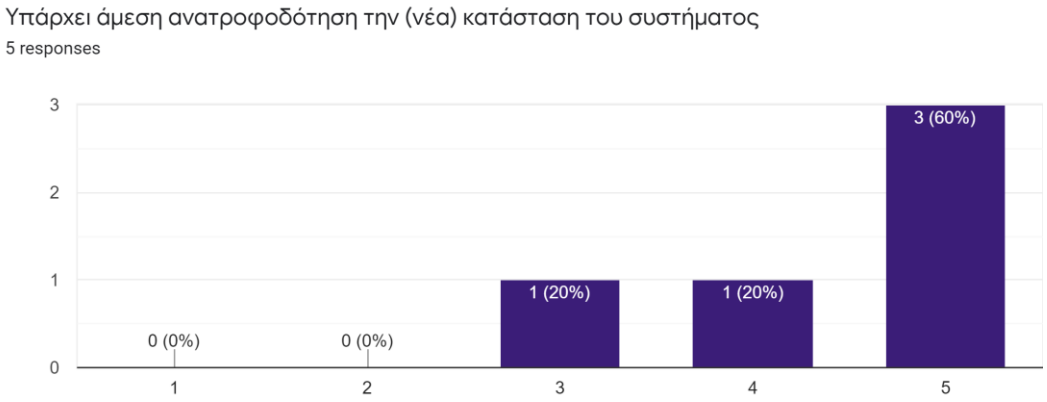
Η βαθμολογία έχει γίνει βάση της πιο κάτω κλίμακας:
1 -Καθόλου
2 -Λίγο
3 -Μέτριο
4 -Καλό
5 -Πλήρως



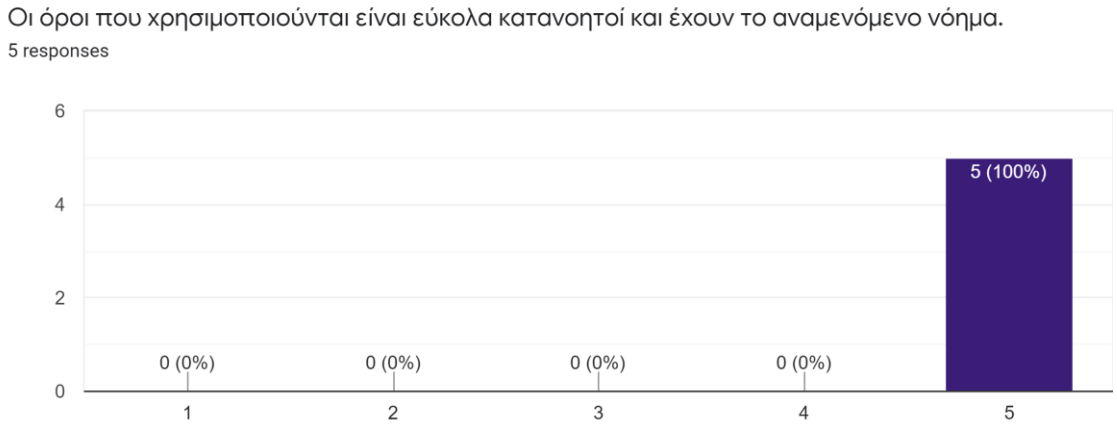
Σχήμα Γ.1 1. Ορατότητα της κατάστασης του συστήματος - Ερώτηση 1



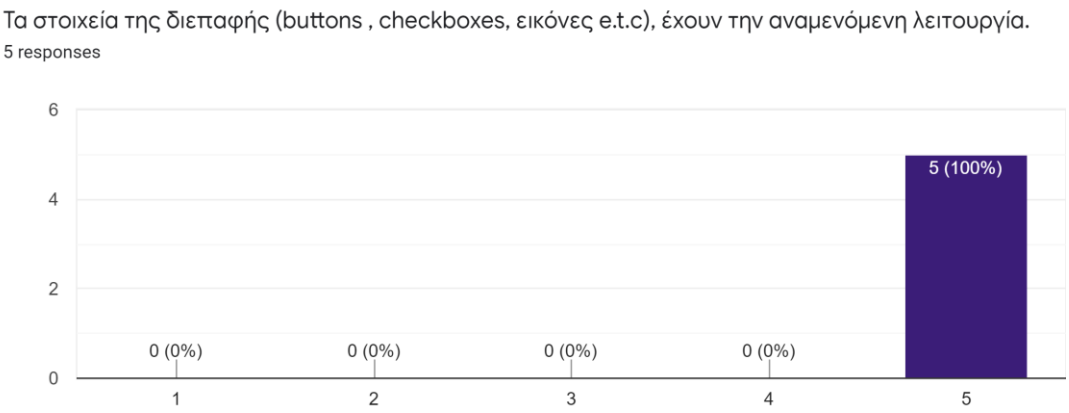
Σχήμα Γ.2 1. Ορατότητα της κατάστασης του συστήματος - Ερώτηση 2



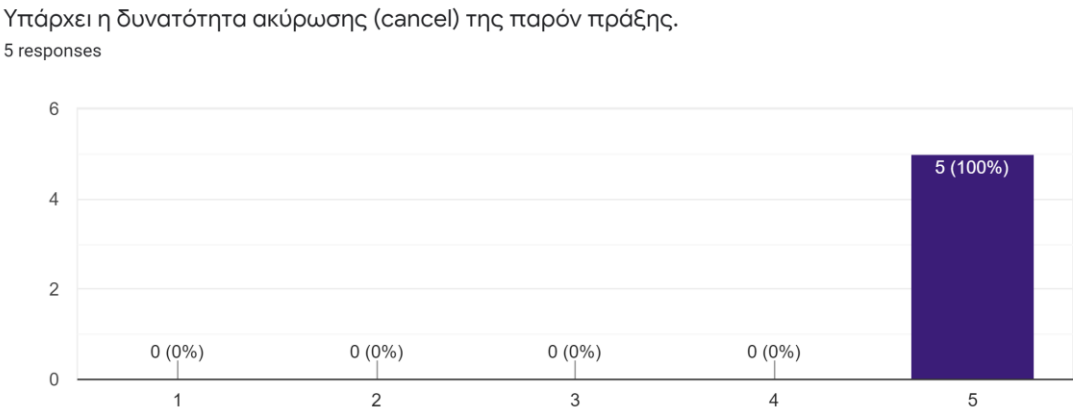
Σχήμα Γ.3 1. Ορατότητα της κατάστασης του συστήματος - Ερώτηση 3



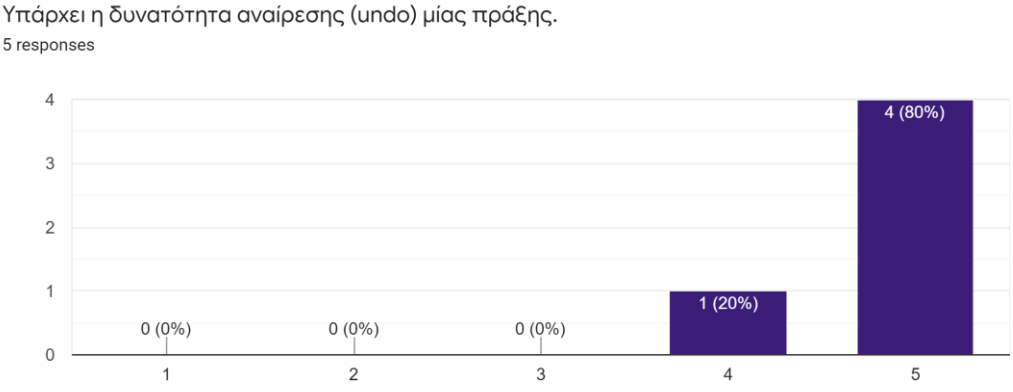
Σχήμα Γ.4 2. Συμφωνία του συστήματος με τον έξω κόσμο - Ερώτηση 1



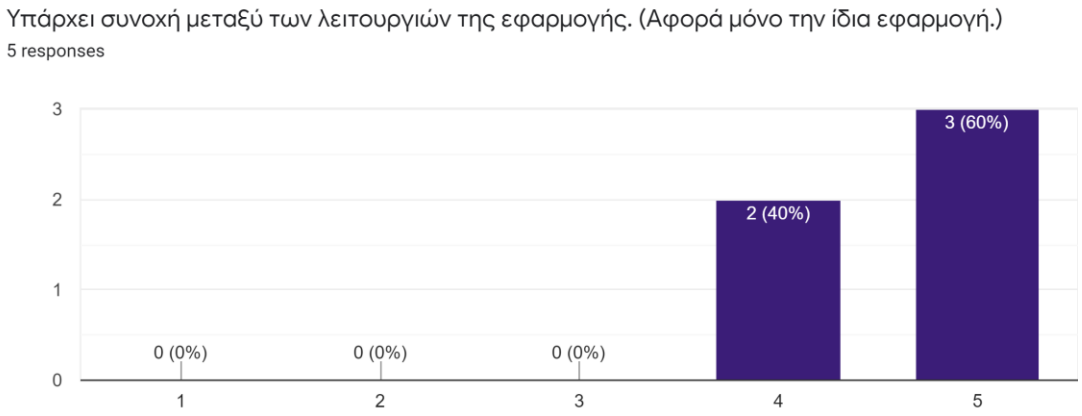
Σχήμα Γ.5 2. Συμφωνία του συστήματος με τον έξω κόσμο - Ερώτηση 2



Σχήμα Γ.6 3. Έλεγχος και ελευθερία του χρήστη - Ερώτηση 1



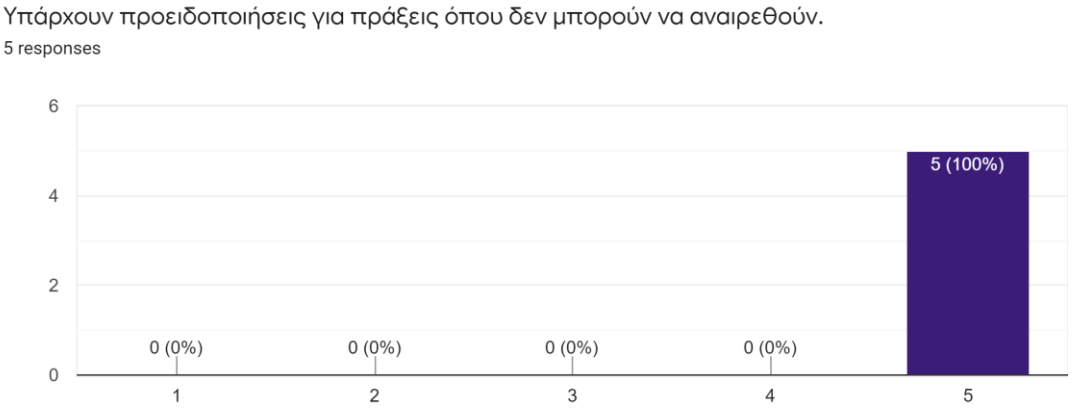
Σχήμα Γ.7 3. Έλεγχος και ελευθερία του χρήστη - Ερώτηση 2



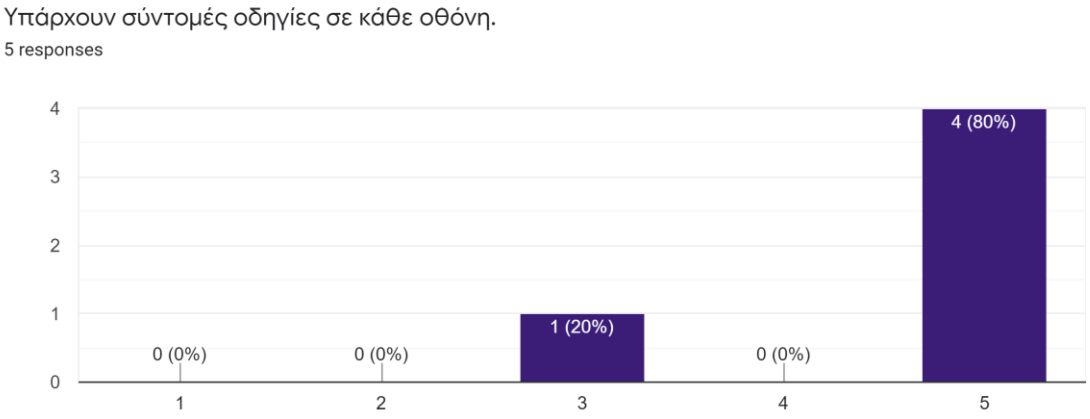
Σχήμα Γ.8 4. Συνοχή και συμμόρφωση έναντι προτύπων - Ερώτηση 1

Σχήμα Γ.9 4. Συνοχή και συμμόρφωση έναντι προτύπων - Ερώτηση 2

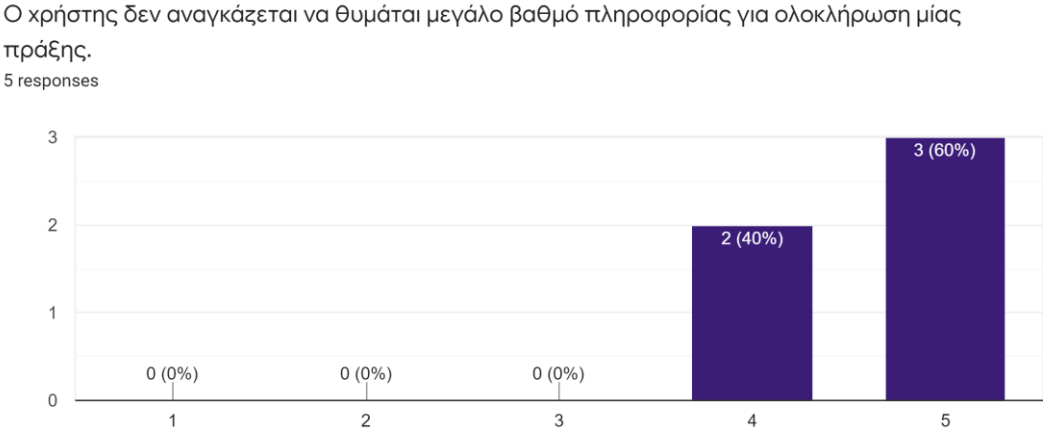
Σχήμα Γ.10 5. Πρόσληψη Σφαλμάτων - Ερώτηση 1



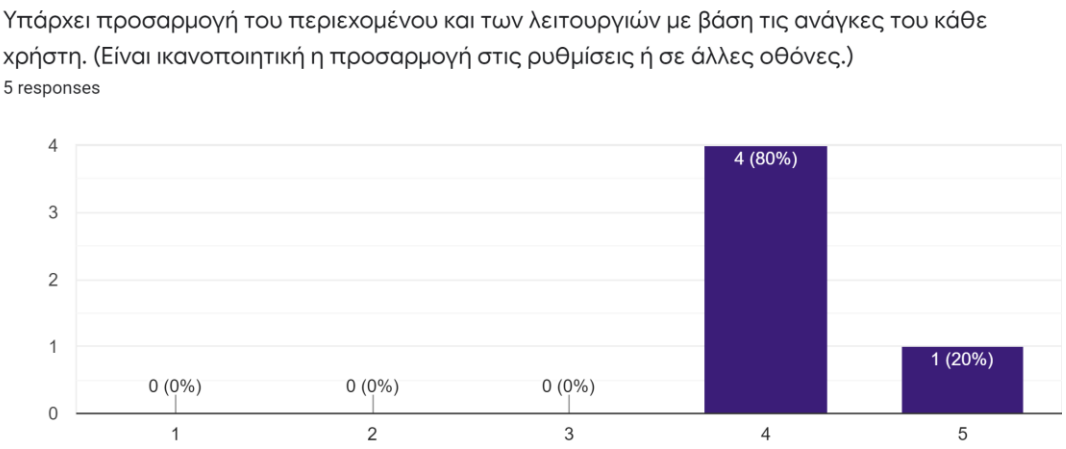
Σχήμα Γ.11 5. Πρόσληψη Σφαλμάτων - Ερώτηση 2



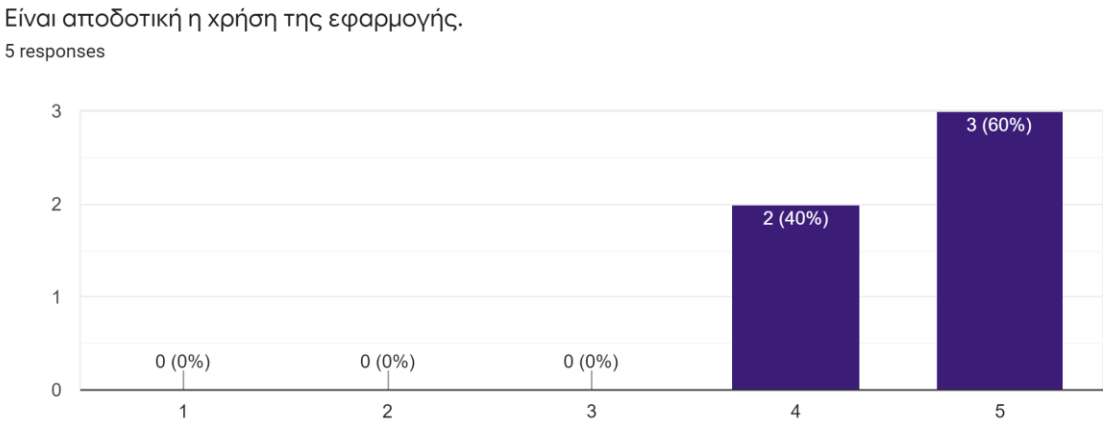
Σχήμα Γ.12 6. Αναγνώριση όχι ανάκληση - Ερώτηση 1



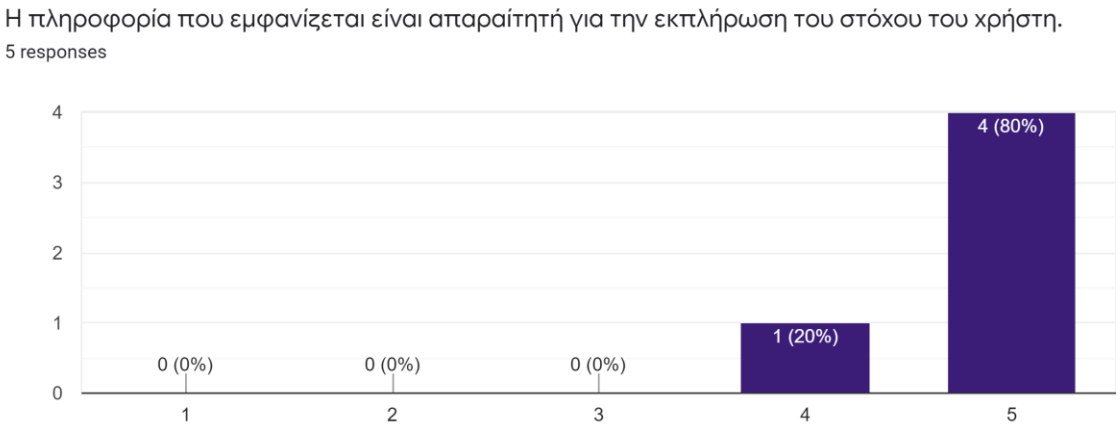
Σχήμα Γ.13 6. Αναγνώριση όχι ανάκληση - Ερώτηση 2



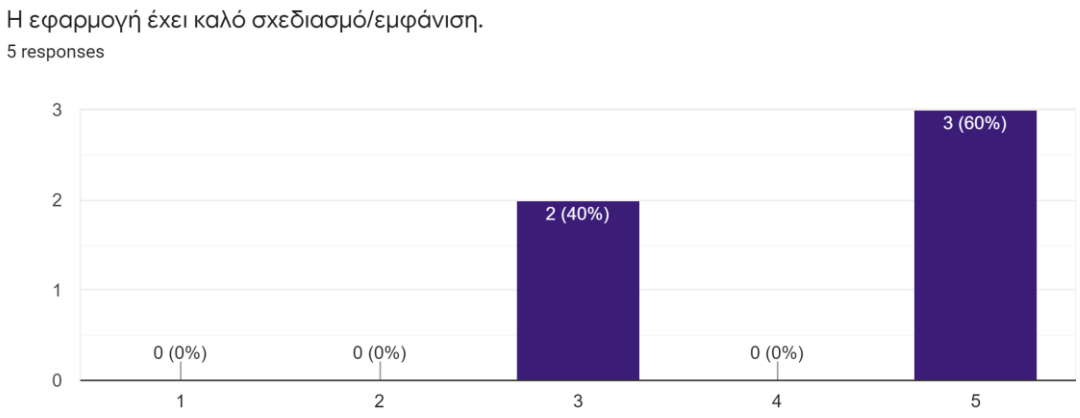
Σχήμα Γ.14 7. Προσαρμοστικότητα και αποδοτικότητα χρήσης - Ερώτηση 1



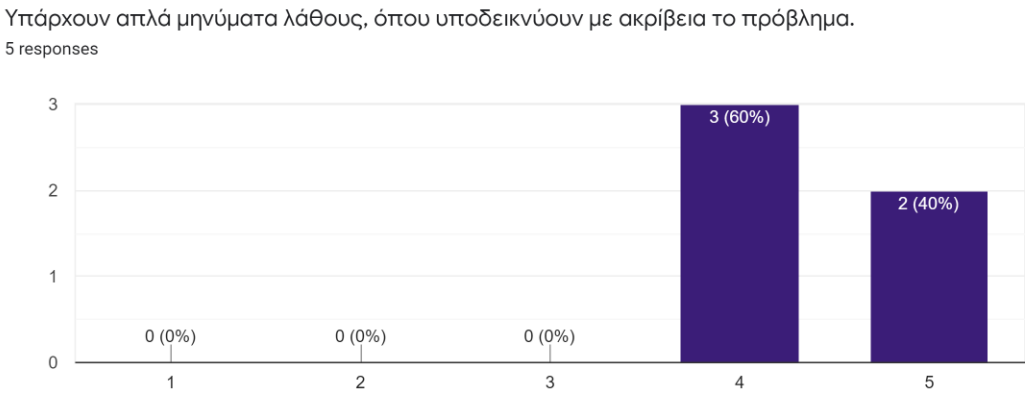
Σχήμα Γ.15 7. Προσαρμοστικότητα και αποδοτικότητα χρήσης - Ερώτηση 2



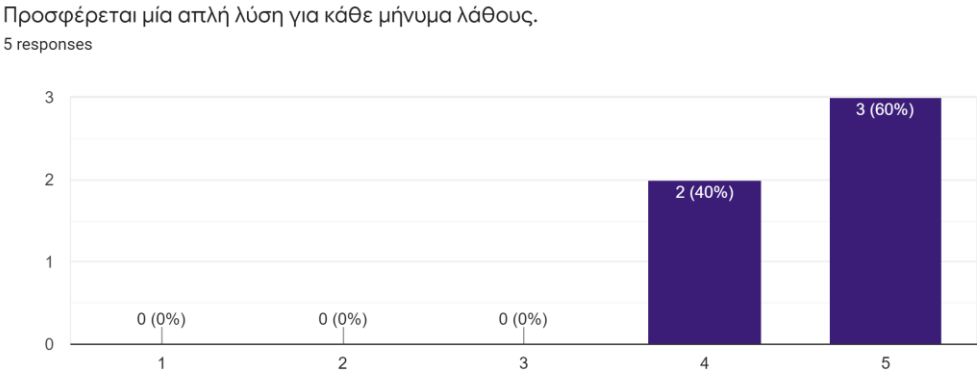
Σχήμα Γ.16 8. Καλαισθητικός σχεδιασμός - Ερώτηση 1



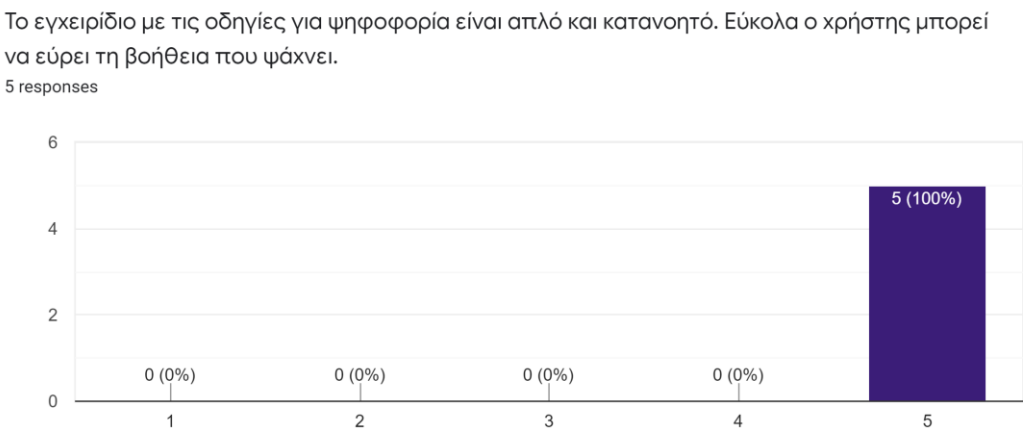
Σχήμα Γ.17 8. Καλαισθητικός σχεδιασμός - Ερώτηση 2



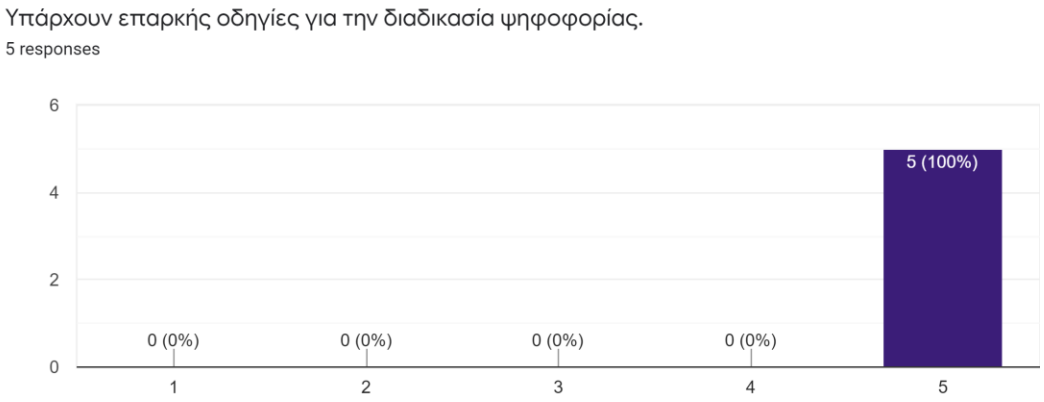
Σχήμα Γ.18 9. Βοήθεια , αναγνώριση , διάγνωση και ανάκαμψη από λάθη - Ερώτηση 1



Σχήμα Γ.19 9. Βοήθεια , αναγνώριση , διάγνωση και ανάκαμψη από λάθη - Ερώτηση 2



Σχήμα Γ.20 10. Βοήθεια και εγχειρίδια - Ερώτηση 1



Σχήμα Γ.21 10. Βοήθεια και εγχειρίδια - Ερώτηση 2

Παράρτημα Δ

Οδηγίες εγκατάστασης του συστήματος

Ο σύνδεσμος για τα αρχεία του συστήματος: https://ucy-my.sharepoint.com/:f:/g/personal/kgeorg01_ucy_ac_cy/Eg2OIVdDT05KmTjnzWbL1sIBsifGEeOu_kPT6NG1QI5j2w?e=ckhrkK

Το σύστημα είναι μόνο προσβάσιμο μόνο σε άτομα που βρίσκονται στο δίκτυο του τμήματος πληροφορικής. Υπάρχει η δυνατότητα για σύνδεση από αποστάσεως μέσο VPN. Ο οδηγός του πανεπιστήμιού για σύνδεση με VPN http://its.cs.ucy.ac.cy/images/stories/uploads/guides/vpn.pdf .

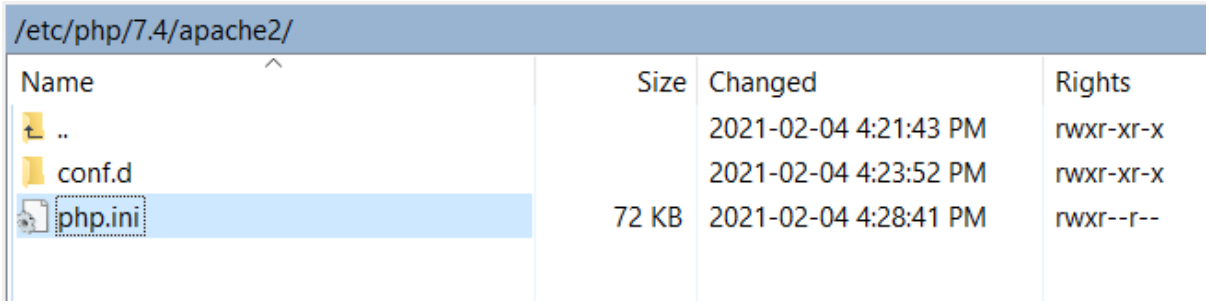
Για την χρήση της εφαρμογής στη διεύθυνση που τρέχει ο χρήστης πρέπει να την εγκαταστήσει και να συνδεθεί. Η εφαρμογή (ElectronicVoting.apk) μπορεί να εγκατασταθεί σε κινητό με λογισμικό android 4.4 ως και android 11 ή σε κάποιο εξομοιωτής (emulator), με android 4.4 ως και android 11, όπως android studio emulator https://developer.android.com/studio/run/emulator. Είναι σημαντικό να σημειωθεί ότι το πιο πιθανό η εφαρμογή μπορεί να δουλεύει για android 11+, οι δοκιμές που έγιναν είναι μέχρι android 11. Ένας εύκολος τρόπος σύνδεσης στην εφαρμογή είναι η χρήση «test##» ονομάτων, όπου όλοι έχουν κωδικό «12345», Για παράδειγμα username: “test10” , password: “12345”. Οι υπόλοιπο χρήστες έχουν το ίδιο όνομα και κωδικό, για παράδειγμα ο χρήστης “aabrahami8l” έχει κωδικό “ aabrahami8l”.

Η ιστοσελίδα του συστήματος είναι προσβάσιμη μέσω του αρχείου “main.php”, (http://thesis.in.cs.ucy.ac.cy/ElectronicVoting/ElectronicVoting/main.php). Οι λειτουργίες τις είναι η δημιουργία κλειδιών κρυπτογράφησης, η έναρξη της εκλογικής διαδικασίας και ο υπολογισμός του τελικού αποτελέσματος. Η δημιουργία κλειδιού κρυπτογράφησης γίνεται μόνο μία φορά στην αρχή της εκλογής. (Χρειάζεται δικαίωμα “write” για να δημιουργηθεί το αρχείο με το κλειδί.) Οι 4 κωδικοί που χρησιμοποιήθηκαν στην δημιουργία του κλειδιού κρυπτογράφησης, θα πρέπει να χρησιμοποιηθούν για τον υπολογισμό του τελικού αποτελέσματος. Το παρόν κλειδί κρυπτογράφησης δημιουργήθηκε τους κωδικούς «ABC», «123», «DEF», «456». Η εκλογική διαδικασία μπορεί να ξεκινήσει με το κουμπί “Start Election” και σταματά όταν υπολογιστή το τελικό αποτέλεσμα.

Σχήμα Δ.1 Η εμφάνιση στης ιστοσελίδας του συστήματος.

Οι επόμενες οδηγίες αφορούν μόνο την χρήση της εφαρμογής σε διαφορετική διεύθυνση. Δεν είναι απαραίτητες αν χρησιμοποιηθεί η τρέχον διεύθυνση του συστήματος.

Αρχικά θα αναφερθεί το λογισμικό του συστήματος. Η android εφαρμογή τρέχει σε τηλέφωνα android με λογισμικό android 4.4 ως android11. Είναι σημαντικό να σημειωθεί ότι το πιο πιθανό η εφαρμογή μπορεί να δουλεύει για android 11+, οι δοκιμές που έγιναν είναι μέχρι android 11. Οι οντότητες τρέχουν σε Linux-Ubuntu, αλλά μπορεί να τρέχουν και σε άλλα λειτουργικά συστήματα. Το λογισμικό του συστήματος είναι apache2, PHP7.2 με "sodium" extension και MySQL. Η διαχείριση του MySQL γίνεται μέσω του phpMyAdmin. Ένας απλός τρόπος εγκατάστασης των πιο πάνω είναι η χρήση του XAMPP. Η ιστοσελίδα του XAMPP είναι https://www.apachefriends.org/index.html. Για την ενεργοποίηση "sodium" extension ("extension=sodium") συμβουλευτείτε τη πιο κάτω ιστοσελίδα: http://phpweb.hostnet.com.br/manual/en/install.pecl.windows.php.

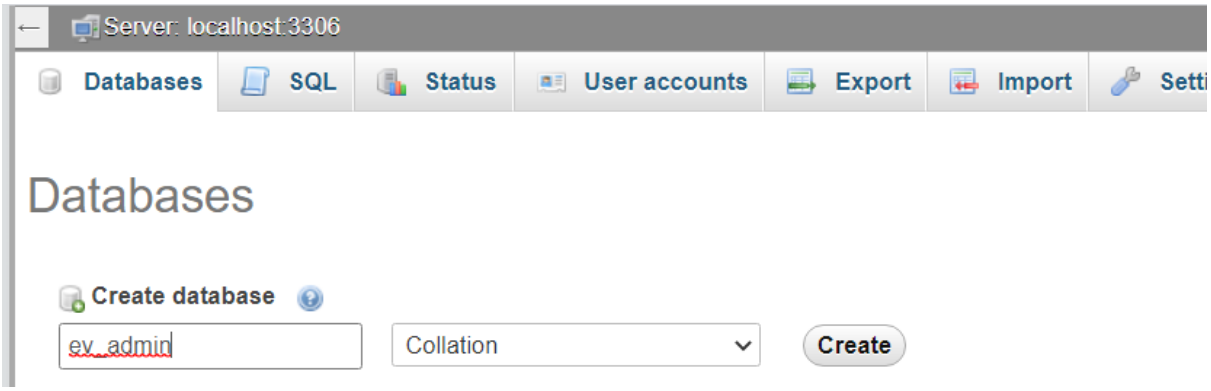


Σχήμα Δ.2 Παράδειγμα τοποθεσίας του php.ini για την ενεργοποίηση του sodium. (Sodium απαιτεί php7.2+)

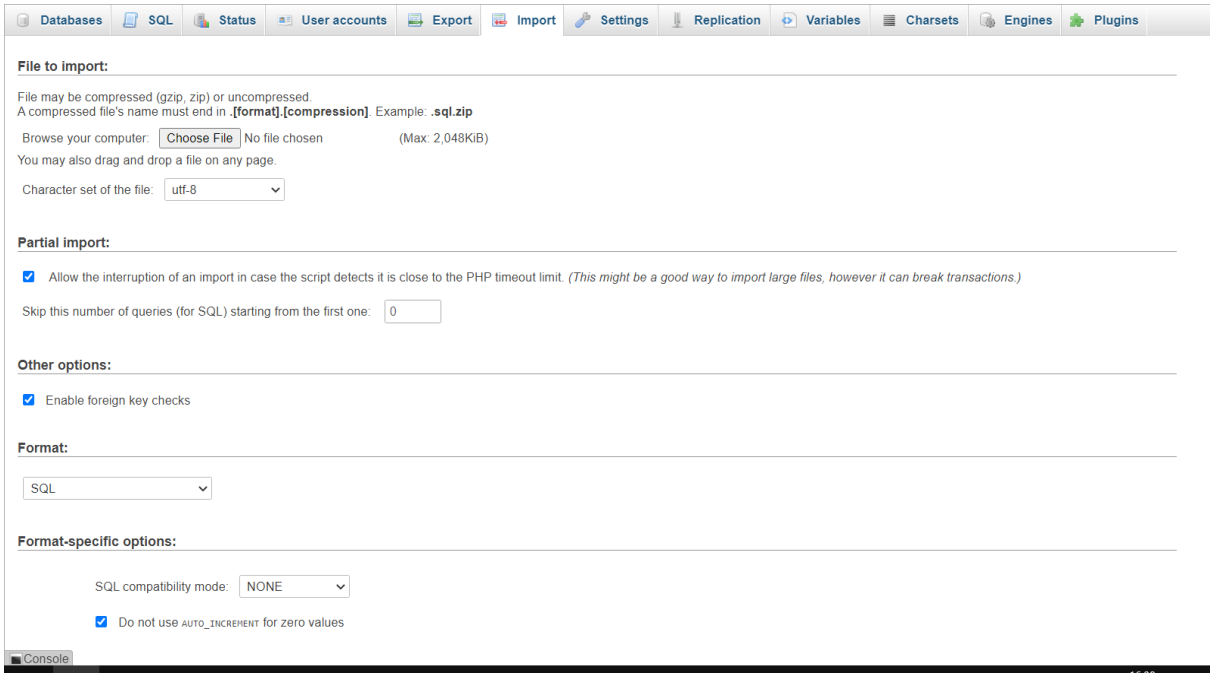
```
936 ;extension=pgsql
937 ;extension=shmop
938
939 ; The MIBS data available in the PHP distribution must be installed.
940 ; See http://www.php.net/manual/en/snmp.installation.php
941 ;extension=snmp
942
943 ;extension=soap
944 ;extension=sockets
945 extension=sodium
946 ;extension=sqlite3
947 ;extension=tidy
948 ;extension=xmlrpc
949 ;extension=xsl
950
951 ;;;;;;;;;;;;;;;;;;;
952 ; Module Settings ;
953 ;;;;;;;;;;;;;;;;;;;
954
955 [CLI Server]
956 ; Whether the CLI web server uses ANSI color coding in its terminal output.
957 cli_server.color = On
```

Σχήμα Δ.3 Με την διαγραφεί του ";", ενεργοποιείται η επέκταση sodium. Μπορεί να χρειάζεται η επανεκκίνηση του apache2.

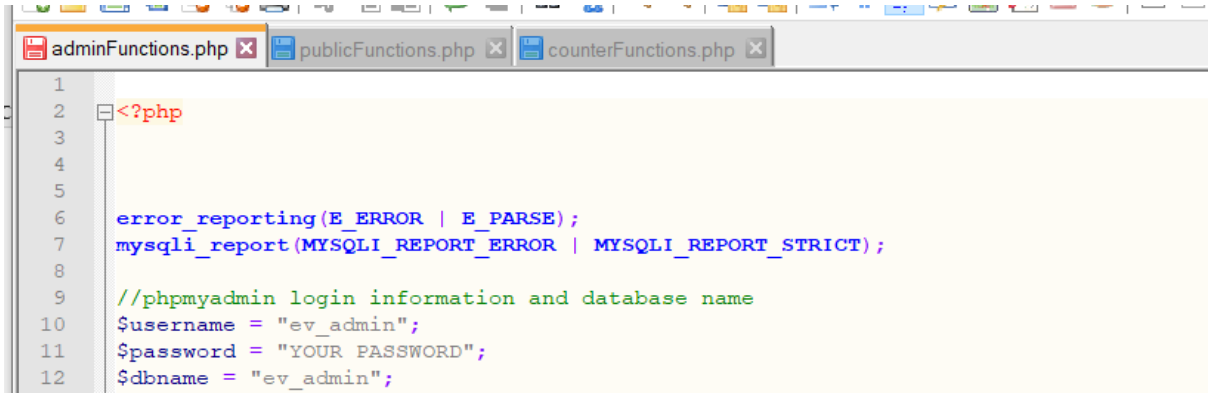
Στη συνέχεια θα αναφερθεί η δημιουργία των βάσεων δεδομένων. Όπως αναφέρθηκε πιο πάνω χρησιμοποιήθηκε phpMyAdmin για την διαχείριση των βάσεων δεδομένων. Υπάρχουν 3 ξεχωριστές βάσεις, το όνομα τις κάθε μίας είναι ev_admin, ev_counter και ev_public. Η κάθε βάση δεδομένων ανήκει στην αντίστοιχη οντότητα και σε κάθε βάση δεδομένων γίνεται εισαγωγή του αντίστοιχου sql αρχείου. Ο διαχειριστής και το κοινό έχουν ψεύτικα δεδομένα (χρήστες και ανακοινώσεις, παρατάξεις, υποψήφιοι) για τον έλεγχο της εφαρμογής, τα οποία μπορούν να αντικατασταθούν με αληθινά δεδομένα. Στο τέλος πρέπει να γίνουν αλλαγές στα αρχεία adminFunctions, counterFunctions και publicFunctions, ώστε ο κωδικός σύνδεσης να είναι ο σωστός.



Σχήμα Δ.4 Στη σελίδα Databases μπορείτε να δημιουργήσετε τις βάσεις δεδομένων.

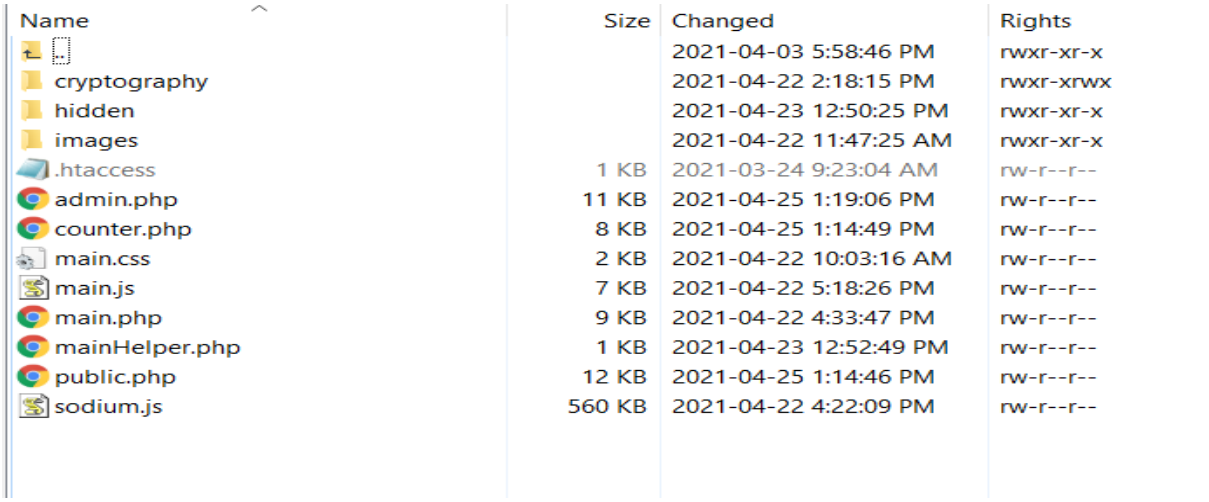


Σχήμα Δ.5 Στη σελίδα Import μπορείτε να εισάγεται τα .sql αρχεία.



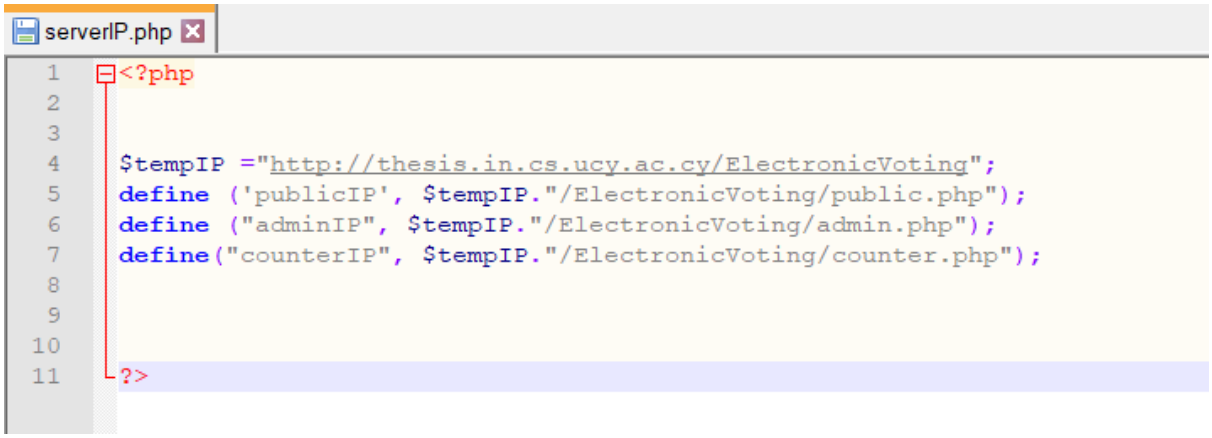
Σχήμα Δ.6 Πρέπει να αλλαχθεί ο κωδικός και τα υπόλοιπα στοιχεία.

Στη συνέχεια θα αναφερθούν οι οδηγίες για το φάκελο “ElectronicVoting”, όπου είναι ο κώδικας των οντοτήτων. Ολόκληρος ο φάκελος μπορεί να τοποθετηθεί στο «/var/www/html» όσο αφορά Linux ή στο φάκελο htdocs του XAMPP. Το αρχείο serverIP στο φάκελο “ElectronicVoting/hidden” πρέπει να περιέχει τη IP διεύθυνση που βρίσκονται τα αρχεία.



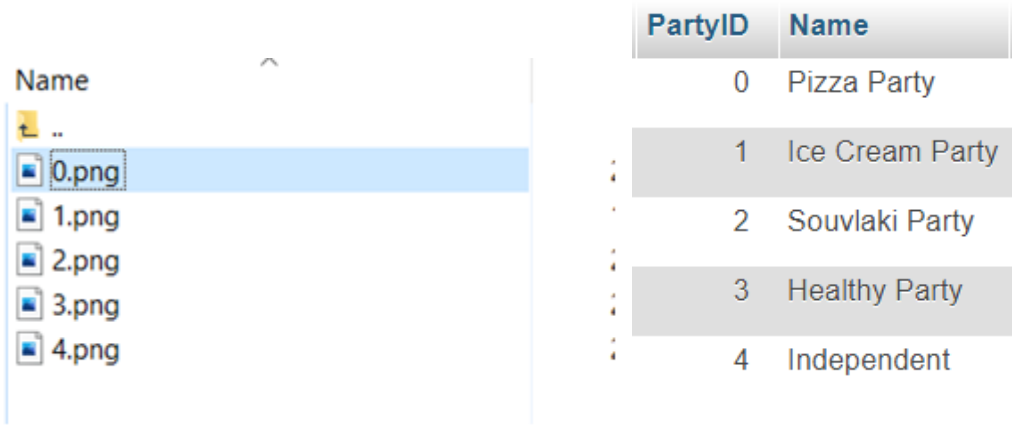
Name	Size	Changed	Rights
..		2021-04-03 5:58:46 PM	rwxr-xr-x
cryptography		2021-04-22 2:18:15 PM	rwxr-xrwx
hidden		2021-04-23 12:50:25 PM	rwxr-xr-x
images		2021-04-22 11:47:25 AM	rwxr-xr-x
.htaccess	1 KB	2021-03-24 9:23:04 AM	rw-r--r--
admin.php	11 KB	2021-04-25 1:19:06 PM	rw-r--r--
counter.php	8 KB	2021-04-25 1:14:49 PM	rw-r--r--
main.css	2 KB	2021-04-22 10:03:16 AM	rw-r--r--
main.js	7 KB	2021-04-22 5:18:26 PM	rw-r--r--
main.php	9 KB	2021-04-22 4:33:47 PM	rw-r--r--
mainHelper.php	1 KB	2021-04-23 12:52:49 PM	rw-r--r--
public.php	12 KB	2021-04-25 1:14:46 PM	rw-r--r--
sodium.js	560 KB	2021-04-22 4:22:09 PM	rw-r--r--

Σχήμα Δ.7 Η εμφάνιση του φακέλου “ElectronicVoting”.

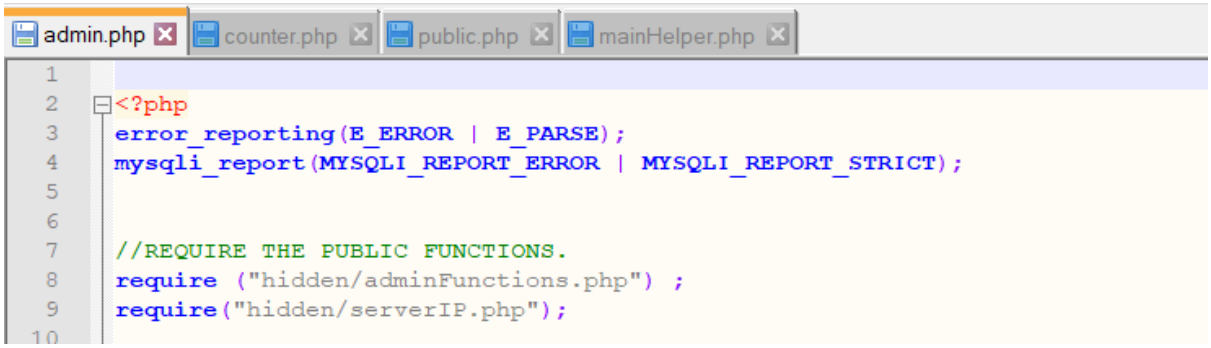


Σχήμα Δ.8 Το “tempIP” πρέπει να είναι η IP διεύθυνση που βρίσκονται τα αρχεία, άρα πρέπει να αλλαχθεί στη νέα διεύθυνση .

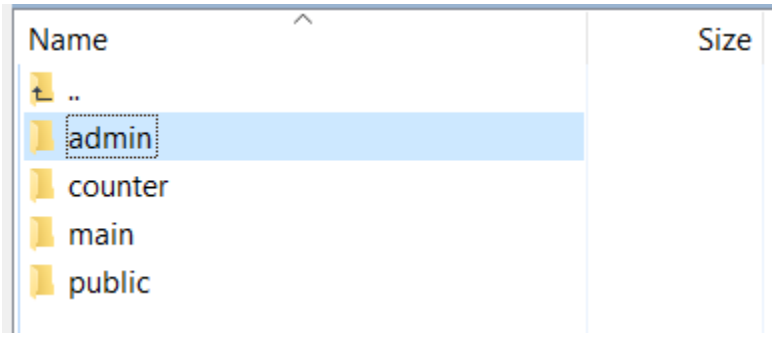
Οι πιο κάτω οδηγίες είναι μόνο χρήσιμες αν χρειαστούν να γίνουν αλλαγές στα δεδομένα για πραγματοποίηση μίας εκλογής ή στην κατανομή των οντοτήτων. Το σύστημα μπορεί να δουλέψει χωρίς να γίνει κάποια αλλαγή. Προς το παρόν οι εικόνες αφορούν τα ψεύτικα δεδομένα. Σε μία πραγματική εκλογική διαδικασία οι εικόνες στο φάκελο «images» πρέπει να αντικατασταθούν με τις εικόνες των παρατάξεων και υποψηφίων βάση το partyID, candidateID στην βάση δεδομένων. Κάθε οντότητα (admin.php , counter.php , public.php, main.php) εξαρτάται από το αρχείο με της μεθόδους της και το “serverIP.php” στο φάκελο “ElectronicVoting/hidden”. Εξαίρεση είναι η οντότητα «main.php», όπου εξαρτάται από όλα τα αρχεία όπου ξεκινούν με main και το sodium.js που βρίσκονται στο φάκελο “ElectronicVoting”. Όσο αφορά τα αρχεία στο φάκελο “ElectronicVoting/cryptography”, κάθε οντότητα εξαρτάται μόνο από τα κλειδιά στο φάκελο της.



Σχήμα Δ.9 Η εικόνα "0.png" στο φάκελο "parties" αφορά την πολιτική ομάδα, στη βάση δεδομένων του κοινού (ev_public), με αναγνωριστικό 0 όπου είναι το Pizza Party.



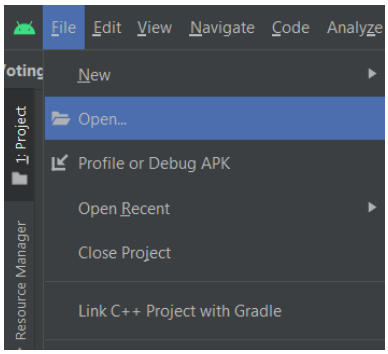
Σχήμα Δ.10 Το αρχείο "admin.php" χρησιμοποιεί της μεθόδους από το αρχείο "adminFunctions.php" και τις σταθερές στο αρχείο "serverIP.php".



Σχήμα Δ.11 Το αρχείο "admin.php" χρησιμοποιεί μόνο τα αρχεία στο "cryptography/admin" φάκελο.

Η τελευταία αλλαγή που έμεινε είναι στο κώδικα της εφαρμογής. Στη ανάπτυξη της εφαρμογής χρησιμοποιήθηκε το android studio με γλώσσα Kotlin, https://developer.android.com/studio. Ο φάκελος "UCYThesisElectronicVoting" είναι το project που δημιουργήθηκε στο android studio και μπορεί να ανοιχθεί με αυτό. Το αρχείο "FinalValues" στο φάκελο "values" περιέχει την διεύθυνση του συστήματος. Πρέπει να

αλλάξουν οι μεταβήτές “serverIP”, “adminIP”, “counterIP” και “publicIP” στη νέα διεύθυνση του συστήματος. Στη συνέχεια να γίνει build η εφαρμογή και να εγκατασταθεί στο κινητό.



Σχήμα Δ.12 Από το android studio , file ->open, μεταβείτε στο φάκελο που είναι το “UCYThesisElectronicVoting” και ανοίξετε το.

```
    //Where the images are
    val serverIP= "http://thesis.in.cs.ucy.ac.cy/ElectronicVoting/ElectronicVoting/"

    //where admin , counter , public are
    val adminIP= "http://thesis.in.cs.ucy.ac.cy/ElectronicVoting/ElectronicVoting/admin.php"
    val publicIP= "http://thesis.in.cs.ucy.ac.cy/ElectronicVoting/ElectronicVoting/public.php"
    val counterIP= "http://thesis.in.cs.ucy.ac.cy/ElectronicVoting/ElectronicVoting/counter.php"
}
}
```

Σχήμα Δ.13 Το αρχείο FinalValues.kt με τις διευθύνσεις των οντοτήτων.

Ο τρόπος υπολογισμούς του κατακερματισμένου κωδικού για την αποθήκευση στη βάση δεδομένων είναι η συνάρτηση “sodium_crypto_pwhash_str_verify”, περισσότερες πληροφορίες στο https://www.php.net/manual/en/function.sodium-crypto-pwhash-str.php και στο https://www.php.net/manual/en/function.sodium-crypto-pwhash-str-verify.php. Μπορεί να χρησιμοποιηθεί άλλη μέθοδος κατακερματισμού του κωδικού για αποθηκεύσει στη βάση δεδομένων αλλά πρέπει να αλλάξει η μέθοδος “validateLogin” στο “ElectronicVoting/hidden/adminFunctions”. Αν διατηρηθεί αυτή η μέθοδος, τότε οι νέοι κωδικοί των χρηστών πρέπει να κατακερματιστούν με το sodium-crypto-pwhash-str, πριν να αποθηκευτούν στην βάση δεδομένων.

username	Firstname	Lastname	email	password
aabrahami8l	Antonietta	Abrahami	aabrahami8l@university.com	$argon2id$v=19$m=262144,t=3,p=1$oWwwikcS0DBjVLvLDNRxfw$aW+70Suj o6GU9Swbb7X+JNSuSj4LI+e4dxbPriRHQNY
aarlott1x	Agathe	Arlott	aarlott1x@university.com	$argon2id$v=19$m=262144,t=3,p=1$pzMjSAJdoQ6SprlmP8...
abasill8o	Andi	Basill	abasill8o@university.com	$argon2id$v=19$m=262144,t=3,p=1$rNjlcEW8q4cZnFkI44...
abaystondu	Ashia	Bayston	abaystondu@university.com	$argon2id$v=19$m=262144,t=3,p=1$CL3Jo1vqP9mQyi746X...
abelamybb	Anthia	Belamy	abelamybb@university.com	$argon2id$v=19$m=262144,t=3,p=1$8rPowGUzSdAlVbZttp...
aboldisoncr	Aloisia	Boldison	aboldisoncr@university.com	$argon2id$v=19$m=262144,t=3,p=1$AZ5OVHcfBS01lRsq8B...

Σχήμα Δ.14 Ο πίνακας user του ev_admin περιέχει του κατακερματισμένους κωδικούς με χρήση sodium-crypto-pwhash-str

```php
function validateLogin ($conn,$username,$password) {

    $sql="CALL getPassword('".$username."')" ;
    $result = $conn->query($sql);
    $row = $result->fetch_assoc();
    $hashedPassword=$row['password'];
    $obj = new stdClass;
    if ($hashedPassword==null) {
        $obj->success="0";
        sleep(2);
    } else {
        $flag = sodium_crypto_pwhash_str_verify($hashedPassword ,$password);
        if ($flag)  $obj->success="1";
        else  $obj->success="0";
    }

    return $obj;
}
```

Σχήμα Δ.15 Η μέθοδος validateLogin, όπου γίνεται η αυθεντικοποίηση του χρήστη.