



ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ
ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Μελέτη συστημάτων ηλεκτρονικής ψηφοφορίας και
ανάπτυξη εφαρμογής»



ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

Ηλεκτρονικό Σύστημα Ψηφοφορίας

Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων

Διεθνές Πανεπιστήμιο Ελλάδος

Σύνδεση

Φοιτητής

Χρυσόμαλλος Κωνσταντίνος 516165

Επιβλέπων

Δρ. Κυριάκος Τσιακμάκης

Φεβρουάριος 2021

Μελέτη συστημάτων ηλεκτρονικής ψηφοφορίας και ανάπτυξη εφαρμογής

Κωδικός: 20214

Φοιτητής: Κωνσταντίνος Χρυσόμαλλος

Εισηγητής: Δρ Κυριάκος Τσιακμάκης

Ημερομηνία ανάληψης Π.Ε. 25-10-2020

Ημερομηνία περάτωσης Π.Ε. 15-01-2021

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως πτυχιακή εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή Κωνσταντίνου Χρυσόμαλλου που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Διεθνές Πανεπιστήμιο της Ελλάδος άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοικτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Περίληψη

Η εργασία αυτή αφορά τη μελέτη συστημάτων και ανάπτυξη εφαρμογής ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου. Μελετήθηκαν υπάρχοντα συστήματα διαδικτυακής ψηφοφορίας και ιδιαίτερα το ελληνικό σύστημα ηλεκτρονικής ψηφοφορίας το Zeus το οποίο χρησιμοποιείται από τα Ελληνικά Πανεπιστήμια και φορείς της εκπαίδευσης. Υλοποιήθηκε μια web εφαρμογή χρησιμοποιώντας το γνωστό PHP framework Laravel για να μπορούν οι φοιτητές και το προσωπικό μέσα στο Τμήμα να δημιουργήσουν μια ηλεκτρονική ψηφοφορία και να συμμετέχουν τα μέλη του τμήματος χρησιμοποιώντας τα ίδια στοιχεία πρόσβασης τους που χρησιμοποιούν και σε άλλες υπηρεσίες.

«Study of electronic voting systems and development of application »

Abstract

This work concerns the study of electronic voting systems and the development of an electronic voting application via the Internet. Existing online voting systems were studied, especially the Greek electronic voting system Zeus, which is used by Greek universities and educational institutions. A web application has been implemented using the well-known PHP framework Laravel so that students and staff within the Department can create an electronic voting and participate in the department using the same access data they use in other services.

Ευχαριστίες

Θέλω να ευχαριστήσω τους γονείς μου για τη συμπαράσταση τους και τον επιβλέπων κ. Τσιακμάκη Κυριάκο για τη συνεχή παιδαγωγική καθοδήγηση, επιστημονικές οδηγίες του και συμβολή του στον κώδικα της εφαρμογής.

Περιεχόμενα

Περίληψη	iv
Abstract	v
Ευχαριστίες	vi
Περιεχόμενα.....	vii
Κατάλογος Σχημάτων	viii
Κεφάλαιο 1ο: Εισαγωγή.....	1
1.1 Εισαγωγή.....	1
1.2 Συνεισφορά της εργασίας.....	2
1.3 Δομή της εργασίας	2
Κεφάλαιο 2ο: Βιβλιογραφική Ανασκόπηση	3
2.1 Εισαγωγή.....	3
2.2 Τύποι Ηλεκτρονικής Ψηφοφορίας	5
2.3 Νομικά ζητήματα που εγείρει η χρήση ηλεκτρονικών μεθόδων ψηφοφορίας.....	8
2.4 Ηλεκτρονικές Ψηφοφορίες ΖΕΥΣ	8
2.5 Πλεονεκτήματα-Μειονεκτήματα ηλεκτρονικής ψηφοφορίας.....	13
Κεφάλαιο 3ο: Τεχνολογία και εργαλεία.....	15
3.1 PHP	15
3.2 MySQL.....	17
3.3 Laravel	18
Κεφάλαιο 4ο: Το σύστημα ηλεκτρονικής ψηφοφορίας	23
4.1 Εισαγωγή – Η διαδικασία	23
4.2 Η εφαρμογή - ιστοσελίδα.....	30
4.3 Η Βάση.....	38
4.4 Ασφάλεια στο σύστημα και στα δεδομένα	43
Κεφάλαιο 5ο: Συμπεράσματα και προτάσεις βελτίωσης	44
ΒΙΒΛΙΟΓΡΑΦΙΑ	46
ΠΑΡΑΡΤΗΜΑ Α.....	47

Κατάλογος Σχημάτων

Σχήμα 2.1: Ηλεκτρονική Ψηφοφορία ZEYΣ	9
Σχήμα 2.2: Απαραίτητα πεδία για τη δημιουργία νέας ψηφοφορίας 1 - Zeus	10
Σχήμα 2.3: Απαραίτητα πεδία για τη δημιουργία νέας ψηφοφορίας 2 - Zeus	11
Σχήμα 3.1: PHP 7	15
Σχήμα 3.2: Laravel λογότυπο	18
Σχήμα 3.3: MVC.....	19
Σχήμα 3.4: Laravel ORM	20
Σχήμα 4.1: Το σύστημα – η εφαρμογή.....	23
Σχήμα 4.2: Εισαγωγή στοιχείων πρόσβασης	23
Σχήμα 4.3: Δημιουργία Ψηφοφορίας	24
Σχήμα 4.4: Η κεντρική σελίδα με τις λίστες	25
Σχήμα 4.5: Διαδικασία από τη δημιουργία μέχρι την αποστολή πρόσκλησης για κάθε μέλος της εφορευτικής.....	25
Σχήμα 4.6: Διαδικασία για την αποδοχή από ένα χρήστη να είναι μέλος μιας εφορευτικής επιτροπής.....	26
Σχήμα 4.7: Διαδικασία κατάθεσης ψήφου από κάποιον Χρήστη.	27
Σχήμα 4.8: Διαδικασία μετά τη λήξη ψηφοφορίας	28
Σχήμα 4.9: Μέθοδος κρυπτογράφηση/αποκρυπτογράφησης για την κατάθεση ψήφου και την εξαγωγή-καταμέτρηση των ψήφων/αποτελεσμάτων.....	29
Σχήμα 4.10: Μέθοδος κρυπτογράφηση/αποκρυπτογράφησης για την κατάθεση ψήφου και την εξαγωγή-καταμέτρηση.....	30
Σχήμα 4.11: Το πεδίο εισαγωγής Τίτλου για τη Ψηφοφορία όταν δεν είναι επιτυχής η εισαγωγή χαρακτήρων	31
Σχήμα 4.12: Τα πεδία εισαγωγής Τίτλου και Περιγραφής για τη Ψηφοφορία όταν είναι επιτυχής η εισαγωγή χαρακτήρων.....	31
Σχήμα 4.13: Τα πεδία εισαγωγής για Ημερομηνία/Ωρα Έναρξης και Λήξης για τη Ψηφοφορία ...	32
Σχήμα 4.14: Η επιλογή για την Ημερομηνία	32
Σχήμα 4.15: Η επιλογή για την Ώρα	33
Σχήμα 4.16: Τα πεδία εισαγωγής/επιλογής για το email Υποστήριξης, της Εφορευτικής Επιτροπής και το είδος των Ψηφοφόρων που μπορούν να συμμετέχουν στη Ψηφοφορία.....	34
Σχήμα 4.17: Το πεδίο εισαγωγής για το email Υποστήριξης όταν δεν ικανοποιούνται οι απαιτούμενες προϋποθέσεις στην εισαγωγή.....	34
Σχήμα 4.18: Το πεδίο εισαγωγής για τα μέλη της εφορευτικής επιτροπής	35
Σχήμα 4.19: Η λίστα για τα μέλη της εφορευτικής επιτροπής όπως την επέλεξε χρήστης	35
Σχήμα 4.20: Τα πεδία για το ελάχιστο και μέγιστο πλήθος επιλογών	36
Σχήμα 4.21: Το πεδίο για την ερώτηση που θα υπάρχει στην Ψηφοφορία για να κατατοπίσει τον ψηφοφόρο	36
Σχήμα 4.22: Προσθήκη κενών επιλογών.....	37

Σχήμα 4.23: Οι επιλογές που έχουν προστεθεί με το κουμπί '+'	37
Σχήμα 4.24: Η βάση με τους πίνακες.....	38
Σχήμα 4.25: Ο πίνακας roll - Δομή	39
Σχήμα 4.26: Ο πίνακας Roll - Περιεχόμενο	39
Σχήμα 4.27: Ο πίνακας committee - Δομή.....	40
Σχήμα 4.28: Ο πίνακας committee - Περιεχόμενο	40
Σχήμα 4.24: Ο πίνακας result - Δομή	40
Σχήμα 4.30: Ο πίνακας result - Περιεχόμενο.....	41
Σχήμα 4.31: Ο πίνακας vote - Δομή	41
Σχήμα 4.32: Ο πίνακας vote - Περιεχόμενο.....	41
Σχήμα 4.33: Η βάση με τους πίνακες.....	42

Κεφάλαιο 1ο: Εισαγωγή

1.1 Εισαγωγή

Η τεχνολογία ηλεκτρονικής ψηφοφορίας σκοπεύει να επιταχύνει την καταμέτρηση των ψηφοφόρων, να μειώσει το κόστος του προσωπικού πληρωμής για τη μέτρηση των ψήφων με μη αυτόματο τρόπο και μπορεί να προσφέρει βελτιωμένη προσβασιμότητα για άτομα με ειδικές ανάγκες. Επίσης, μακροπρόθεσμα, τα έξοδα αναμένεται να μειωθούν. Τα αποτελέσματα μπορούν να αναφερθούν και να δημοσιευτούν γρηγορότερα. Οι ψηφοφόροι εξοικονομούν χρόνο και κόστος, έχοντας τη δυνατότητα να ψηφίσουν ανεξάρτητα από την τοποθεσία τους. Αυτό μπορεί να αυξήσει τη συνολική προσέλευση των ψηφοφόρων. Οι ομάδες πολιτών που επωφελούνται περισσότερο από τις ηλεκτρονικές εκλογές είναι αυτές που ζουν στο εξωτερικό, πολίτες που ζουν σε αγροτικές περιοχές μακριά από τα εκλογικά κέντρα και τα άτομα με ειδικές ανάγκες με κινητικά προβλήματα.

Η εργασία αυτή αφορά τη μελέτη συστημάτων και ανάπτυξη εφαρμογής ηλεκτρονικής ψηφοφορίας. Μελετήθηκαν υπάρχοντα συστήματα διαδικτυακής ψηφοφορίας και με επίκεντρο το ελληνικό σύστημα ηλεκτρονικής ψηφοφορίας το Zeus το οποίο χρησιμοποιείται από τα Ελληνικά Πανεπιστήμια και φορείς της εκπαίδευσης. Υλοποιήθηκε μια web εφαρμογή χρησιμοποιώντας το γνωστό PHP framework Laravel για να μπορούν οι φοιτητές και το προσωπικό μέσα στο Τμήμα να δημιουργήσουν μια ηλεκτρονική ψηφοφορία και να συμμετέχουν τα μέλη του τμήματος χρησιμοποιώντας τα ίδια στοιχεία πρόσβασης τους που χρησιμοποιούν και σε άλλες υπηρεσίες.

Ο κύριος στόχος αυτής της εργασίας είναι η μελέτη, η σχεδίαση και η υλοποίηση ενός ασφαλούς συστήματος ηλεκτρονικής ψηφοφορίας που να μπορεί να χρησιμοποιείται από κάθε χρήστη στο Τμήμα.

Συγκεκριμένα, οι επιμέρους στόχοι της εργασίας είναι:

Όλοι οι χρήστες-μέλη του των υπηρεσιών του Τμήματος να μπορούν να έχουν πρόσβαση στο σύστημα Ηλεκτρονικής Ψηφοφορίας.

Οι χρήστες να μπορούν να δημιουργήσουν σε μια ηλεκτρονική ψηφοφορία.

Οι χρήστες να μπορούν να συμμετέχουν ως εφορευτική επιτροπή ή απλοί ψηφοφόροι σε μια ηλεκτρονική ψηφοφορία.

Οι ψήφοι να είναι μυστικοί και κρυπτογραφημένοι.

Η κρυπτογράφηση και η αποκρυπτογράφηση της ψήφου για την καταμέτρηση να γίνεται με κωδικούς που διαθέτει η εφορευτική επιτροπή χωρίς να αποθηκεύεται η κάθε ψήφος σε κάποιο χώρο.

Τα τελικά αποτελέσματα μιας ψηφοφορίας να είναι διαθέσιμα στα μέλη.

1.2 Συνεισφορά της εργασίας

Στην εργασία παρουσιάζεται μια εφαρμογή ενός ασφαλούς συστήματος ηλεκτρονικής ψηφοφορίας που να μπορεί να χρησιμοποιείται από κάθε χρήστη στο Τμήμα. Μπορούν να διοργανώνονται απλές ψηφοφορίες που αφορούν το Τμήμα από κάποιον φοιτητή ή κάποιο μέλος του προσωπικού. Εκτός από την ασφάλεια που παρέχει το μεγαλύτερο κέρδος για το τμήμα είναι η χρήση του από πιστοποιημένους χρήστες που ανήκουν σε αυτό και έχουν πρόσβαση σε ηλεκτρονικές υπηρεσίες του.

1.3 Δομή της εργασίας

Στο πρώτο κεφάλαιο παρουσιάζεται μια μικρή εισαγωγή της εργασίας και οι στόχοι της.

Επιπρόσθετα, αναφέρεται η συνεισφορά της εργασίας και σε ποια σημεία επικεντρώνεται η ανάλυση της.

Στο δεύτερο κεφάλαιο παρουσιάζεται η βιβλιογραφική ανασκόπηση παρόμοιων συστημάτων.

Στο τρίτο κεφάλαιο περιγράφεται η τεχνολογία που χρησιμοποιήθηκε και τα βοηθητικά εργαλεία που ενσωματώνονται σε αυτό.

Στο τέταρτο κεφάλαιο αναλύεται η εφαρμογή με σχήματα και διαγράμματα ενώ στο τέλος παρουσιάζεται και η βάση που χρησιμοποιήθηκε.

Στο πέμπτο κεφάλαιο παρουσιάζονται τα συμπεράσματα της εργασίας και θέματα για μελλοντική έρευνα ενώ στο τέλος της εργασίας παρατίθεται το παράρτημα με κάποιους από τους κώδικες που χρησιμοποιήθηκαν στην εργασία.

Κεφάλαιο 2ο: Βιβλιογραφική Ανασκόπηση

2.1 Εισαγωγή

Με την πάροδο των ετών έχουν δημιουργηθεί ορισμένα ειδικά συστήματα τα οποία προσαρμόζονται στη διαδικασία ψηφοφορίας και έχει γίνει προσπάθεια να διασφαλιστεί το υλικό και το λογισμικό αυτών των συσκευών για να βγει το σωστό αποτέλεσμα και να διασφαλιστεί στον χρήστη η εμπιστευτικότητα των δεδομένων τους και η εμπιστοσύνη ότι η ψήφος τους καταγράφηκε. Μερικά από αυτά τα συστήματα είναι:

Η ηλεκτρονική ψηφοφορία είναι η ψηφοφορία που χρησιμοποιεί ηλεκτρονικά μέσα είτε για να βοηθήσει είτε να φροντίσει για τη μετάδοση και τη μέτρηση των ψήφων.

Ανάλογα με τη συγκεκριμένη εφαρμογή, η ηλεκτρονική ψηφοφορία μπορεί να χρησιμοποιεί αυτόνομα ηλεκτρονικά μηχανήματα ψηφοφορίας (που ονομάζονται επίσης EVM) ή υπολογιστές συνδεδεμένους στο Διαδίκτυο. Μπορεί να περιλαμβάνει μια σειρά υπηρεσιών Διαδικτύου, από τη βασική μετάδοση των αποτελεσμάτων σε πίνακα έως την πλήρη λειτουργία διαδικτυακής ψηφοφορίας μέσω κοινών συνδεδεμένων οικιακών συσκευών. Ο βαθμός αυτοματοποίησης μπορεί να περιορίζεται στη καταγραφή μιας ψηφοφορίας σε χαρτί, ή μπορεί να είναι ένα ολοκληρωμένο σύστημα εισαγωγής ψηφοφορίας, καταγραφής ψηφοφορίας, κρυπτογράφησης δεδομένων και μετάδοσης σε διακομιστές, και ενοποίηση των εκλογικών αποτελεσμάτων.

Ένα αξιολογικό σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να εκτελεί τα περισσότερα από αυτά, ενώ πρέπει να συμμορφώνεται με ένα σύνολο προτύπων που έχουν θεσπιστεί από ρυθμιστικούς φορείς και πρέπει επίσης να είναι ικανό να αντιμετωπίσει επιτυχώς ισχυρές απαιτήσεις που σχετίζονται με την ασφάλεια, την ακρίβεια, την ακεραιότητα, την ταχύτητα, το απόρρητο, τη δυνατότητα ελέγχου, τη δυνατότητα πρόσβασης, οικονομική αποδοτικότητα, επεκτασιμότητα και οικολογική βιωσιμότητα.

Η τεχνολογία ηλεκτρονικής ψηφοφορίας μπορεί να περιλαμβάνει κάρτες διάτρησης, συστήματα ψηφοφορίας οπτικής σάρωσης και εξειδικευμένα περίπτερα ψηφοφορίας (συμπεριλαμβανομένων αυτοτελών ηλεκτρονικών συστημάτων ψηφοφορίας άμεσης εγγραφής ή DRE). Μπορεί επίσης να περιλαμβάνει μετάδοση ψηφοφοριών και ψήφων μέσω τηλεφώνων, ιδιωτικών δικτύων υπολογιστών ή του Διαδικτύου.

Γενικά, μπορούν να προσδιοριστούν δύο βασικοί τύποι ηλεκτρονικής ψηφοφορίας:

- ηλεκτρονική ψηφοφορία η οποία εποπτεύεται με φυσική παρουσία από εκπροσώπους κυβερνητικών ή ανεξάρτητων εκλογικών αρχών (π.χ. ηλεκτρονικά μηχανήματα ψηφοφορίας που βρίσκονται σε εκλογικά κέντρα)

- απομακρυσμένη ηλεκτρονική ψηφοφορία μέσω του Διαδικτύου (ονομάζεται i-voting) όπου ο ψηφοφόρος υποβάλλει την ψήφο του ηλεκτρονικά στις εκλογικές αρχές, από οποιαδήποτε τοποθεσία.

Έχει αποδειχθεί ότι καθώς τα συστήματα ψηφοφορίας γίνονται πιο περίπλοκα και περιλαμβάνουν λογισμικό, πάντα θα υπάρχουν δυνατές διαφορετικές μέθοδοι εκλογικής απάτης. Ορισμένοι αμφισβητούν τη χρήση ηλεκτρονικής ψηφοφορίας από θεωρητική άποψη, υποστηρίζοντας ότι οι άνθρωποι δεν μπορούν να επαληθεύσουν τις λειτουργίες που συμβαίνουν σε μια ηλεκτρονική μηχανή οπότε δεν μπορούν να το εμπιστευτούν. Επιπλέον, ορισμένοι εμπειρογνώμονες υπολογιστών έχουν υποστηρίξει ότι οι άνθρωποι δεν μπορούν να εμπιστευτούν οποιονδήποτε προγραμματισμό δεν έχουν συντάξει.

Η χρήση της ηλεκτρονικής ψηφοφορίας στις εκλογές παραμένει αμφιλεγόμενο ζήτημα. Ορισμένες χώρες όπως η Ολλανδία και η Γερμανία έχουν σταματήσει να τη χρησιμοποιούν αφού αποδείχθηκε ότι είναι αναξιόπιστη, ενώ η Ινδική εκλογική επιτροπή το προτείνει. Η συμμετοχή πολλών ενδιαφερομένων, συμπεριλαμβανομένων των εταιρειών που κατασκευάζουν αυτά τα μηχανήματα, καθώς και των πολιτικών κομμάτων που κερδίζουν από την απάτη το περιπλέκει περαιτέρω.

Πολλές ανασφάλειες έχουν βρεθεί σε εμπορικά μηχανήματα ψηφοφορίας, όπως η χρήση ενός προεπιλεγμένου κωδικού πρόσβασης διαχείρισης. Έχουν επίσης αναφερθεί περιπτώσεις για μηχανήματα που κάνουν απρόβλεπτα λάθη. Βασικά ζητήματα με την ηλεκτρονική ψηφοφορία είναι επομένως η διαφάνεια ενός συστήματος για δημόσια εξέταση από εξωτερικούς εμπειρογνώμονες, η δημιουργία ενός εγγράψιμου εγγράφου των ψήφων και μια αλυσίδα φύλαξης αρχείων. Ακόμη, υπάρχει ο κίνδυνος τα αποτελέσματα των εμπορικών μηχανών ψηφοφορίας να αλλάξουν από την εταιρεία που παρέχει το μηχάνημα. Δεν υπάρχει καμία εγγύηση ότι τα αποτελέσματα συλλέγονται και αναφέρονται με ακρίβεια.

Στις Ηνωμένες Πολιτείες, η ηλεκτρονική ψηφοφορία, ιδίως η DRE, θα μπορούσε να διευκολύνει την εκλογική απάτη και να μην είναι πλήρως ελεγχόμενη. Επιπλέον, η ηλεκτρονική ψηφοφορία έχει επικριθεί ως περιττή και δαπανηρή. Χώρες όπως η Ινδία συνεχίζουν να χρησιμοποιούν ηλεκτρονική ψηφοφορία, αρκετές χώρες έχουν ακυρώσει τα συστήματα ηλεκτρονικής ψηφοφορίας ή έχουν αποφασίσει κατά της ευρείας κλίμακας διάθεσης, ιδίως των Κάτω Χωρών, της Ιρλανδίας, της Γερμανίας και του Ηνωμένου Βασιλείου λόγω ζητημάτων αξιοπιστίας των EVM.

Επιπλέον, άτομα χωρίς πρόσβαση στο Διαδίκτυο ή χωρίς δεξιότητες χρήσης του εξαιρούνται από την διαδικασία. Το λεγόμενο ψηφιακό χάσμα περιγράφει το χάσμα μεταξύ εκείνων που έχουν πρόσβαση στο Διαδίκτυο και εκείνων που δεν το έχουν. Ανάλογα με τη χώρα ή ακόμη και τις περιφέρειες μιας χώρας, το χάσμα διαφέρει. Αυτή η ανησυχία αναμένεται να γίνει λιγότερο σημαντική στο μέλλον, καθώς ο αριθμός των χρηστών του Διαδικτύου τείνει να αυξάνεται.

Το κύριο ψυχολογικό ζήτημα είναι η εμπιστοσύνη. Οι ψηφοφόροι φοβούνται ότι η ψήφος τους θα μπορούσε να αλλάξει από έναν ιό στον υπολογιστή τους ή κατά τη μετάδοση σε κυβερνητικούς διακομιστές.

2.2 Τύποι Ηλεκτρονικής Ψηφοφορίας

Τα ηλεκτρονικά συστήματα ψηφοφορίας για τα εκλογικά σώματα χρησιμοποιούνται από τη δεκαετία του 1960 όταν ξεκίνησε το ντεμπούτο των συστημάτων καρτών. Η πρώτη διαδεδομένη χρήση τους ήταν στις ΗΠΑ όπου 7 κομητείες άλλαξαν σε αυτήν τη μέθοδο για τις προεδρικές εκλογές του 1964. Τα νεότερα οπτικά συστήματα σάρωσης επιτρέπουν σε έναν υπολογιστή να μετρά το σήμα ενός ψηφοφόρου σε μια ψηφοφορία. Οι μηχανές ψηφοφορίας DRE που συλλέγουν και συγκεντρώνουν ψήφους σε ένα μόνο μηχάνημα, χρησιμοποιούνται από όλους τους ψηφοφόρους σε όλες τις εκλογές στη Βραζιλία και την Ινδία, καθώς και σε μεγάλη κλίμακα στη Βενεζουέλα και τις Ηνωμένες Πολιτείες.[1]

Τα συστήματα ψηφοφορίας μέσω Διαδικτύου έχουν κερδίσει δημοτικότητα και έχουν χρησιμοποιηθεί για κυβερνητικές εκλογές και δημοψηφίσματα στην Εσθονία και την Ελβετία, καθώς και για δημοτικές εκλογές στον Καναδά και για κομματικές εκλογές στις Ηνωμένες Πολιτείες και τη Γαλλία. Η ψηφοφορία μέσω Διαδικτύου έχει επίσης χρησιμοποιηθεί ευρέως σε διαδικασίες συμμετοχικής κατάρτισης προϋπολογισμού σε εθνικό επίπεδο, συμπεριλαμβανομένης της Βραζιλίας, της Γαλλίας, των Ηνωμένων Πολιτειών, της Πορτογαλίας και της Ισπανίας. [2] [3]

Υπάρχουν επίσης υβριδικά συστήματα που περιλαμβάνουν μια ηλεκτρονική συσκευή σήμανσης ψηφοφορίας (συνήθως ένα σύστημα οθόνης αφής παρόμοιο με ένα DRE) ή άλλη βοηθητική τεχνολογία για την εκτύπωση ενός ίχνους ελέγχου εγγράφου επαληθευμένου ψηφοφόρου και, στη συνέχεια, χρησιμοποιήστε ένα ξεχωριστό μηχάνημα για ηλεκτρονικό πίνακα.[4]

Υπάρχουν οι βασικοί τύποι:

- Ηλεκτρονικό σύστημα ψηφοφορίας με βάση το χαρτί
- Ηλεκτρονικό σύστημα ψηφοφορίας απευθείας καταγραφής (DRE)
- Σύστημα ψηφοφορίας δημόσιου δικτύου DRE
- Διαδικτυακή ψηφοφορία

Ηλεκτρονικό σύστημα ψηφοφορίας με βάση το χαρτί

Τα συστήματα ψηφοφορίας που βασίζονται σε χαρτί προέρχονται από ένα σύστημα όπου οι ψήφοι ψηφίζονται και υπολογίζονται με το χέρι, χρησιμοποιώντας χαρτί. Με την έλευση του ηλεκτρονικού λογισμικού δημιουργήθηκαν συστήματα όπου οι χάρτινες κάρτες ή τα φύλλα θα μπορούσαν να σημειωθούν με το χέρι, αλλά να μετρήθηκαν ηλεκτρονικά. Αυτά τα συστήματα περιλάμβαναν ψηφοφορία με κάρτες με διατρητική μηχανή, μετέπειτα ψηφιακά συστήματα ψηφοφορίας με στυλό.

Αυτά τα συστήματα μπορεί να περιλαμβάνουν συσκευή σήμανσης ή ηλεκτρονικό δείκτη ψηφοφορίας που επιτρέπει στους ψηφοφόρους να κάνουν τις επιλογές τους χρησιμοποιώντας μια ηλεκτρονική συσκευή εισόδου, συνήθως ένα σύστημα οθόνης αφής παρόμοιο με ένα DRE.

Ηλεκτρονικό σύστημα ψηφοφορίας απευθείας καταγραφής (DRE)

Είναι ένα ηλεκτρονικό μηχάνημα ψηφοφορίας απευθείας καταγραφής (μηχανή ψηφοφορίας DRE) που καταγράφει ψήφους μέσω μίας οθόνης ψηφοφορίας που διαθέτει μηχανικά ή ηλεκτροοπτικά εξαρτήματα που μπορούν να ενεργοποιηθούν από τον ψηφοφόρο (συνήθως κουμπιά ή οθόνη αφής). Επεξεργάζεται τα δεδομένα μέσω ενός προγράμματος υπολογιστή και καταγράφει τα δεδομένα ψηφοφορίας και εικόνες ψηφοφορίας στη μνήμη. Μετά τις εκλογές παράγει έναν πίνακα των δεδομένων ψηφοφορίας που είναι αποθηκευμένα σε αφαιρούμενη μνήμη (για πχ sdcard) και σε έντυπο αντίγραφο. Το σύστημα μπορεί επίσης να παρέχει ένα μέσο για τη μετάδοση μεμονωμένων ψηφοφοριών ή συνόλων ψήφων σε μια κεντρική τοποθεσία για ενοποίηση και αναφορά αποτελεσμάτων από περιφέρειες στην κεντρική τοποθεσία. Η συσκευή άρχισε να χρησιμοποιείται μαζικά το 1996, στη Βραζιλία, όπου το 100% του εκλογικού συστήματος διεξάγεται με μηχανήματα. Τα προβλήματα που αναφέρθηκαν είναι η καθυστέρηση κατά τη ψήφο και προγραμματιστικά λάθη στις εκλογές των ΗΠΑ που δεν υπολόγιζε σωστά τον αριθμό των ψηφοφόρων.

Σύστημα ψηφοφορίας δημόσιου δικτύου DRE

Ένα δημόσιο δίκτυο DRE σύστημα ψηφοφορίας είναι ένα εκλογικό σύστημα που χρησιμοποιεί ηλεκτρονικά ψηφοδέλτια και μεταδίδει δεδομένα ψηφοφορίας από το μέρος ψηφοφορίας σε άλλη τοποθεσία μέσω δημόσιου δικτύου. Τα δεδομένα της ψηφοφορίας μπορούν να διαβιβάζονται ως μεμονωμένα ψηφοδέλτια καθώς εκδίδονται, περιοδικά ως παρτίδες ψηφοφορίας καθ 'όλη την ημέρα των εκλογών, ή ως μία παρτίδα στο τέλος της ψηφοφορίας. Αυτό περιλαμβάνει ψηφοφορία μέσω Διαδικτύου καθώς και τηλεφωνική ψηφοφορία. Το σύστημα ψηφοφορίας DRE δημόσιου δικτύου μπορεί να χρησιμοποιεί είτε τη μέθοδο μέτρησης είτε τον κεντρικό υπολογισμό. Η μέθοδος της κεντρικής μέτρησης συγκεντρώνει ψηφοδέλτια από πολλούς χώρους σε μια κεντρική τοποθεσία. Η

ψηφοφορία μέσω Διαδικτύου μπορεί να χρησιμοποιεί απομακρυσμένες τοποθεσίες (ψηφοφορία από οποιονδήποτε υπολογιστή με δυνατότητα Internet) ή μπορεί να χρησιμοποιεί παραδοσιακές τοποθεσίες ψηφοφορίας με θαλάμους ψηφοφορίας που αποτελούνται από συστήματα ψηφοφορίας συνδεδεμένα στο Διαδίκτυο.

Διαδικτυακή ψηφοφορία

Οι εμπειρογνώμονες στον τομέα της ασφάλειας έχουν βρει προβλήματα ασφάλειας σε κάθε προσπάθεια ψηφοφορίας στο διαδίκτυο, συμπεριλαμβανομένων συστημάτων στην Αυστραλία, Εσθονία, Ελβετία, Ρωσία, και Ηνωμένες Πολιτείες. [3] Έχει υποστηριχθεί ότι τα πολιτικά κόμματα που έχουν περισσότερη στήριξη από ψηφοφόρους που δεν είναι εξοικειωμένοι με το Διαδίκτυο ενδέχεται να χάσουν στις εκλογές λόγω της ηλεκτρονικής ψηφοφορίας, η οποία τείνει να έχει περισσότερους ψηφοφόρους στην ανώτερη / μεσαία τάξη.

Δεν είναι βέβαιο εάν η μείωση του ψηφιακού χάσματος θα προωθούσε τις ίσες ευκαιρίες ψήφου για άτομα σε διάφορα κοινωνικά, οικονομικά και εθνικά περιβάλλοντα. Μάλλον αυτό εξαρτάται όχι μόνο από την προσβασιμότητα στο Διαδίκτυο, αλλά επίσης εξαρτάται από το επίπεδο εξοικείωσης των ανθρώπων με το Διαδίκτυο. [3]

Οι επιπτώσεις της ψηφοφορίας μέσω Διαδικτύου στη συνολική προσέλευση των ψηφοφόρων είναι ασαφείς. Μια μελέτη του 2017 για ψηφοφορία στο διαδίκτυο σε δύο ελβετικές ψηφοφορίες διαπίστωσε ότι δεν είχε καμία επίδραση στην προσέλευση και μια μελέτη του 2009 για τις εθνικές εκλογές της Εσθονίας βρήκε παρόμοια αποτελέσματα. [5]

Αντιθέτως, ωστόσο, η εισαγωγή διαδικτυακής ψηφοφορίας στις δημοτικές εκλογές στην επαρχία του Οντάριο του Καναδά είχε ως αποτέλεσμα μια μέση αύξηση της προσέλευσης περίπου 3,5 ποσοστιαίες μονάδες. [6]

Παγκοσμίως υπάρχουν αρκετά συστήματα για ηλεκτρονική ψηφοφορία. Μερικά από αυτά είναι το InfoPoll Software [7] όπου οι χρήστες μπορούν να σχεδιάζουν HTML φόρμες για να δημιουργήσουν ψηφοφορίες ή ερωτηματολόγια και τα συστήματα TrueBallot[8] και Truevote[9] με πολλές υπηρεσίες και οργάνωση online ψηφοφορίας με πληρωμή.

Στην Ελλάδα το σύστημα online ψηφοφορίας που χρησιμοποιείται σε μεγαλύτερο ποσοστό και υιοθετήθηκε να χρησιμοποιείται για τις εκλογικές διαδικασίες στα Ελληνικά Πανεπιστήμια είναι το Σύστημα ZEYΣ [10]. Είναι ένα πληροφοριακό σύστημα που χρησιμοποιεί το Διαδίκτυο για την διεξαγωγή

οποιασδήποτε ψηφοφορίας. Οι ψηφοφόροι μπορούν να ψηφίζουν με άκρως μυστικότητα χωρίς να υπάρχει ο κίνδυνος διαρροής προσωπικών ψήφων. Ο ψηφοφόρος δέχεται ηλεκτρονικά μήνυμα με την ημερομηνία και την ώρα έναρξης και λήξης της ψηφοφορίας. Επίσης, κωδικούς κρυπτογράφησης/αποκρυπτογράφησης έχουν μόνο τα μέλη της εφορευτικής επιτροπής, ώστε οι διαχειριστές του συστήματος να μην μπορούν να αποκρυπτογραφήσουν τα ψηφοδέλτια.

2.3 Νομικά ζητήματα που εγείρει η χρήση ηλεκτρονικών μεθόδων ψηφοφορίας

Εφαρμογή στις ΗΠΑ

Οι ΗΠΑ χρησιμοποιούν τη διαδικασία ηλεκτρονικής ψηφοφορίας για πολλά χρόνια στις πολιτικές εκλογές τους. Τα μηχανήματά τους λειτουργούν με το σύστημα DRE, που σημαίνει ότι καταγράφουν την ψήφο στη μνήμη τους, αλλά χωρίς να εκδίδουν έγγραφο που να το αποδεικνύει. Έτσι, όσο η ψηφοφορία είναι μυστική και δεν καταγράφεται, κανείς δεν μπορεί μετρήσει τα ψηφοδέλτια και να επιβεβαιώσει το αποτέλεσμα και εκτός από αυτό που έχει καταγράφεται, είτε είναι σωστό είτε λάθος, και αυτό θεωρείται οριστικό. Το πρόβλημα με αυτές τις μηχανές ήταν ένα πλήγμα στις εκλογές του 2000, όπου ξέσπασε σκάνδαλο που αποκάλυψε την απάτη με τα ηλεκτρονικά μηχανήματα. Στις Προεδρικές εκλογές 2000 με υποψηφίους τον Τζορτζ Μπους και Αλ Γκορ η καταμέτρηση των ψήφων στην πολιτεία της Φλόριντα η τελική διαφορά ψήφων ήταν 537 ψήφοι για τον Τζορτζ Μπους, ενώ ο Αλ Γκορ έλαβε 0,5% περισσότερες ψήφους ΗΠΑ. Για το λόγο αυτό, το ζήτημα έχει λάβει περαιτέρω διαστάσεις. Έτσι στις κομητείες της Volusia, PalmBeach, Maimi-Dade, Broward, όπου σύμφωνα με τον εκλογικό νόμο του κράτους χρησιμοποιήθηκε ένα άλλο σύστημα της απλής ψηφοφορίας όπου αναφέρονται τα ονόματα των υποψηφίων και κάθε ψηφοφόρος δηλώνει την προτίμησή του με διάτρηση της ψήφου με ένα στυλό σε ένα συγκεκριμένο σημείο. [3]

Μπορεί να εφαρμόστηκε αλλά αποδείχθηκε ότι το αποτέλεσμα ήταν και πάλι το ίδιο και ο Al Gore ζήτησε καταμέτρηση ψήφων με το χέρι.

Και ενώ το δικαστήριο στην Πολιτεία της Φλόριντα διέταξε την δια χειρός επανακαταμέτρηση, ο George Bush έκανε έφεση με αποτέλεσμα η υπόθεση να πάει στο Ανώτατο Δικαστήριο των ΗΠΑ.

Η απόφαση του δικαστηρίου ήταν ότι η επανακαταμέτρηση με το χέρι των ψηφοδελτίων ήταν αντίθετο με το Σύνταγμα των ΗΠΑ, επειδή δεν πραγματοποιούνταν ενιαία σε όλες τις κομητείες, αφού δεν είχε οριστεί.

2.4 Ηλεκτρονικές Ψηφοφορίες ZEYΣ

Η Ψηφιακή Κάλπη ZEYΣ [10] είναι ένα πληροφοριακό σύστημα, για τη διεξαγωγή της διαδικασίας των εκλογών παντός τύπου, με ψηφιακό τρόπο. Η προετοιμασία της ψηφοφορίας από τη διεξάγουσα

αρχή, και η υποβολή της ψήφου από τους ψηφοφόρους, γίνονται απομακρυσμένα μέσω του Διαδικτύου.

Zeus Demo

Γνωρίστε το Zeus. Εισάγετε διεύθυνση email για να σας σταλούν τα στοιχεία ενός δοκιμαστικού λογαριασμού.

Διεύθυνση email:

Δημιουργία δοκιμαστικού λογαριασμού

Σχήμα 2.1: Ηλεκτρονική Ψηφοφορία ZEYS

Όπως αναφέρει η εταιρεία που το υλοποίησε [10]: *Η Ψηφιακή Κάλπη ZEYS μπορεί να αξιοποιηθεί από κάθε ενδιαφερόμενο που επιθυμεί να διοργανώσει εκλογές παντός τύπου.*

Η επικοινωνία των αρχών και των ψηφοφόρων με το πληροφοριακό σύστημα ZEYS γίνεται μέσω ενός απλού web browser, ενώ προστατεύεται όπως ακριβώς και οι ηλεκτρονικές οικονομικές συναλλαγές. Η ακεραιότητα της ψηφοφορίας είναι μαθηματικά επαληθεύσιμη από τον καθένα μέσω της χρήσης κρυπτογραφίας, και χωρίς καμία προσβολή του απόρρητου. Υποστηρίζονται πολλαπλά είδη ψηφοδελτίων και εκλογικών συστημάτων, όπως ερωτήσεις πολλαπλών επιλογών, ψηφοφορίες με διαφορετικό ψηφοδέλτιο ανά συνδυασμό, και ψηφοδέλτια για ταξινομική ψήφο (STV).

Η «Ψηφιακή Κάλπη Zeus» είναι ένα πληροφοριακό σύστημα για την αδιάβλητη διεξαγωγή απόρρητων ψηφοφοριών με αμιγώς ηλεκτρονικό τρόπο. Τόσο η προετοιμασία της ψηφοφορίας από τη διεξάγουσα αρχή, όσο και η υποβολή της ψήφου από τους ψηφοφόρους, γίνονται απομακρυσμένα μέσω Διαδικτύου.

Ψηφοφορίες **Δημιουργία ψηφοφορίας**

Για τη δημιουργία νέας ψηφοφορίας, εισάγετε τα απαραίτητα στοιχεία παρακάτω.

Δοκιμαστική ψηφοφορία
Επιλέξτε το πεδίο αν πρόκειται για δοκιμαστική ψηφοφορία

Τύπος ψηφοφορίας
Επιλέξτε τον τύπο της ψηφοφορίας

Απλή ψηφοφορία με μία ή περισσότερες ερωτήσεις

Τίτλος ψηφοφορίας
Τίτλος ψηφοφορίας

Περιγραφή ψηφοφορίας
Περιγραφή ψηφοφορίας

Σχήμα 2.2: Απαραίτητα πεδία για τη δημιουργία νέας ψηφοφορίας 1 - Zeus

Οποιοσδήποτε χρήστης μπορεί να δημιουργήσει μια δοκιμαστική ψηφοφορία.

Πρέπει να εισάγει τα απαραίτητα στοιχεία που φαίνονται στα Σχήματα 2.2 και 2.3.

Στην συνέχεια πρέπει να δημιουργήσει κάλπη και να ορίσει εφορευτική επιτροπή.

Η διαδικασία περιγράφεται στην ιστοσελίδα της Zeus και παρακάτω αναφέρεται ένα μικρό κομμάτι αυτούσιο.

Έναρξη της ψηφοφορίας

Συμπληρώστε την ημερομηνία και ώρα έναρξης της ψηφοφορίας

Λήξη της ψηφοφορίας

Συμπληρώστε την ημερομηνία και ώρα λήξης της ψηφοφορίας

Εφορευτική επιτροπή

Συμπληρώστε τη λίστα μελών της εφορευτικής επιτροπής με τα e-mails τους. Π.χ.

Κωσταντίνος Κωστόπουλος, kwstopoulos@email.com

Ιωάννης Γιαννόπουλος, giannhs@gmail.com

Email υποστήριξης

Οι ψηφοφόροι μπορούν να απευθύνονται σε αυτό το e-mail για υποστήριξη σε θέματα της ψηφοφορίας

Τηλέφωνο υποστήριξης

Οι ψηφοφόροι θα μπορούν να επικοινωνούν σε αυτό το τηλέφωνο για υποστήριξη σε θέματα της ψηφοφορίας

Γλώσσα επικοινωνίας

Επιλέξτε τη γλώσσα που θα χρησιμοποιηθεί για τα μηνύματα των email

Όροι κατάθεσης ψήφου

Οι ψηφοφόροι θα πρέπει να αποδεχθούν το παρακάτω κείμενο προκειμένου να μπορέσουν να καταθέσουν την ψήφο τους.

Σχήμα 2.3: Απαραίτητα πεδία για τη δημιουργία νέας ψηφοφορίας 2 - Zeus

Η διαδικασία ψηφοφορίας, επιγραμματικά:

Η διεξάγουσα αρχή συντάσσει τα ψηφοδέλτια και τη λίστα των ψηφοφόρων και ορίζει την εφορευτική επιτροπή. Η λίστα των ψηφοφόρων αποτελείται από τα ονοματεπώνυμά τους και την ηλεκτρονική τους διεύθυνση.

Οι ψηφοφόροι λαμβάνουν στην ηλεκτρονική τους διεύθυνση μήνυμα με το οποίο καλούνται να ψηφίσουν. Το μήνυμα περιέχει σύνδεσμο (link) που οδηγεί στο ψηφιακό παραπέτασμα μέσα στο οποίο

προετοιμάζεται η ψήφος. Το παραπέτασμα θα ενεργοποιηθεί όταν η εφορευτική επιτροπή εκκινήσει την ψηφοφορία.

Η εφορευτική επιτροπή εκκινεί και στο τέλος λήγει την ψηφοφορία.

Οι ψηφοφόροι ψηφίζουν εντός του ορισμένου χρονικού διαστήματος, και λαμβάνουν ψηφιακή απόδειξη της συμμετοχής τους.

Με το πέρας της ψηφοφορίας, η εφορευτική επιτροπή δίνει την εντολή για την αυτόματη κατάμετρηση των ψηφοδελτίων.

Το απόρρητο της ψήφου είναι ευθύνη της εφορευτικής επιτροπής, και είναι πρακτικά εξασφαλισμένο καθώς αρκεί να υπάρχει ένα και μόνο τίμιο μέλος στην επιτροπή.

Ο Ψηφοφόρος

Ο ψηφοφόρος λαμβάνει μήνυμα στο ηλεκτρονικό του ταχυδρομείο όταν η ψηφοφορία είναι έτοιμη να αρχίσει. Το μήνυμα τον πληροφορεί για την ακριβή ημερομηνία και ώρα έναρξης και λήξης της ψηφοφορίας. Για κάθε αλλαγή που γίνεται λαμβάνει και νέο μήνυμα.

Στο μήνυμα περιέχεται ένας προσωπικός και απόρρητος σύνδεσμος στον ιστότοπο του συστήματος «Ζευς». Η διαδικασία υποβολής της ψήφου ξεκινά ακολουθώντας το σύνδεσμο αυτό, εφόσον βέβαια η ψηφοφορία βρίσκεται ήδη σε εξέλιξη. Διαφορετικά ο ψηφοφόρος ενημερώνεται αναλόγως.

Στην οθόνη του ψηφοφόρου εμφανίζεται ένα εισαγωγικό σημείωμα που περιγράφει τη διαδικασία υποβολής ψήφου. Η διαδικασία αποτελείται από δύο βήματα, την επιλογή των υποψηφίων στο ψηφοδέλτιο, και την υποβολή του ψηφοδελτίου.

Στο βήμα της επιλογής, εμφανίζεται στην οθόνη μια αναπαράσταση ενός ψηφοδελτίου, καθώς και οι απαραίτητες πληροφορίες και οδηγίες. Ο ψηφοφόρος συνθέτει διαδραστικά το ψηφοδέλτιο της επιλογής του.

Όταν ολοκληρώσει τη διαδικασία της επιλογής, ο ψηφοφόρος προχωρά στην υποβολή του ψηφοδελτίου. Το επιλεγμένο ψηφοδέλτιο κρυπτογραφείται στον τοπικό υπολογιστή του ψηφοφόρου και στη συνέχεια υποβάλλεται μέσω δικτύου στο σύστημα «Ζευς». Το σύστημα εκδίδει ψηφιακή απόδειξη καταχώρισης της ψήφου σε μορφή απλού αρχείου κειμένου, την οποία ο ψηφοφόρος οφείλει να φυλάξει, καθώς είναι απαραίτητη για την υποβολή και επεξεργασία τυχόν ενστάσεων.

Η Εφορευτική Επιτροπή

Τα μέλη της εφορευτικής επιτροπής στο σύστημα «Ζευς» είναι οι κλειδοκράτορες της ψηφοφορίας. Τα μέλη της επιτροπής λαμβάνουν ειδικά κρυπτογραφικά κλειδιά, τους Κωδικούς Ψηφοφορίας. Οι κωδικοί αυτοί είναι όλοι απαραίτητοι για τη διεξαγωγή της ψηφοφορίας καθώς και για την αποκρυπτογράφηση των αποτελεσμάτων. Εάν χαθεί έστω και ένας, η ψηφοφορία δε θα μπορέσει να ολοκληρωθεί, καθώς θα είναι αδύνατη η αποκρυπτογράφηση των ψηφοδελτίων. Κάθε μέλος της εφορευτικής επιτροπής είναι υπεύθυνο για τη διαφύλαξη του δικού του Κωδικού, ενώ το σύστημα «Ζευς» έχει και αυτό ένα Κωδικό για κάθε ψηφοφορία, σαν να ήταν μέλος της επιτροπής.

Η πρώτη πράξη του κάθε μέλους της επιτροπής είναι να εισέλθει στον ιστότοπο της ψηφοφορίας, να παράξει έναν καινούριο Κωδικό Ψηφοφορίας, και στη συνέχεια να καταθέσει το δημόσιο τμήμα του στο σύστημα «Ζευς». Η ψηφοφορία μπορεί να αρχίσει μόνο όταν όλα τα μέλη της επιτροπής έχουν εκτελέσει και επιβεβαιώσει αυτό το βήμα.

Μετά το πέρας της ψηφοφορίας η αποκρυπτογράφηση των ψηφοδελτίων είναι αδύνατη χωρίς όλους τους Κωδικούς Ψηφοφορίας. Κάθε μέλος της εφορευτικής επιτροπής συνδέεται με το σύστημα «Ζευς» για να παρέχει τα κρυπτογραφικά δεδομένα που είναι απαραίτητα για την εξαγωγή των περιεχομένων των ψηφοδελτίων. Η παροχή των κρυπτογραφικών δεδομένων δεν προσβάλλει το απόρρητο της ψηφοφορίας.

2.5 Πλεονεκτήματα-Μειονεκτήματα ηλεκτρονικής ψηφοφορίας

Μερικά από τα πλεονεκτήματα της ηλεκτρονικής ψηφοφορίας είναι τα παρακάτω:

Με την ηλεκτρονική ψηφοφορία έχουμε το πλεονέκτημα της εξοικονόμησης χρόνου. Οι μηχανές σήμερα είναι αρκετά τεχνολογικά προηγμένες και αυτοματοποιημένες, γεγονός που βοηθά στην ταχύτερη και ακριβέστερη μέτρηση των ψήφων, καθώς η συμβολή του ανθρώπινου παράγοντα δεν είναι απαραίτητη.

Η ηλεκτρονική ψηφοφορία συμβάλλει στην εξοικονόμηση χρημάτων. Όσον αφορά τις κυβερνητικές δαπάνες είναι το ανθρώπινο δυναμικό που θα χρειαστεί για την παρακολούθηση των εκλογών, το μέρος που θα χρειαστεί για τη διεξαγωγή των εκλογών και το ποσό χαρτιού που θα χρησιμοποιηθεί για την παραγωγή των ψηφοφόρων. Για τον ίδιο τον ψηφοφόρο, το κόστος ταξιδιού θα αποφευχθεί ώστε να μπορεί να παρευρεθεί στον τόπο όπου πρέπει να ψηφίσει.

Από τα πιο σημαντικά είναι ότι θα υπάρξει κινητοποίηση των πολιτών. Το ποσοστό της αποχής από τις εκλογές αυξάνεται λόγω απόστασης και συνωστισμού. Ιδίως σε εποχές μιας πανδημίας ή κάτι παρόμοιο οι πολίτες μπορούν να ψηφίσουν από το σπίτι τους χωρίς να έρθουν σε επαφή με άλλους ανθρώπους.

Μειονεκτήματα:

Η μυστικότητα της ψήφου αποτελεί βασικό θέμα για κάθε ψηφοφορία και για αυτό πρέπει να διασφαλίζεται. Λόγω της φύσης της διαδικασίας ο ψηφοφόρος πρέπει να εισάγει τα προσωπικά του στοιχεία μαζί με την ψήφο του με αποτέλεσμα οι διαχειριστές να έχουν τη δυνατότητα να δουν η κάθε ψήφος από ποιον έχει προέλθει και αυτό ίσως να επηρεάσει το αποτέλεσμα.

Το διαδίκτυο και τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις από μη εξουσιοδοτημένα άτομα, τα οποία επεμβαίνουν στα συστήματα με αποτέλεσμα να τίθεται το θέμα της ακεραιότητας της ψήφου.

Η καταμέτρηση των ψήφων απαιτεί τη συμβολή του ανθρώπινου παράγοντα. Το άτομο που αναλαμβάνει να εκτελέσει αυτή τη διαδικασία είναι άγνωστο και έτσι υπάρχει η πιθανότητα παρεμβολής στο αποτέλεσμα.

Σε μια ψηφοφορία καλούνται να ψηφίσουν όλα τα άτομα (πχ άνω των 18 ετών) μιας χώρας και είναι ένα συνταγματικά κατοχυρωμένο δικαίωμα. Τα μεγαλύτερα σε ηλικία άτομα όμως δεν έχουν την ίδια γνώση και την ίδια οικειότητα με την τεχνολογία όπως τα νεαρότερα. Αυτό συνεπάγεται κοινωνικός αποκλεισμός μερικών ατόμων από τη διαδικασία κάτι που επηρεάζει πολύ το αποτέλεσμα των εκλογών αφού δεν είναι σε θέση να ψηφίζουν όλοι. Αυτό παραβιάζει το άρθρο 51 παρ. 5 του Συντάγματος για την υποχρεωτική άσκηση του εκλογικού δικαιώματος.

Κεφάλαιο 3ο: Τεχνολογία και εργαλεία

Στο κεφάλαιο αυτό θα περιγράψει η τεχνολογία που χρησιμοποιήθηκε για την υλοποίηση της ηλεκτρονικής ψηφοφορίας.

3.1 PHP

Η PHP - Hypertext PreProcessor [11], είναι μια script γλώσσα συγγραφής που εμφανίζεται στην ιστοσελίδα HTML και εκτελείται σε scripting από διακομιστή. Ο ανταγωνισμός με την PHP είναι οποιαδήποτε script γλώσσα: Microsoft ASP (Active Server Pages) και Sun's JSP (JavaServer Pages).

Το μεγαλύτερο μέρος της σύνταξής της, η PHP το έχει πάρει από την C, την Java και την Perl και διαθέτει και μερικά δικά της μοναδικά χαρακτηριστικά. Ο σκοπός της γλώσσας είναι να δώσει τη δυνατότητα στους προγραμματιστές να δημιουργούν δυναμικές ιστοσελίδες.



Σχήμα 3.1: PHP 7

Ο κώδικας PHP επεξεργάζεται συνήθως σε έναν διακομιστή Ιστού από έναν διερμηνέα PHP που υλοποιείται ως λειτουργική μονάδα, δαίμονας ή ως εκτελέσιμο Common Gateway Interface (CGI). Σε έναν διακομιστή ιστού, το αποτέλεσμα του ερμηνευμένου και εκτελεσμένου κώδικα PHP - που μπορεί να είναι οποιοσδήποτε τύπος δεδομένων, όπως δημιουργημένο HTML ή δυαδικά δεδομένα εικόνας - θα αποτελούσε το σύνολο ή μέρος μιας απόκρισης HTTP. Υπάρχουν διάφορα συστήματα προτύπων ιστού, συστήματα διαχείρισης περιεχομένου Ιστού και πλαίσια ιστού τα οποία μπορούν να

χρησιμοποιηθούν για διευκόλυνση της δημιουργίας αυτής της απόκρισης. Επιπλέον, το PHP μπορεί να χρησιμοποιηθεί για πολλές εργασίες προγραμματισμού εκτός του περιβάλλοντος ιστού, όπως αυτόνομες γραφικές εφαρμογές και ρομποτικός έλεγχος drone. Ο αυθαίρετος κωδικός PHP μπορεί επίσης να ερμηνευτεί και να εκτελεστεί μέσω διεπαφής γραμμής εντολών (CLI).

Ο τυπικός διερμηνέας PHP, που τροφοδοτείται από το Zend Engine,[12] είναι ελεύθερο λογισμικό που κυκλοφορεί βάσει της άδειας PHP. Η PHP έχει μεταφερθεί ευρέως και μπορεί να αναπτυχθεί στους περισσότερους διακομιστές ιστού σε σχεδόν κάθε λειτουργικό σύστημα και πλατφόρμα, δωρεάν. Η γλώσσα PHP εξελίχθηκε χωρίς γραπτή επίσημη προδιαγραφή ή πρότυπο έως το 2014, με την αρχική εφαρμογή να λειτουργεί ως το de facto πρότυπο το οποίο άλλες εφαρμογές στόχευαν να ακολουθήσουν. Από το 2014, οι εργασίες συνεχίστηκαν για τη δημιουργία μιας επίσημης προδιαγραφής PHP.[13]

Υποστηρίζει τις πιο πολλές βάσεις δεδομένων και από τις πιο σημαντικές είναι MySQL Oracle PostgreSQL. Η PHP παρέχει επίσης υποστήριξη για συνομιλία μ' άλλες υπηρεσίες, χρησιμοποιώντας πρωτόκολλα όπως τα IMAP, SNMP, NNTP, POP3 ή και το HTTP.

Η νεότερη έκδοση της PHP είναι η 7.

Κατά τη διάρκεια του 2014 και του 2015, αναπτύχθηκε μια νέα μεγάλη έκδοση PHP, η οποία αριθμήθηκε PHP 7. Ενώ το πείραμα PHP 6 Unicode δεν είχε κυκλοφορήσει ποτέ, πολλά άρθρα και τίτλοι βιβλίων αναφέρθηκαν στο όνομα PHP 6, το οποίο θα μπορούσε να προκαλέσει σύγχυση εάν μια νέα κυκλοφορία επρόκειτο να επαναχρησιμοποιήσει το όνομα. Μετά από ψηφοφορία, επιλέχθηκε το όνομα PHP 7. Το θεμέλιο του PHP 7 είναι ένας κλάδος PHP που αρχικά ονομάστηκε PHP επόμενης γενιάς (rhnrg). Συντάχθηκε από τους Dmitry Stogov, Xinchun Hui και Nikita Popov, [13] και στόχευε να βελτιστοποιήσει την απόδοση της PHP επαναπροσδιορίζοντας το Zend Engine διατηρώντας παράλληλα σχεδόν ολοκληρωμένη συμβατότητα γλώσσας. Έως τις 14 Ιουλίου 2014, τα σημεία αναφοράς που βασίζονται στο WordPress, το οποίο χρησίμευσε ως η κύρια σουίτα αναφοράς για το έργο rhnrg, παρουσίασαν σχεδόν 100% αύξηση στην απόδοση. Οι αλλαγές από το rhnrg αναμένεται επίσης να κάνουν ευκολότερη τη βελτίωση της απόδοσης στο μέλλον, καθώς οι πιο συμπαγείς δομές δεδομένων και άλλες αλλαγές θεωρούνται ότι ταιριάζουν καλύτερα για μια επιτυχημένη μετάβαση σε έναν μεταγλωττιστή just-in-time (JIT). Λόγω των σημαντικών αλλαγών, ο επανασχεδιασμένος μηχανισμός Zend ονομάζεται Zend Engine 3, αντικαθιστώντας τον Zend Engine 2 που χρησιμοποιείται στο PHP 5. Λόγω των σημαντικών εσωτερικών αλλαγών στο rhnrg, πρέπει να λάβει έναν νέο αριθμό μεγάλης έκδοσης PHP, αντί για μια μικρή έκδοση PHP 5, σύμφωνα με τη διαδικασία κυκλοφορίας της PHP. Συγκεκριμένα, περιελάμβανε τις ακόλουθες αλλαγές: Πολλοί μηχανισμοί σφάλματος PHP παλαιού τύπου ή ανακτήσιμοι επιπέδου αντικαταστάθηκαν με σύγχρονες αντικειμενοστρεφείς εξαιρέσεις. Η σύνταξη για μεταβλητή αποπαραπομπή επεξεργάστηκε ώστε να είναι εσωτερικά πιο συνεπής και πλήρης, επιτρέποντας τη χρήση των τελεστών `->`, `[]`, `()`, `{}` και `::`, με αυθαίρετες σημαντικές

εκφράσεις στην αριστερή πλευρά. Η υποστήριξη για παλαιότερες μεθόδους κατασκευαστή τύπου PHP 4 καταργήθηκε. Η συμπεριφορά της δήλωσης foreach άλλαξε ώστε να είναι πιο προβλέψιμη. Οι κατασκευαστές για τις λίγες τάξεις που είναι ενσωματωμένοι στο PHP που επέστρεψαν μηδέν μετά την αποτυχία άλλαξαν για να ρίξουν μια εξαίρεση αντί για συνέπεια. Αρκετές διεπαφές προγραμματισμού εφαρμογών διακομιστή (SAPIs) που δεν έχουν διατηρηθεί ή καταργηθεί, καταργήθηκαν από τον πυρήνα της PHP, κυρίως την παλιά mysql επέκταση. Η συμπεριφορά του τελεστή list () άλλαξε για να αφαιρέσει υποστήριξη για συμβολοσειρές. Η υποστήριξη καταργήθηκε για τους οριοθέτες τύπου ASP παλαιού τύπου <% and%> και <script language = "php"> ... </script>. Η υποστήριξη για δεκαεξαδικό αριθμό σε ορισμένες μετατροπές από συμβολοσειρές σε τύπους αριθμών καταργήθηκε. Οι χειριστές αριστεράς και δεξιάς αλλαγής άλλαξαν ώστε να συμπεριφέρονται με μεγαλύτερη συνέπεια σε όλες τις πλατφόρμες. Οι μετατροπές μεταξύ αριθμών κυμαινόμενου σημείου και ακέραιων αριθμών (π.χ. το άπειρο άλλαξαν σε μηδέν) και εφαρμόστηκαν με μεγαλύτερη συνέπεια σε όλες τις πλατφόρμες. Το PHP 7 περιλάμβανε επίσης νέες δυνατότητες γλώσσας. Πιο συγκεκριμένα, εισάγει δηλώσεις τύπου επιστροφής για συναρτήσεις που συμπληρώνουν τις υπάρχουσες δηλώσεις τύπων παραμέτρων και υποστήριξη για τους τύπους κλίμακας (ακέραιος, float, string και boolean) σε δηλώσεις παραμέτρων και τύπου επιστροφής.

3.2 MySQL

Η MySQL [14] είναι μία βάση δεδομένων και η πιο δημοφιλής από τα Συστήματα Διαχείρισης Βάσεων Δεδομένων (DBMS). Για να μπορούν τα DBMS να έχουν κάποιους κοινούς άξονες αναφοράς έχει αναπτυχθεί η γλώσσα SQL (Structured Query Language) ή οποία επιτρέπει μέσα από ένα σύστημα εντολών, την προσπέλαση των δομημένων δεδομένων που περιέχει ένα DBMS. Κάθε DBMS ουσιαστικά δέχεται και εκτελεί ένα σετ εντολών SQL για να διαχειριστεί τα δεδομένα του. Η MySQL είναι μία διανομή (έκδοση) της γλώσσας SQL και ένα MySQL DBMS είναι ένα σύστημα που δέχεται εντολές της MySQL.

Η βάση δεδομένων είναι μία συλλογή δεδομένων κατάλληλα αποθηκευμένων σε έναν υπολογιστή προκειμένου να μπορούν να προσπελαστούν, διαχειριστούν και ενημερωθούν από τον χρήστη που τις διαχειρίζεται. Οι ενέργειες αυτές επάνω στα δεδομένα γίνονται μέσα από τα Συστήματα Διαχείρισης Βάσεων Δεδομένων (DataBase Management Systems - DBMS), τα οποία έχουν κατάλληλους μηχανισμούς για να προσπελούν οργανωμένες δομές δεδομένων και να τις επεξεργάζονται.

Η MySQL αποτελεί ελεύθερο. Αντίστοιχα με την MySQL υπάρχουν και άλλα συστήματα δωρεάν ή με πληρωμή. Από τα πιο γνωστά DBMS είναι ο SQL Server της Microsoft, ο Oracle SQL server, η DB2 κ.ά.

Maria Db

Το MariaDB [15] είναι ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων ανοιχτού κώδικα (RDBMS), το οποίο είναι μια εξαιρετικά συμβατή αντικατάσταση της MySQL. Το MariaDB αναπτύχθηκε ως μια διακλάδωση λογισμικού της MySQL το 2009 ως απόκριση στην εξαγορά της MySQL από την Oracle. Η πρόθεση της MariaDB είναι να παραμείνει δωρεάν και λογισμικό ανοιχτού κώδικα βάσει της άδειας GNU General Public License.

3.3 Laravel

Η ανάπτυξη σύνθετων έργων απαιτεί ακρίβεια και την απλούστερη δυνατή προσέγγιση. Οι περισσότερες διαδικτυακές εφαρμογές αναπτύσσονται σε PHP Frameworks. Αυτά τα Πλαίσια προσφέρουν μεγαλύτερη ασφάλεια, ακεραιότητα και φυσικά ευκολία, μειώνοντας έτσι το κόστος ανάπτυξης.



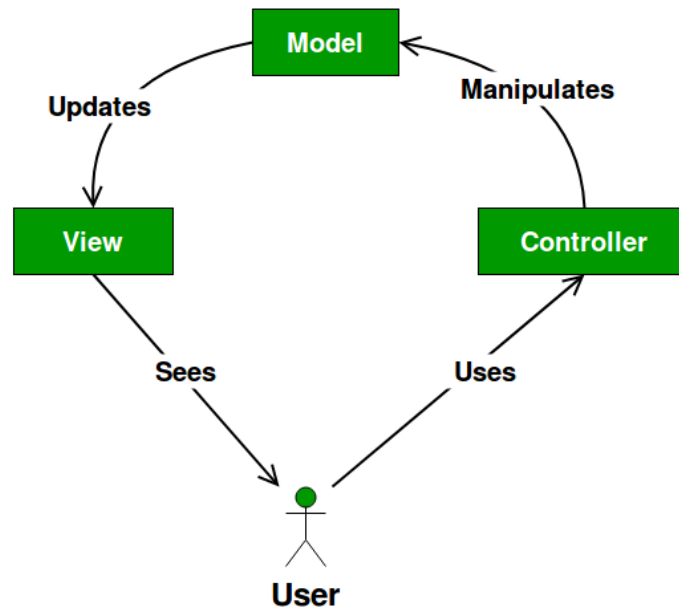
Σχήμα 3.2: Laravel λογότυπο

Το Laravel [16] θεωρείται ένα από τα καλύτερα PHP Framework αυτήν τη στιγμή από την κοινότητα των προγραμματιστών. Παρέχει εγκυρότητα και υπεροχή σε ολόκληρο το έργο, ενώ διευκολύνει την ανάπτυξη με τα ενσωματωμένα εργαλεία προγραμματιστή του, καθώς και την ευκολία εγκατάστασης σε άλλα πλαίσια.

Παρακάτω παρουσιάζονται κύρια πλεονεκτήματα της χρήσης του Laravel.

Αρχιτεκτονική MVC

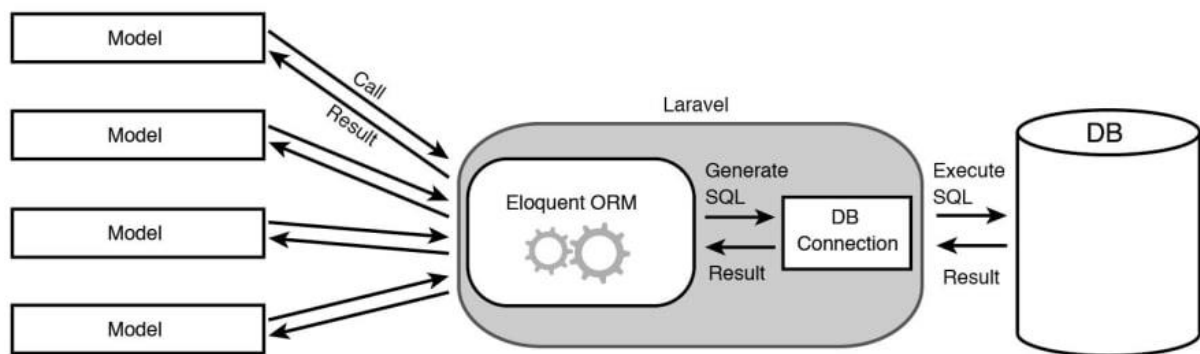
Το Laravel συνεργάζεται με την αρχιτεκτονική MVC[17], δηλαδή Model - View - Controller, το οποίο εξασφαλίζει την καλύτερη διάκριση μεταξύ της λογικής της εφαρμογής και της παρουσίασής της. Επιτρέπει τον διαχωρισμό της διαδικασίας ανάπτυξης και έτσι επιτυγχάνει βελτιωμένη απόδοση σε κάθε τομέα. Έτσι, οι προγραμματιστές μπορούν να γράψουν καλύτερο κώδικα και φυσικά να έχουν μια πιο λεπτομερή τεκμηρίωση του έργου.



Σχήμα 3.3: MVC

Γρήγορο και απλό σύστημα ORM

Η βασική λειτουργία ORM [18] ή Object-Relational Mapping, χρησιμοποιείται για την ανάπτυξη σύνθετων εφαρμογών για ιστοσελίδες. Το Laravel διαθέτει ένα πολύ γρήγορο σύστημα ORM που ονομάζεται Eloquent. Περιλαμβάνει ένα τρόπο, που μας επιτρέπει να γράφουμε σύνθετα ερωτήματα SQL με απλή PHP σύνταξη και ο κάθε πίνακας της βάσης δεδομένων, έχει τα κατάλληλα μοντέλα για την διασύνδεση του με την εφαρμογή.



Σχήμα 3.4: Laravel ORM

Λειτουργίες ασφάλειας

Το Laravel παρέχει μια πολύ καλή ασφάλεια σε όλη τη διαδικασία ανάπτυξης και στο τελικό έργο. Προστατεύει την εφαρμογή από σοβαρές απειλές όπως SQL injections, CSR forgery και cross-site scripting.

Επίσης, το Laravel χρησιμοποιεί hashed και salted passwords οι οποίοι δεν μπορούν να αποθηκευτούν σε plain text στην βάση δεδομένων. Χρησιμοποιεί τον αλγόριθμο Bcrypt hashing που δημιουργεί κρυπτογραφημένα passwords. Τέλος, χρησιμοποιεί SQL statements για να αποτρέψει επιθέσεις.

Artisan Command Line - Γραμμή εντολών

Το Laravel διαθέτει γραμμή εντολών που μέσω αυτής μπορεί κάποιος να διαχειρίζεται το περιβάλλον του έργου. Απλοποιεί τις επαναλαμβανόμενες διαδικασίες και εργασίες που χρειάζεται να γίνουν με χειροκίνητο τρόπο. Το Laravel έχει ένα ενσωματωμένο εργαλείο που ονομάζεται Artisan για τη χρήση του command line και αυτό βοηθά στη δημιουργία του έτοιμων κομματιών κώδικα καθώς και της αρχιτεκτονικής της βάσης δεδομένων μαζί με τα λεγόμενα migrations. Οπότε είναι η ευκολότερη διαχείριση της βάσης δεδομένων. Πολύ συχνά χρησιμοποιείται για την δημιουργία αρχείων όπως controllers.

Εργαλείο Blade

Διαθέτει ένα ενσωματωμένο template εργαλείο που ονομάζεται Blade και βοηθά στην δυναμική παρουσίαση του περιεχομένου της ιστοσελίδας. Τα templates του Laravel φορτώνουν γρήγορα και μπορούν εύκολα να επεκταθούν μέσω μιας πληθώρας εργαλείων και προσθηκών.

Βιβλιοθήκες

Το Laravel έχει ένα πολύ μεγάλο αριθμό βιβλιοθηκών για να μας διευκολύνει σε πολλές διαδικασίες ανάπτυξης. Για παράδειγμα η βιβλιοθήκη για το Authentication παρέχει σημαντικές λειτουργίες όπως προστασία CSRF, Bcrypt, κρυπτογράφηση κωδικών, hashing κλπ.

Σύστημα Packaging

Συνήθως η ανάπτυξη των web εφαρμογών σε Laravel βασίζεται σε λίγες (περίπου 22) βιβλιοθήκες που χρησιμοποιούνται σε διαφορετικά ενότητες και προσθήκες. Αυτό το σύστημα βοηθά στην ανάπτυξη εύκολων και γρήγορων responsive εφαρμογών. Βασίζεται και προσαρμόζεται στις τελευταίες εκδόσεις PHP. Επίσης, υπάρχει η δυνατότητα προσθήκης από χιλιάδες πακέτα για διάφορες χρήσεις.

Micro-Framework Lumen

Μαζί με το Laravel υπάρχει ένα μικρό framework που ονομάζεται Lumen [19]. Αυτό είναι ένας μικρός κλώνος του Laravel με λιγότερες λειτουργίες και εστιάζει σε πολύ γρήγορες εφαρμογές. Το βασικό του χαρακτηριστικό είναι ότι δεν έχει front-end λειτουργίες και χρησιμοποιείται για την δημιουργία γρήγορων APIs.

Σύστημα Migration

Το σύστημα migration στο Laravel διευκολύνει την επέκταση της βάσης δεδομένων χωρίς να χρειάζεται η επαναδημιουργία της κάθε φορά που χρειάζεται.

Unit Testing

Αυτό το χαρακτηριστικό χρησιμοποιείται για την αποφυγή από μη αναμενόμενες συμπεριφορές της εφαρμογής. Με το unit testing το οποίο καταναλώνει αρκετό χρόνο ανάπτυξης, επιτρέπει την ορθή λειτουργία και την απαλοιφή των λαθών της εφαρμογής.

Το Laravel προσφέρει μοναδικές και επεκτάσιμες λύσεις με μία πολύ μεγάλη κοινότητα προγραμματιστών να το υποστηρίζει.

Κεφάλαιο 4ο: Το σύστημα ηλεκτρονικής ψηφοφορίας

4.1 Εισαγωγή – Η διαδικασία

Ο χρήστης πρέπει να συνδεθεί στο σύστημα αφού πατήσει το κουμπί σύνδεση όπως φαίνεται στο παρακάτω σχήμα.



Ηλεκτρονικό Σύστημα Ψηφοφορίας

Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων

Διεθνές Πανεπιστήμιο Ελλάδος

[Σύνδεση](#)

Σχήμα 4.1: Το σύστημα – η εφαρμογή

Στη συνέχεια πρέπει να βάλει το email και το password του όπως φαίνεται στο παρακάτω σχήμα.

Ηλεκτρονικό Σύστημα Ψηφοφορίας

Email

Password

Login

Σχήμα 4.2: Εισαγωγή στοιχείων πρόσβασης

Μετά την επιτυχή είσοδο – σύνδεση του χρήστη μεταφέρεται στην Κεντρική σελίδα και σε αυτήν μπορεί να πατήσει το κουμπί για τη Δημιουργία Νέας Ψηφοφορίας.



Τμήμα Μηχανικών
Πληροφορικής και Ηλεκτρονικών
Συστημάτων

Έξοδος

[donkixwtis1990@gmail.com]

Ηλεκτρονικές Ψηφοφορίες

Μπορείτε να δημιουργήσετε μια νέα ηλεκτρονική ψηφοφορία και να δείτε σε ποιές ψηφοφορίες είσαστε διαχειριστής, σε ποιές είσαστε εφορευτική επιτροπή και σε ποιές έχετε ψηφίσει

Δημιουργία Νέας Ψηφοφορίας

Σχήμα 4.3: Δημιουργία Ψηφοφορίας

Επίσης, μπορεί να δει πληροφορίες όσον αφορά Ψηφοφορίες στις οποίες είναι Διαχειριστής, μέλος ή υποψήφιο μέλος εφορευτικής επιτροπής και σε ποιες ψηφοφορίες έχει ψηφίσει.

Διαχειριστής στις ψηφοφορίες

Δεν είσαστε Διαχειριστής σε καμιά Ψηφοφορία Εφορευτική Επιτροπή

Εφορευτική επιτροπή στις ψηφοφορίες

Δεν έχετε οριστεί σε καμιά Ψηφοφορία Εφορευτική Επιτροπή

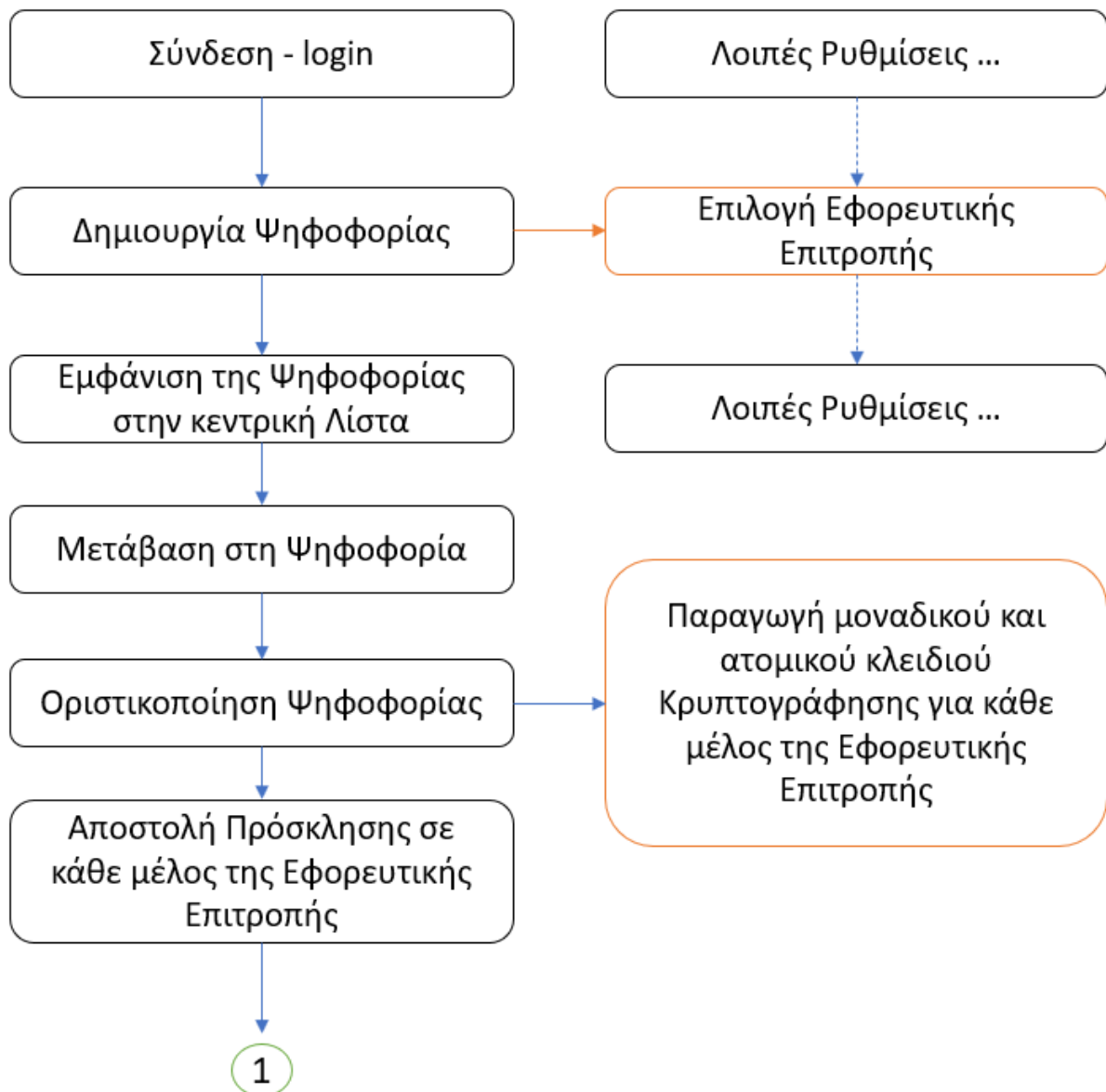
Συμμετοχή στις ψηφοφορίες (έχετε ψηφίσει στις παρακάτω)

Δεν έχετε ψηφίσει σε καμιά Ψηφοφορία Εφορευτική Επιτροπή

Σχήμα 4.4: Η κεντρική σελίδα με τις λίστες

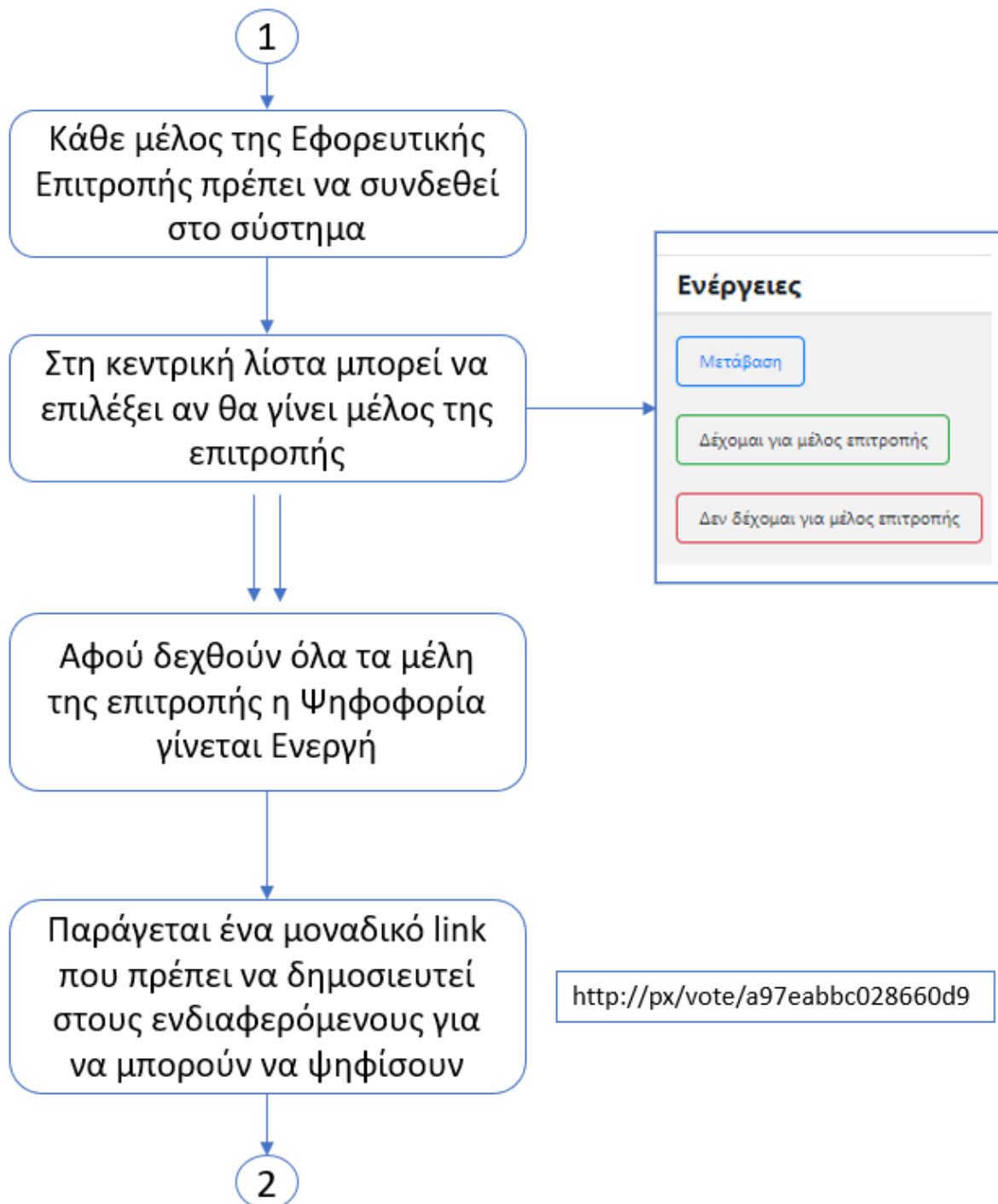
Στο παρακάτω σχήμα 4.5 παρουσιάζεται η διαδικασία για τα πρώτα βήματα, από τη δημιουργία μέχρι την αποστολή πρόσκλησης για κάθε μέλος της εφορευτικής. Προς το παρόν το σύστημα δεν στέλνει email αλλά παράγει ένα μοναδικό-ατομικό κωδικό για κάθε μέλος στη βάση.

Έτσι το κάθε μέλος αρκεί μόνο να συνδεθεί στο σύστημα και να κάνει Αποδοχή για τη συγκεκριμένη ψηφοφορία

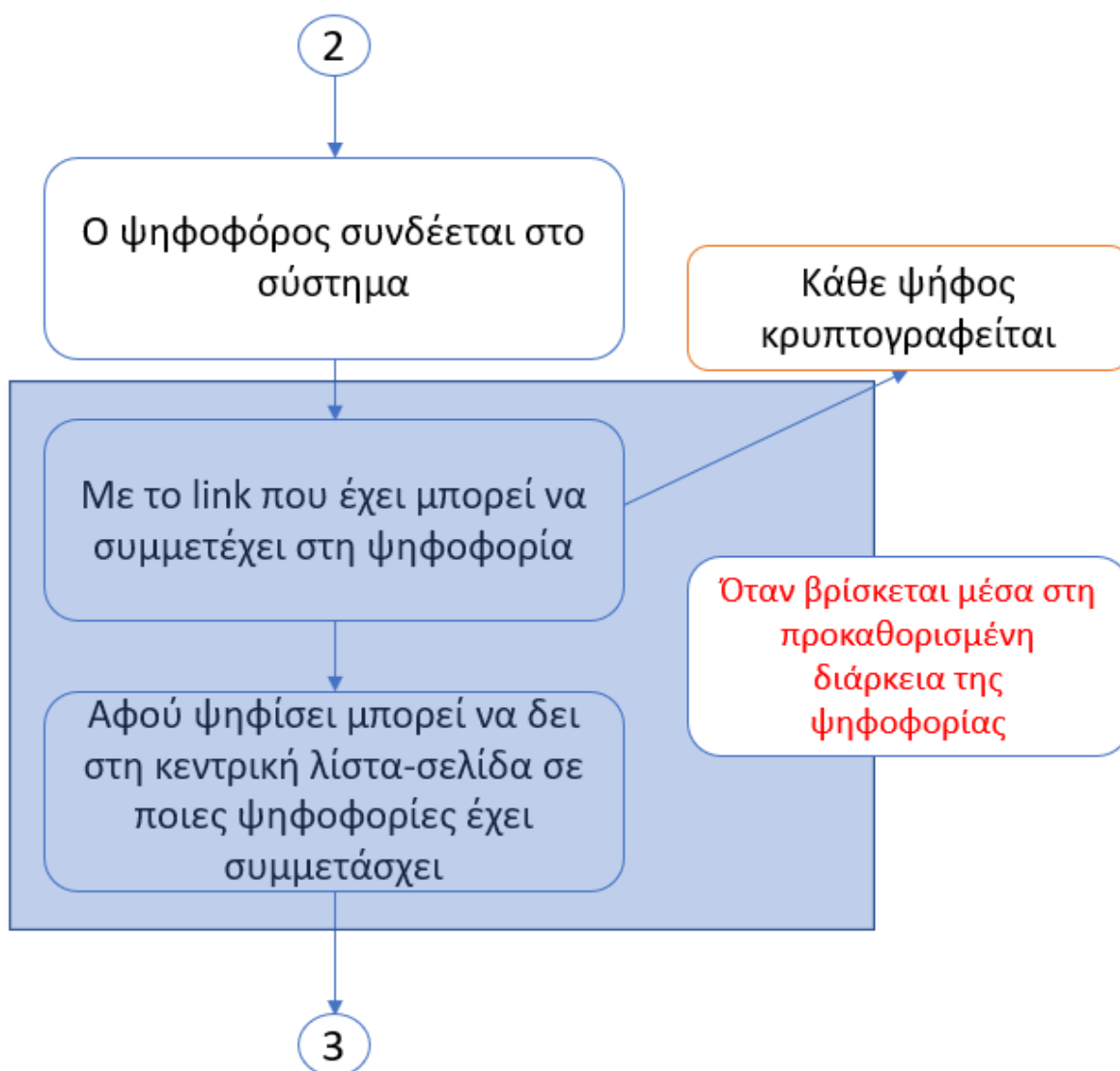


Σχήμα 4.5: Διαδικασία από τη δημιουργία μέχρι την αποστολή πρόσκλησης για κάθε μέλος της εφορευτικής

Στο επόμενο σχήμα 4.6 παρουσιάζεται η διαδικασία για την αποδοχή από ένα χρήστη, ότι δέχεται να είναι μέλος μιας εφορευτικής επιτροπής. Στη κεντρική λίστα μπορεί να επιλέξει αν θα γίνει μέλος της επιτροπής. Αφού δεχθούν όλα τα μέλη της επιτροπής η Ψηφοφορία γίνεται Ενεργή. Στη συνέχεια παράγεται ένα μοναδικό link που πρέπει να δημοσιευτεί στους ενδιαφερόμενους για να μπορούν να ψηφίσουν.

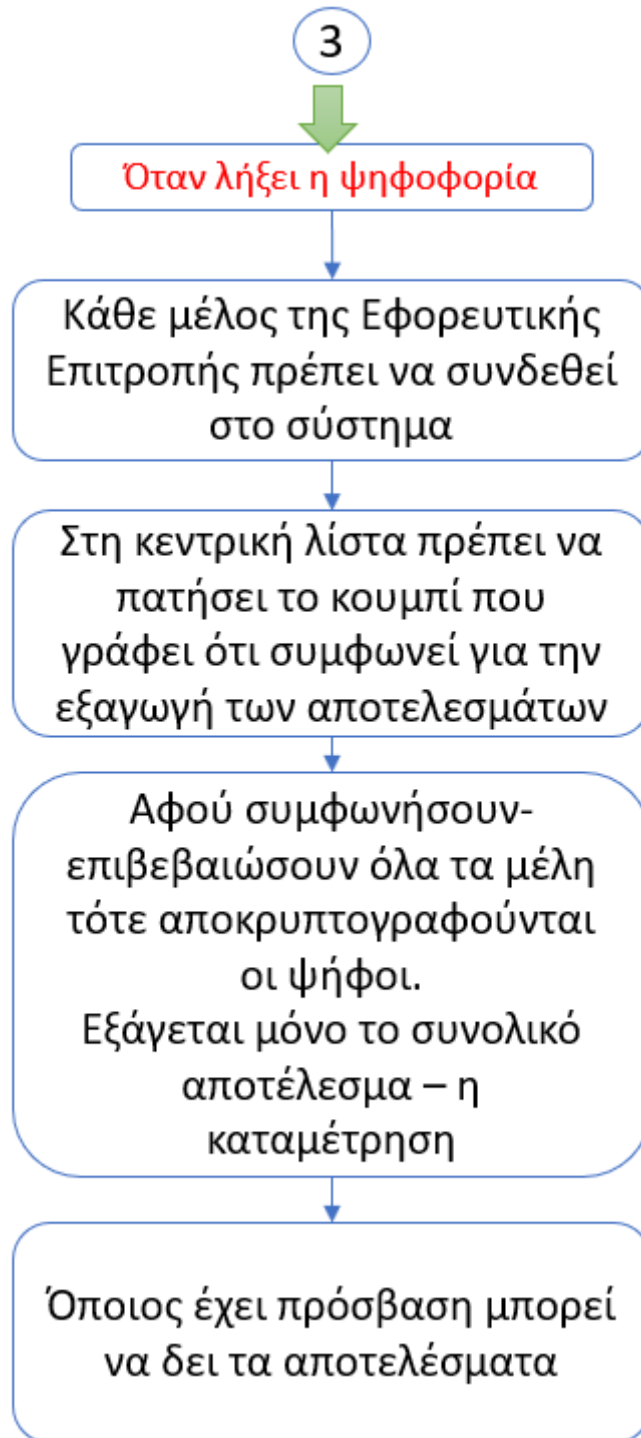


Σχήμα 4.6: Διαδικασία για την αποδοχή από ένα χρήστη να είναι μέλος μιας εφορευτικής επιτροπής



Σχήμα 4.7: Διαδικασία κατάθεσης ψήφου από κάποιον Χρήστη.

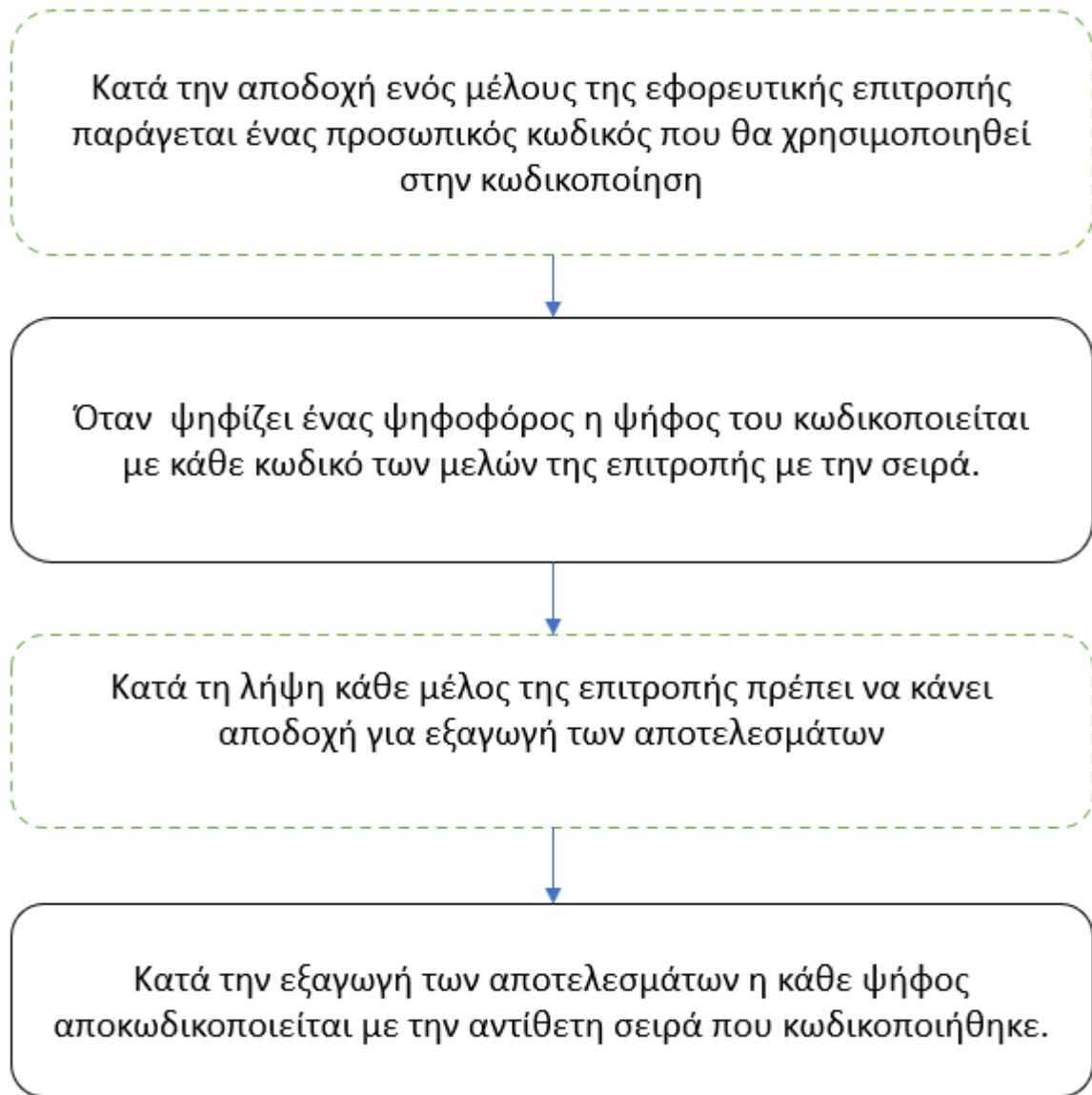
Στο Σχήμα 4.7 παρουσιάζεται η διαδικασία κατάθεσης ψήφου από κάποιον Χρήστη. Ο ψηφοφόρος συνδέεται στο σύστημα και με το link που έχει μπορεί να συμμετέχει στη ψηφοφορία μόνο όταν βρίσκεται μέσα στη προκαθορισμένη διάρκεια της ψηφοφορίας και αυτή είναι ενεργή. Κάθε ψήφος κρυπτογραφείται. Αφού ψηφίσει μπορεί να δει στη κεντρική λίστα-σελίδα σε ποιες ψηφοφορίες έχει συμμετάσχει.



Σχήμα 4.8: Διαδικασία μετά τη λήξη ψηφοφορίας

Όταν λήξει η ψηφοφορία κάθε μέλος της Εφορευτικής Επιτροπής πρέπει να συνδεθεί στο σύστημα. Στη κεντρική λίστα πρέπει να πατήσει το κουμπί που γράφει ότι συμφωνεί για την εξαγωγή των αποτελεσμάτων. Αφού συμφωνήσουν-επιβεβαιώσουν όλα τα μέλη τότε αποκρυπτογραφούνται οι

ψηφοί. Εξάγεται μόνο το συνολικό αποτέλεσμα – η καταμέτρηση. Όποιος έχει πρόσβαση μπορεί να δει τα αποτελέσματα.



Σχήμα 4.9: Μέθοδος κρυπτογράφηση/αποκρυπτογράφησης για την κατάθεση ψήφου και την εξαγωγή-καταμέτρηση των ψήφων/αποτελεσμάτων

Στο Σχήμα 4.9 παρουσιάζεται η μέθοδος κρυπτογράφηση/αποκρυπτογράφησης για την κατάθεση ψήφου και την εξαγωγή-καταμέτρηση των ψήφων/αποτελεσμάτων.

Κατά την αποδοχή ενός μέλους της εφορευτικής επιτροπής παράγεται ένας προσωπικός κωδικός που θα χρησιμοποιηθεί στην κωδικοποίηση. Όταν ψηφίζει ένας ψηφοφόρος η ψήφος του κωδικοποιείται με κάθε κωδικό των μελών της επιτροπής με την σειρά. Κατά τη λήψη κάθε μέλος της επιτροπής πρέπει

να κάνει αποδοχή για εξαγωγή των αποτελεσμάτων. Κατά την εξαγωγή των αποτελεσμάτων η κάθε ψήφος αποκωδικοποιείται με την αντίθετη σειρά που κωδικοποιήθηκε.

Δεν αποθηκεύεται και δεν γνωρίζει κανένας τι ψήφισε κάποιος χρήστης.

Κατά την εξαγωγή των ψήφων γίνεται μόνο καταμέτρηση.

4.2 Η εφαρμογή - ιστοσελίδα

Στο υποκεφάλαιο αυτό θα περιγραφεί η εφαρμογή-ιστοσελίδα του συστήματος.

Δημιουργία ψηφοφορίας

Τίτλος ψηφοφορίας

 ✓

Περιγραφή ψηφοφορίας

 ✓

Σχήμα 4.10: Μέθοδος κρυπτογράφηση/αποκρυπτογράφησης για την κατάθεση ψήφου και την εξαγωγή-καταμέτρηση

Στο σχήμα 4.10 παρουσιάζονται τα πεδία εισαγωγής Τίτλου και Περιγραφής για τη Ψηφοφορία.

Δημιουργία ψηφοφορίας

Τίτλος ψηφοφορίας

Ο τίτλος είναι υποχρεωτικός.

Σχήμα 4.11: Το πεδίο εισαγωγής Τίτλου για τη Ψηφοφορία όταν δεν είναι επιτυχής η εισαγωγή χαρακτήρων


Στο σχήμα 4.11 παρουσιάζεται το πεδίο εισαγωγής Τίτλου για τη Ψηφοφορία όταν δεν είναι επιτυχής η εισαγωγή χαρακτήρων.

Δημιουργία ψηφοφορίας

Τίτλος ψηφοφορίας

Περιγραφή ψηφοφορίας

Σχήμα 4.12: Τα πεδία εισαγωγής Τίτλου και Περιγραφής για τη Ψηφοφορία όταν είναι επιτυχής η εισαγωγή χαρακτήρων.

Στο σχήμα 4.12 παρουσιάζονται τα πεδία εισαγωγής Τίτλου και Περιγραφής για τη Ψηφοφορία όταν είναι επιτυχής η εισαγωγή χαρακτήρων.

Έναρξη της ψηφοφορίας

Συμπληρώστε την ημερομηνία και ώρα έναρξης της ψηφοφορίας

Ημερομηνία έναρξης

06-01-2021

Ώρα έναρξης

09:00



Λήξη της ψηφοφορίας

Συμπληρώστε την ημερομηνία και ώρα λήξης της ψηφοφορίας

Ημερομηνία λήξης

06-01-2021

Ώρα λήξης

09:00



Σχήμα 4.13: Τα πεδία εισαγωγής για Ημερομηνία/Ώρα Έναρξης και Λήξης για τη Ψηφοφορία

Στα σχήματα 4.12-4.13 παρουσιάζονται τα πεδία εισαγωγής για Ημερομηνία/Ώρα Έναρξης και Λήξης για τη Ψηφοφορία και οι επιλογές τους.

Έναρξη της ψηφοφορίας

Συμπληρώστε την ημερομηνία και ώρα έναρξης της ψηφοφορίας

Ημερομηνία έναρξης

06-01-2021

Ώρα έναρξης

09:00



Calendar popup for January 2021. The title is "Ιανουάριος 2021". The days of the week are labeled: Δε, Τρ, Τε, Πε, Πα, Σα, Κυ. The calendar grid shows the following dates:

Δε	Τρ	Τε	Πε	Πα	Σα	Κυ
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

The date 06 is highlighted in yellow. A green checkmark and dropdown arrow icon are visible to the right of the calendar.

Σχήμα 4.14: Η επιλογή για την Ημερομηνία

Δημιουργία ψηφοφορίας

Τίτλος ψηφοφορίας

Εκλογή Προέδρου

Περιγραφή ψηφοφορίας

Μια μικρή περιγραφή της ψηφοφορίας

Έναρξη της ψηφοφορίας

Συμπληρώστε την ημερομηνία και ώρα έναρξης

Ημερομηνία έναρξης

06-01-2021

07:00
07:15
07:30
07:45
08:00
08:15
08:30
08:45
09:00
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
11:45
12:00

09:00 ✓

Σχήμα 4.15: Η επιλογή για την Ώρα

Στο σχήμα 4.16 παρουσιάζονται τα πεδία εισαγωγής/επιλογής για το email Υποστήριξης, της Εφορευτικής Επιτροπής και το είδος των Ψηφοφόρων που μπορούν να συμμετέχουν στη Ψηφοφορία.


Email υποστήριξης

Οι ψηφοφόροι μπορούν να απευθύνονται σε αυτό το e-mail για υποστήριξη σε θέματα της ψηφοφορίας

Εφορευτική επιτροπή

Η λίστα εφορευτικής επιτροπής είναι υποχρεωτική. Προτείνεται το βασικό μέλος να είναι ο διαχειριστής - ο δημιουργός της Ψηφοφορίας. Επιτρέπεται η μονομελής. Μέγιστο τα πέντε μέλη.

  Αναζήτηση 

Ψηφοφόροι

Οι ψηφοφόροι μπορεί να ανήκουν στις παρακάτω κατηγορίες

- Φοιτητές + Εκπαιδευτικό Προσωπικό
- Φοιτητές
- Εκπαιδευτικό Προσωπικό

Σχήμα 4.16: Τα πεδία εισαγωγής/επιλογής για το email Υποστήριξης, της Εφορευτικής Επιτροπής και το είδος των Ψηφοφόρων που μπορούν να συμμετέχουν στη Ψηφοφορία

Email υποστήριξης

Οι ψηφοφόροι μπορούν να απευθύνονται σε αυτό το e-mail για υποστήριξη σε θέματα της ψηφοφορίας

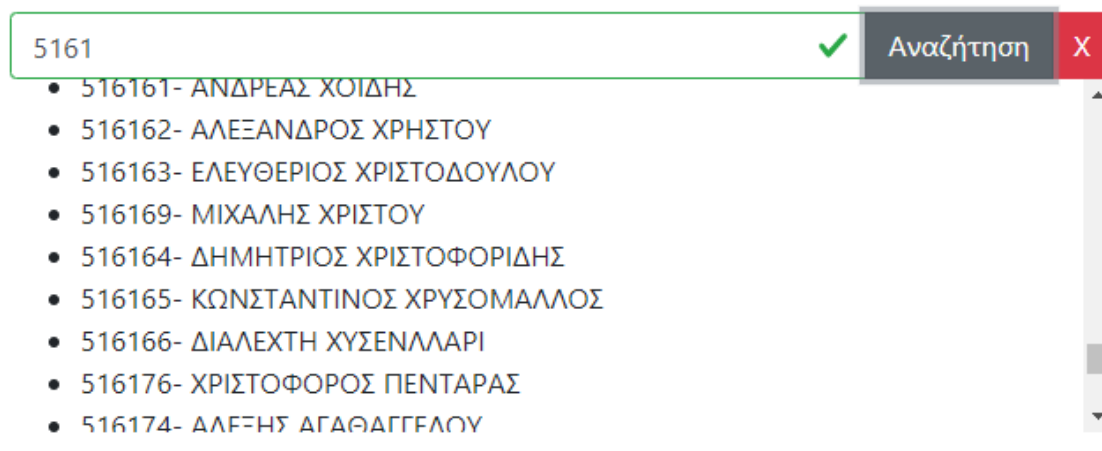
To email είναι υποχρεωτικό.

Σχήμα 4.17: Το πεδίο εισαγωγής για το email Υποστήριξης όταν δεν ικανοποιούνται οι απαιτούμενες προϋποθέσεις στην εισαγωγή

Στο σχήμα 4.17 παρουσιάζεται το πεδίο εισαγωγής για το email Υποστήριξης όταν δεν ικανοποιούνται οι απαιτούμενες προϋποθέσεις στην εισαγωγή.

Εφορευτική επιτροπή

Η λίστα εφορευτικής επιτροπής είναι υποχρεωτική. Προτείνεται το βασικό μέλος να είναι ο διαχειριστής - ο δημιουργός της Ψηφοφορίας. Επιτρέπεται η μονομελής. Μέγιστο τα πέντε μέλη.



5161 ✓ Αναζήτηση X

- 516161- ΑΝΔΡΕΑΣ ΧΟΙΔΗΣ
- 516162- ΑΛΕΞΑΝΔΡΟΣ ΧΡΗΣΤΟΥ
- 516163- ΕΛΕΥΘΕΡΙΟΣ ΧΡΙΣΤΟΔΟΥΛΟΥ
- 516169- ΜΙΧΑΛΗΣ ΧΡΙΣΤΟΥ
- 516164- ΔΗΜΗΤΡΙΟΣ ΧΡΙΣΤΟΦΟΡΙΔΗΣ
- 516165- ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΡΥΣΟΜΑΛΛΟΣ
- 516166- ΔΙΑΛΕΧΤΗ ΧΥΣΕΝΛΛΑΡΙ
- 516176- ΧΡΙΣΤΟΦΟΡΟΣ ΠΕΝΤΑΡΑΣ
- 516174- ΑΛΕΞΗΣ ΑΓΑΘΑΓΓΕΛΟΥ

Σχήμα 4.18: Το πεδίο εισαγωγής για τα μέλη της εφορευτικής επιτροπής

Στο σχήμα 4.18 παρουσιάζεται το πεδίο εισαγωγής για τα μέλη της εφορευτικής επιτροπής. Ο χρήστης εισάγει τουλάχιστον 3 γράμματα και εμφανίζονται τα αποτελέσματα από τα οποία μπορεί να επιλέξει ο χρήστης.

Εφορευτική επιτροπή

Η λίστα εφορευτικής επιτροπής είναι υποχρεωτική. Προτείνεται το βασικό μέλος να είναι ο διαχειριστής - ο δημιουργός της Ψηφοφορίας. Επιτρέπεται η μονομελής. Μέγιστο τα πέντε μέλη.

1. 516165- ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΡΥΣΟΜΑΛΛΟΣ
2. 516164- ΔΗΜΗΤΡΙΟΣ ΧΡΙΣΤΟΦΟΡΙΔΗΣ
3. 516171- ΠΕΤΡΟΣ ΓΕΩΡΓΙΟΥ



5161 ✓ Αναζήτηση X

- 516164- ΔΗΜΗΤΡΙΟΣ ΧΡΙΣΤΟΦΟΡΙΔΗΣ
- 516165- ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΡΥΣΟΜΑΛΛΟΣ
- 516171- ΠΕΤΡΟΣ ΓΕΩΡΓΙΟΥ

Σχήμα 4.19: Η λίστα για τα μέλη της εφορευτικής επιτροπής όπως την επέλεξε ο χρήστης

Στο σχήμα 4.19 παρουσιάζεται η λίστα για τα μέλη της εφορευτικής επιτροπής όπως την επέλεξε ο χρήστης.

Ελάχιστο Πλήθος Επιλογών

Πόσους ψήφους το ελάχιστο πρέπει να βάλει ο ψηφοφόρος

Θα περιέχει η ψηφοφορία τη Λευκή ψήφο;

Μέγιστο Πλήθος Επιλογών

Μέχρι πόσους ψήφους μπορεί να βάλει ο ψηφοφόρος

Σχήμα 4.20: Τα πεδία για το ελάχιστο και μέγιστο πλήθος επιλογών


Στο σχήμα 4.20 παρουσιάζονται τα πεδία για το ελάχιστο και μέγιστο πλήθος επιλογών και η επιλογή αν θα συμπεριληφθεί η λευκή ψήφος στη ψηφοφορία. Το ελάχιστο πρέπει να είναι πάνω από ένα και το 1 σημαίνει ο ψηφοφόρος πρέπει να βάλει μια τουλάχιστον ψήφο. Το μέγιστο σημαίνει μέχρι πόσες ψήφους μπορεί να βάλει. Αν ήταν 2 σημαίνει ότι ο ψηφοφόρος μπορεί να βάλει μέχρι και 2 ψήφους.

Ερώτηση και Επιλογές

Εδώ θα ορίσετε την ερώτηση που θα θέσετε στους ψηφοφόρους και τις επιλογές από τις οποίες θα επιλέξει ο ψηφοφόρος.

Επιτρέπεται μόνο μια επιλογή μόνο όταν είναι ενεργοποιημένη η Λευκή ψήφος.

Ερώτηση: 

Επιλογές (διπλό κλικ πάνω στην επιλογή για διαγραφή) 

Σχήμα 4.21: Το πεδίο για την ερώτηση που θα υπάρχει στην Ψηφοφορία για να κατατοπίσει τον ψηφοφόρο


Στο σχήμα 4.21 παρουσιάζεται το πεδίο για την ερώτηση που θα υπάρχει στην Ψηφοφορία για να κατατοπίσει τον ψηφοφόρο.

Ερώτηση και Επιλογές

Εδώ θα ορίσετε την ερώτηση που θα θέσετε στους ψηφοφόρους και τις επιλογές από τις οποίες θα επιλέξει ο ψηφοφόρος.

Επιτρέπεται μόνο μια επιλογή μόνο όταν είναι ενεργοποιημένη η Λευκή ψήφος.

Ερώτηση: 


Επιλογές (διπλό κλικ πάνω στην επιλογή για διαγραφή) 

-
-

Σχήμα 4.22: Προσθήκη κενών επιλογών

Επιτρέπεται μόνο μια επιλογή μόνο όταν είναι ενεργοποιημένη η Λευκή ψήφος.

Ερώτηση: 

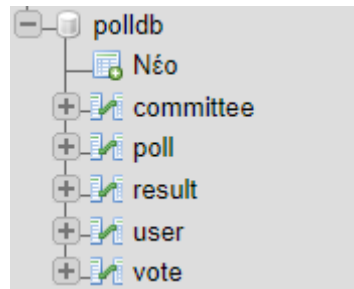
Επιλογές (διπλό κλικ πάνω στην επιλογή για διαγραφή) 

-
-

Σχήμα 4.23: Οι επιλογές που έχουν προστεθεί με το κουμπί '+'

Στα σχήματα 4.22-4.23 παρουσιάζονται οι επιλογές που έχουν προστεθεί με το κουμπί '+'. Υπάρχει δυνατότητα απεριόριστης προσθήκης και διαγραφής.

4.3 Η Βάση



Σχήμα 4.24: Η βάση με τους πίνακες

Η βάση κατασκευάστηκε με MySQL MariaDB και στο σχήμα 4.24 παρουσιάζεται το σχέδιο με τους πίνακες που χρησιμοποιήθηκαν.

Στα επόμενα σχήματα παρουσιάζονται οι πίνακες και τα πεδία που περιλαμβάνει ο καθένας.

Οι πίνακες όλοι διαθέτουν τα πεδία `id` που είναι το κεντρικό κλειδί και είναι αύξων αριθμός,

Το `active` για να προσδιοριστεί αν είναι ενεργή η εγγραφή.

Τα πεδία `created_at` και `updated_at` είναι για την αποθήκευση για το πότε δημιουργήθηκε και πότε ανανεώθηκε η εγγραφή στη βάση.

#	Όνομα	Τύπος	Σύνθεση	Χαρακτηριστικά	Κενό	Προεπιλογή	Σχόλια	Πρόσθετα
1	id 🗝️	int(10)		UNSIGNED	Όχι	Καμία		AUTO_INCREMENT
2	active	tinyint(3)		UNSIGNED	Όχι	1		
3	statuspoll	tinyint(4)			Όχι	1		
4	guid 🗝️	varchar(16)	utf8mb4_general_ci		Ναι	NULL		
5	user_id	int(10)		UNSIGNED	Όχι	Καμία		
6	title	varchar(300)	utf8mb4_general_ci		Όχι	Καμία		
7	description	text	utf8mb4_general_ci		Ναι	NULL		
8	datestart	datetime			Όχι	Καμία		
9	dateend	datetime			Όχι	Καμία		
10	timestart	time			Όχι	09:00:00		
11	timeend	time			Όχι	14:00:00		
12	emailsupport	varchar(100)	utf8mb4_general_ci		Όχι	Καμία		
13	commembers	longtext	utf8mb4_bin		Όχι	Καμία		
14	voters	tinyint(3)		UNSIGNED	Όχι	Καμία		
15	minchoice	tinyint(3)		UNSIGNED	Όχι	1		
16	maxchoice	tinyint(3)		UNSIGNED	Όχι	1		
17	whitevote	tinyint(3)		UNSIGNED	Όχι	0		
18	question	varchar(300)	utf8mb4_general_ci		Όχι	Καμία		
19	choices	longtext	utf8mb4_bin		Όχι	Καμία		
20	created_at	timestamp			Ναι	current_timestamp()		
21	updated_at	timestamp			Ναι	current_timestamp()		

Σχήμα 4.25: Ο πίνακας poll - Δομή

id	active	statuspoll	guid	user_id	title	description
1	0	3	afe36d72a1d7ae68	65	Πειραματικός Τίτλος 1	
2	1	6	afe36d72a1d7ae69	65	Πειραματικός Τίτλος 2	
3	1	1	afe36d72a1d7ae62	1474	Πειραματικός Τίτλος 3	
4	1	2	b6871602f6472732	65	Πειραματικός Τίτλος 4 nai	rete
5	1	1	9db4efe1a37ba60e	65	Πειραματικός Τίτλος 5	
6	1	1	32bb5d079b169dc8	65	Πειραματικός Τίτλος 6	aaa
13	1	1	b7b68dda53fff7be	5717	Εκλογή Προέδρου	Μια μικρή περιγραφή για την εκλογή Προέδρου
14	1	1	fa780a67a11a0f56	5717	Εκλογή Αντιπροέδρου	
15	1	1	9415dc6b1048f970	5717	Να γίνει η εξεταστική Φεβρουαρίου δια ζώσης;	

Σχήμα 4.26: Ο πίνακας Poll - Περιεχόμενο

#	Όνομα	Τύπος	Σύνθεση	Χαρακτηριστικά	Κενό	Προεπιλογή	Σχόλια	Πρόσθετα
1	id 🗝️	int(10)		UNSIGNED	Όχι	Καμία		AUTO_INCREMENT
2	active	tinyint(3)		UNSIGNED	Όχι	1		
3	user_id	int(10)		UNSIGNED	Όχι	Καμία		
4	poll_id	int(10)		UNSIGNED	Όχι	Καμία		
5	cryptocode	varchar(32)	utf8mb4_general_ci		Όχι	Καμία		
6	codeconfirmed	tinyint(3)		UNSIGNED	Όχι	0		
7	pollconfirmed	tinyint(3)		UNSIGNED	Όχι	0		
8	created_at	timestamp			Όχι	current_timestamp()		
9	updated_at	timestamp			Όχι	current_timestamp()		

Σχήμα 4.27: Ο πίνακας committee - Δομή

id	active	user_id	poll_id	cryptocode	codeconfirmed	pollconfirmed
1	0	736	1	2c7b98d0789f1895e7abf99ffd043f10	1	0
2	0	1474	1	fc73da715259a119ef802c33fcb46af6	1	0
3	0	1653	1	d5d770142bfe4267cf15840941dcf076	1	0
10	1	733	2	e64f3732977fb765592bf5b50306e657	1	1
11	1	1475	2	34b1b28444b97f049fe3e20a40d64046	1	1
12	1	65	2	ffdce7a5e5fc299cc6cb2b174344805c	1	1
13	1	65	4	c22b18ea8296567773bc813e6c26ea09	1	1
14	1	503	4	1354a3e80804e4d6658b3b2142b34ea9	0	0
15	1	618	4	c57e241f75fd33b15ed62fb50b66c098	0	0
16	1	65	16	253686bbdfe12a4a610c394e8321ee9e	1	1
17	1	732	16	3762135e1ef7f26f1e516495cc971ddb	1	1
18	1	5540	16	50828c7c481af3fb9754b03c318a28c8	1	1
19	1	5540	17	f3e102dde625e92f6e5f0aab7c0a7504	0	0

Σχήμα 4.28: Ο πίνακας committee - Περιεχόμενο

#	Όνομα	Τύπος	Σύνθεση	Χαρακτηριστικά	Κενό	Προεπιλογή	Σχόλια	Πρόσθετα
1	id 🗝️	int(10)		UNSIGNED	Όχι	Καμία		AUTO_INCREMENT
2	active	tinyint(3)		UNSIGNED	Όχι	1		
3	user_id	int(10)		UNSIGNED	Όχι	Καμία		
4	poll_id	int(10)		UNSIGNED	Όχι	Καμία		
5	sumresults	longtext	utf8mb4_bin		Όχι	Καμία		
6	whitevote	tinyint(4)		UNSIGNED	Όχι	0		
7	totalsum	int(10)		UNSIGNED	Όχι	0		
8	created_at	timestamp			Όχι	current_timestamp()		
9	updated_at	timestamp			Όχι	current_timestamp()		

Σχήμα 4.29: Ο πίνακας result - Δομή

id	active	user_id	poll_id	sumresults	whitevote	totalsum
3	1	65	2	[1,2,1]	1	4
5	1	5717	16	[1,1,1,0,0]	1	3

Σχήμα 4.30: Ο πίνακας result - Περιεχόμενο

#	Όνομα	Τύπος	Σύνθεση	Χαρακτηριστικά	Κενό	Προεπιλογή	Σχόλια	Πρόσθετα
1	id 🗝️	int(10)		UNSIGNED	Όχι	Καμία		AUTO_INCREMENT
2	active	tinyint(3)		UNSIGNED	Όχι	1		
3	user_id	int(10)		UNSIGNED	Όχι	Καμία		
4	poll_id	int(10)		UNSIGNED	Όχι	Καμία		
5	cryptovote	text	utf8mb4_bin		Όχι	Καμία		
6	created_at	timestamp			Όχι	current_timestamp()		
7	updated_at	timestamp			Όχι	current_timestamp()		

Σχήμα 4.31: Ο πίνακας vote - Δομή

id	active	user_id	poll_id	cryptovote
18	0	65	1	eyJpdil6lmJMa0JyUWd4aG85VG44OWNCQmFkeWc9PSIsInZhbH...
23	1	65	2	eyJpdil6lko3bHNLZDFtbTVPRUczVTlxSDZBRmc9PSIsInZhbH...
24	1	15	2	eyJpdil6lIRHM0p6czBJT0FENFJDRzJvb1BTQIE9PSIsInZhbH...
25	1	101	2	eyJpdil6lkFHVm9TdEdlemdPQWF0a1d4a25vS0E9PSIsInZhbH...
26	1	12118	2	eyJpdil6ljNXTmlwWE9uY2FJeXVDNGlvb01MaWc9PSIsInZhbH...
27	1	12	16	eyJpdil6lIZzNzBwZy9XeVdudUJsQTIMMIV3Q3c9PSIsInZhbH...
28	1	5717	16	eyJpdil6lmpiQm1yVUhlbExscY1ZWZ5NkRaUIE9PSIsInZhbH...
29	1	5540	16	eyJpdil6ljlObnZwU2J4UXREamU4cjJMWjBocUE9PSIsInZhbH...

Σχήμα 4.32: Ο πίνακας vote - Περιεχόμενο

4.4 Ασφάλεια στο σύστημα και στα δεδομένα

Διασφάλιση του απορρήτου της ψήφου

Το στεγανό για την προστασία του απορρήτου είναι η κρυπτογράφηση της ψήφου. Κάθε ψήφος κρυπτογραφείται διαδοχικά με τα κλειδιά της επιτροπής τα οποία δεν γνωρίζει κάποιος άλλος χρήστης. Η αποκρυπτογράφηση πραγματοποιείται μόνο όταν επιβεβαιώσουν όλα τα μέλη της εφορευτικής επιτροπής και οι ψήφοι αποκωδικοποιούνται με την αντίστροφη σειρά με την οποία κρυπτογραφήθηκαν. Να σημειωθεί ότι δεν αποθηκεύεται πουθενά η ψήφος του κάθε ψηφοφόρου αλλά γίνεται μόνο καταμέτρηση για την κάθε επιλογή.

Ασφάλεια με κωδικούς πρόσβασης στην ιστοσελίδα.

Ο χρήστης μπορεί να συνδεθεί με το σύστημα μόνο αν εισάγει σωστά τα στοιχεία του, email και password. Τότε δημιουργείται ένα session που αποθηκεύει τα στοιχεία του χρήστη.

Ασφάλεια με session για την αυθεντικοποίηση στην επικοινωνία του χρήστη με το σύστημα

Όλες οι ενέργειες του χρήστη πραγματοποιούνται μέσω του session που έχει αποθηκευτεί για τον χρήστη κατά την επιτυχή σύνδεση-είσοδο του. Αν πατηθεί ένα κουμπί για μια ενέργεια ή οποιαδήποτε άλλη ενέργεια που χρειάζεται το σύστημα ελέγχει αν αυτή η ενέργεια έγινε από εξουσιοδοτημένο χρήστη που έχει συνδεθεί επιτυχώς στο σύστημα. Το session αποθηκεύεται στο server και έχει περιορισμένη διάρκεια.

Ασφάλεια επικοινωνίας δεδομένων με SSL

Η επικοινωνία του χρήστη με το σύστημα-ιστοσελίδα πραγματοποιείται μέσω SSL ασφαλούς επικοινωνίας για να παρέχεται ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Το SSL [20] χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών εγκαθιστώντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου.

Κεφάλαιο 5ο: Συμπεράσματα και προτάσεις βελτίωσης

Παρουσιάστηκε και αναλύθηκε μελέτη ορισμένων ηλεκτρονικών ψηφοφοριών και μια εφαρμογή ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου που υλοποιήθηκε με Laravel και βάση δεδομένων mySql.

Μελετήθηκαν υπάρχοντα συστήματα διαδικτυακής ψηφοφορίας και με επίκεντρο το ελληνικό σύστημα ηλεκτρονικής ψηφοφορίας το Zeus το οποίο χρησιμοποιείται από τα Ελληνικά Πανεπιστήμια και φορείς της εκπαίδευσης. Υλοποιήθηκε μια web εφαρμογή χρησιμοποιώντας το γνωστό PHP framework Laravel για να μπορούν οι φοιτητές και το προσωπικό μέσα στο Τμήμα να δημιουργήσουν μια ηλεκτρονική ψηφοφορία και να συμμετέχουν τα μέλη του τμήματος χρησιμοποιώντας τα ίδια στοιχεία πρόσβασης τους που χρησιμοποιούν και σε άλλες υπηρεσίες.

Ο χρήστης που χρησιμοποιεί την ιστοσελίδα πρόσβασης στο σύστημα είναι εξουσιοδοτημένος. Όλοι οι χρήστες-μέλη του των υπηρεσιών του Τμήματος να μπορούν να έχουν πρόσβαση στο σύστημα Ηλεκτρονικής Ψηφοφορίας και μπορούν να δημιουργήσουν σε μια ηλεκτρονική ψηφοφορία. Οι χρήστες μπορούν να συμμετέχουν ως εφορευτική επιτροπή ή απλοί ψηφοφόροι σε μια ηλεκτρονική ψηφοφορία.

Οι ψήφοι να είναι μυστικοί και κρυπτογραφημένοι ενώ η κρυπτογράφηση και η αποκρυπτογράφηση της ψήφου για την καταμέτρηση να γίνεται με κωδικούς που διαθέτει η εφορευτική επιτροπή χωρίς να αποθηκεύεται η κάθε ψήφος σε κάποιο χώρο.

Η ασφάλεια του συστήματος περιεγράφηκε στο προηγούμενο κεφάλαιο και μπορούμε να συμπεράνουμε ότι η χρήση session σε κάθε απαίτηση του διασφαλίζει την αυθεντικοποίηση του χρήστη χωρίς να απαιτείται συνεχώς η εισαγωγή email-password.

Όσον αφορά τις βελτιώσεις από τις πιο σημαντικές είναι η διαχείριση των κωδικών της εφορευτικής επιτροπής και η προσθήκη και άλλων ειδών ψηφοφορίας. Το πρώτο αφορά την ασφάλεια της κρυπτογράφησης και της αποκρυπτογράφησης της ψήφου και των αποτελεσμάτων. Στην παρούσα έκδοση της εφαρμογής οι κωδικοί είναι ατομικοί, μυστικοί και αποθηκευμένοι στη βάση για κάθε μέλος της εφορευτικής επιτροπής. Αυτό σημαίνει ότι ο διαχειριστής με κάποιο τρόπο θα μπορούσε να έχει πρόσβαση στα αποτελέσματα. Για να αποφευχθεί αυτό οι κωδικοί πρέπει να αποστέλλονται με email σε κάθε μέλος ξεχωριστά και να τον έχει μόνο αυτός. Όταν ζητηθεί η αποκρυπτογράφηση και η εξαγωγή των αποτελεσμάτων τότε να τον εισάγουν με δική τους ευθύνη. Βέβαια σε περίπτωση που χαθεί ένας κωδικός η ψηφοφορία είναι άκυρη. Όσο αφορά το δεύτερο θα μπορούσε η εφαρμογή να υποστηρίζει και άλλου είδους ψηφοφορίες όπως είναι η χρήση με βάρη ή με βαθμούς.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Saltman, Roy. Effective Use of computing technology in vote-tallying,2016-02-11 at Wikiwix. *NIST*.
- [2] Fujiwara, Thomas (2015). "Voting Technology, Political Responsiveness, and Infant Health: Evidence From Brazil". *Econometrica*. **83** (2): 423–464
- [3] https://en.wikipedia.org/wiki/Electronic_voting
- [4] https://en.wikipedia.org/wiki/DRE_voting_machine
- [5] Germann, Micha; Serdült, Uwe (2017-06-01). "Internet voting and turnout: Evidence from Switzerland" *Electoral Studies*. **47**: 1–12.
- [6] Goodman, Nicole; Stokes, Leah C. (July 2020). "Reducing the Cost of Voting: An Evaluation of Internet Voting's Effect on Turnout". *British Journal of Political Science*
- [7] <http://infopoll.com/>
- [8] <http://www.trueballot.com/trueballot.aspx>
- [9] <https://truevote.com.au/>
- [10] <https://zeus.grnet.gr/zeus/>
- [11] <https://www.php.net/manual/en/migration70.new-features.php>
- [12] <https://www.zend.com/>
- [13] <https://en.wikipedia.org/wiki/PHP>
- [14] <https://www.mysql.com/>
- [15] <https://mariadb.org/>
- [16] <https://laravel.com/>
- [17] <https://en.wikipedia.org/wiki/Model%E2%80%93view%E2%80%93controller>
- [18] https://en.wikipedia.org/wiki/Object%E2%80%93relational_mapping
- [19] <https://lumen.laravel.com/>
- [20] <https://www.ssl.com/faqs/faq-what-is-ssl/>

ΠΑΡΑΡΤΗΜΑ Α

Στο παράρτημα αυτό αναφέρονται τα βασικά κομμάτια του κώδικα που χρησιμοποιήθηκε.

```
<?php

namespace App\Http\Controllers;

use Illuminate\Http\Request;
use Illuminate\Support\Facades\Log;
use Illuminate\Support\Facades\DB;
use DateTime;

use Illuminate\Encryption\Encrypter;

class PollController extends Controller
{
    function index()
    {
        if (session('loggedin') == 0)
            return redirect('/');

        $users = DB::select('select * from user where active = ?', [1]);
        return view('poll', ['poll' => null, 'date1' => '', 'date2' => '', 'userscommembers' => '']);
    }

    function getpoll($id)
    {
        Log::info("getpoll");

        if (session('loggedin') == 0)
            return redirect('/');

        $user = session('loggeduser');
        $user_id = $user->id;
        $poll = DB::select('select * from poll where active = 1 and id=?', [$id]);

        $date1='';
        $date2='';
        $userscommembers='';

        if ($poll != null)
        {
            $poll=$poll[0];

            $phpdate1 = strtotime( $poll->datestart );
            $date1 = date( 'm-d-Y', $phpdate1 );
        }
    }
}
```

```

    $phpdate2 = strtotime( $poll->dateend );
    $date2 = date( 'm-d-Y', $phpdate2 );

    $data=json_decode($poll->commembers);
    $query_include = "" . implode( ",", "" , $data ) . "";

    $query = "select user.id, user.am, user.name from user where active = 1 and id IN (". $quer
y_include . ")";
    $userscommembers = DB::select($query);
    return view('poll', [ 'poll' => $poll, 'date1' => $date1, 'date2' => $date2, 'userscommembe
rs' => $userscommembers]);
}
else
    return redirect('/main');
}

function savepoll(Request $request)
{

    if (session('loggedin') == 0)
        return redirect('/');

    $user = session('loggeduser');
    $user_id = $user->id;

    $pollid = is_int(intval($request->input('pollid'))) ? $request->input('pollid') : 0;
    $poll = DB::select('select * from poll where active = 1 and user_id=? and id=?', [$user_id, $p
ollid ]);

    if($poll != null) if($poll[0]->statuspoll != 1)
        return response()-
>json(array('msg' => 'Η Ψηφοφορία δεν μπορεί να επεξεργαστεί', 'status' => false));

    $formData = urldecode($request->input('formData'));
    preg_match_all("/([^&=]+)=([^&=]+)/", $formData, $r);
    $result = array_combine($r[1], $r[2]);
    Log::info($result); //Log::info($result['title']);

    $memberscomm = $request->input('memberscomm');
    $choicesarray = $request->input('choicesarray');
    //Log::info('memberscomm= '.count($memberscomm));
    Log::info('choicesarray= '.count($choicesarray));

    if (!isset($result['title'])) $title = '';
    else $title = $result['title'];

    if (!isset($result['description'])) $description = '';
    else $description = $result['description'];

```

```

if (!isset($result['whitevote'])) $whitevotecheck = 0;
else
{
    $whitevotecheck = $result['whitevote'] = 'on'?1:0;
}

if (!isset($result['minchoice'])) $minchoice = 1;
else $minchoice = is_int(intval($result['minchoice'])) ? $result['minchoice'] : 1;

Log::info('maxchoice= '.$result['maxchoice']);
if (!isset($result['maxchoice'])) $maxchoice = 1;
else $maxchoice = is_int(intval($result['maxchoice'])) ? $result['maxchoice'] : 1;
Log::info('maxchoice= '.$maxchoice);

if (!isset($result['emailsupport'])) $emailsupport = '';
else $emailsupport = $result['emailsupport'];

if (!isset($result['question'])) $question = '';
else $question = $result['question'];

if (!isset($result['chradio'])) $voters = 1;
else $voters = is_int(intval($result['chradio'])) ? $result['chradio'] : 1;

if (isset($result['datepickerstart'])) $datestart = $result['datepickerstart'];
else return response()-
>json(array('msg' => 'Πρόβλημα με Ημερομηνία Έναρξης', 'status' => false));
if (isset($result['datepickerend'])) $dateend = $result['datepickerend'];
else return response()-
>json(array('msg' => 'Πρόβλημα με Ημερομηνία Λήξης', 'status' => false));
if (isset($result['timestart'])) $timestart = $result['timestart'];
else return response()->json(array('msg' => 'Πρόβλημα με Ωρα Έναρξης', 'status' => false));
if (isset($result['timeend'])) $timeend = $result['timeend'];
else return response()->json(array('msg' => 'Πρόβλημα με Ωρα Λήξης', 'status' => false));

$date1 = DateTime::createFromFormat('d-m-Y', $datestart);
if ($date1 == FALSE) return response()-
>json(array('msg' => 'Πρόβλημα με Ημερομηνία Έναρξης', 'status' => false));
$date2 = DateTime::createFromFormat('d-m-Y', $dateend);
if ($date2 == FALSE) return response()-
>json(array('msg' => 'Πρόβλημα με Ημερομηνία Λήξης', 'status' => false));

$time1 = DateTime::createFromFormat('H:i', $timestart);
if ($time1 == FALSE) return response()-
>json(array('msg' => 'Πρόβλημα με Ωρα Έναρξης', 'status' => false));
$time2 = DateTime::createFromFormat('H:i', $timeend);
if ($time2 == FALSE) return response()-
>json(array('msg' => 'Πρόβλημα με Ωρα Λήξης', 'status' => false));

```

```

$date1->setTime($time1->format('H'), $time1->format('i'));
$date1->format('Y-m-d H:i:s');

$date2->setTime($time2->format('H'), $time2->format('i'));
$date2->format('Y-m-d H:i:s');

$datenow = date('Y-m-d H:i:s');

if ($date1 > $date2) return response()-
>json(array('msg' => 'Η Ημερομηνία Λήξης δεν μπορεί να είναι προγενέστερη της Έναρξης', 'status' => false));

if ($date1 < $datenow || $date2 < $datenow) return response()-
>json(array('msg' => 'Οι ημερομηνίες δεν μπορεί να είναι προγενέστερες από σήμερα', 'status' => false));

if (!isset($memberscomm) || (count($memberscomm) < 1 && count($memberscomm) > 5))
return response()-
>json(array('msg' => 'Η λίστα εφορευτικής επιτροπής είναι υποχρεωτική και δεν μπορεί να είναι άδεια. Η λίστα εφορευτικής επιτροπής είναι υποχρεωτική. Προτείνεται το βασικό μέλος να είναι ο διαχειριστής - ο δημιουργός της Ψηφοφορίας. Επιτρέπεται η μονομελής. Μέγιστο τα πέντε μέλη.', 'status' => false));

if (!isset($choicesarray) || (count($choicesarray) <= 1 && $whitevotecheck == 0))
return response()-
>json(array('msg' => 'Το πλήθος των επιλογών πρέπει να είναι πάνω από δύο.', 'status' => false));

if (count($choicesarray) == 0 && $whitevotecheck == 1)
return response()-
>json(array('msg' => 'Το πλήθος των επιλογών πρέπει να είναι πάνω από ένα όταν είναι ενεργοποιημένη η Λευκή ψήφος.', 'status' => false));

if (!isset($result['title']) || strlen($result['title']) <= 5 || strlen($result['title']) > 300) return response()-
>json(array('msg' => 'Το πλήθος των χαρακτήρων του τίτλου πρέπει να είναι μεγαλύτερος από 5 και μικρότερος από 300 ', 'status' => false));

if (strlen($description) > 1000) return response()-
>json(array('msg' => 'Το πλήθος των χαρακτήρων της περιγραφής πρέπει να είναι μικρότερος από 1000 ', 'status' => false));

if (!isset($result['question']) || strlen($result['question']) <= 5 || strlen($result['question']) > 300) return response()-
>json(array('msg' => 'Το πλήθος των χαρακτήρων της ερώτησης πρέπει να είναι μεγαλύτερος από 5 και μικρότερος από 300 ', 'status' => false));

$queryState = false;

```

```

if($poll)
{

$queryState = DB::table('poll')
->where('active', 1)
->where('id', $pollid)
->where('user_id', $user_id)
->update(['title' => $title, 'description' => $description,
'datestart' => $date1, 'dateend' => $date2,
'timestart' => $timestart, 'timeend' => $timeend,
'emailsupport' => $emailsupport, 'commembers' => json_encode($memberscomm),
'voters' => $voters, 'whitevote' => $whitevotecheck,
'minchoice' => $minchoice, 'maxchoice' => $maxchoice,
'question' => $question, 'choices' => json_encode($choicesarray)]);

//Αν δεν έχει γίνει κανένα update επιστρέφει 0
if($queryState == 0) $queryState = true;
}
else
{
$guid = sprintf('%04x%04x%04x%04x', mt_rand(0, 0xffff), mt_rand(0, 0xffff), mt_rand(0, 0xffff)
, mt_rand(0, 0xffff));

$queryState = DB::insert('insert into poll (active, statuspoll, guid, user_id, title, description, datestart, dateend, timestart, timeend, emailsupport, commembers, voters, minchoice, maxchoice, whitevote, question, choices) values (?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?)', [1, 1, $guid, $user_id, $title, $description, $date1, $date2, $timestart, $timeend, $emailsupport, json_encode($memberscomm), $voters, $minchoice, $maxchoice, $whitevotecheck, $question, json_encode($choicesarray)]);
}

if ($queryState) {
// the query succeed
$arr = array('msg' => 'Αποθηκεύτηκε', 'status' => true);
} else {
// the query failed
$arr = array('msg' => 'Κάποιο πρόβλημα παρουσιάστηκε - Ξαναπροσπαθήστε', 'status' => false
);
}

return response()->json($arr);
}

function removepoll(Request $request)
{
Log::info("removepoll");

if (session('loggedin') == 0)

```

```

        return redirect('/');

$user = session('loggeduser');
$user_id = $user->id;

$guid = $request->input('guid');
$poll = DB::select('select * from poll where active = 1 and user_id=? and guid=?', [$user_id,
$guid ]);

if($poll)
{
    $poll = $poll[0];
    if($poll->statuspoll > 3)
        return response()-
>json(array('msg' => 'Η Ψηφοφορία δεν μπορεί να διαγραφεί', 'status' => false));

    DB::table('poll')
    ->where('active', 1)
    ->where('id', $poll->id)
    ->where('user_id', $user_id)
    ->update(['active' => 0]);

    DB::table('committee')
    ->where('active', 1)
    ->where('poll_id', $poll->id)
    ->update(['active' => 0]);

    DB::table('vote')
    ->where('active', 1)
    ->where('poll_id', $poll->id)
    ->update(['active' => 0]);

    DB::table('result')
    ->where('active', 1)
    ->where('poll_id', $poll->id)
    ->update(['active' => 0]);

    return response()->json(array('msg' => 'Η Ψηφοφορία απενεργοποιήθηκε', 'status' => true));
}

return response()->json(array('msg' => 'Δεν υπάρχει αυτή η Ψηφοφορία', 'status' => false));
}

```