2021-01

þÿ £ Ç µ ´ ¹ ± Ã ¼ Ì Â º ± ¹ Å » ¿ À ¿ ¯ · Ã ·

þÿ µ Æ ± Á ¼ ¿ ³ ® Â Ã Å » » ¿ ³ ® Â º ± ¹

þÿ ¿ À Ä ¹ º ¿ À ¿ ¯ · Ã · Â µ À ¹ ´ · ¼ ¹ ¿ » ¿ ³ ¹ º

þÿ ´ µ ´ ¿ ¼ - ½ É ½ ¼ µ Ç Á ® Ã · Ä µ Ç ½ ¿ ›

þÿ À Á ¿ Ã Ä ± Ã ¯ ± Â Ä · Â ¹ ´ ¹ É Ä ¹ º Ì Ä · Ä ±

þÿ À µ Á ¯ À Ä É Ã · Ç Á ® Ã · Â ³ ¹ ± Ä ¿ ½ ¹

þÿ ’ ± Á ´ ¬ Á · Â , • ¹ º Ì » ± ¿ Â

ΙΑΝΟΥΑΡΙΟΣ 2021

Πανεπιστήμιο Νεάπολις Πάφου

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ, ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΙΤΛΟΣ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ:

ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΕΦΑΡΜΟΓΗΣ ΣΥΛΛΟΓΗΣ ΚΑΙ ΟΠΤΙΚΟΠΟΙΗΣΗΣ ΕΠΙΔΗΜΙΟΛΟΓΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ:

ΠΕΡΙΠΤΩΣΗ ΧΡΗΣΗΣ ΓΙΑ ΤΟΝ ΙΟ COVID-19

ΝΙΚΟΛΑΟΣ ΒΑΡΔΑΡΗΣ

ΙΑΝΟΥΑΡΙΟΣ, 2021

Πανεπιστήμιο Νεάπολις Πάφου

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ, ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΙΤΛΟΣ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ:

ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΕΦΑΡΜΟΓΗΣ ΣΥΛΛΟΓΗΣ ΚΑΙ ΟΠΤΙΚΟΠΟΙΗΣΗΣ ΕΠΙΔΗΜΙΟΛΟΓΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ: ΠΕΡΙΠΤΩΣΗ ΧΡΗΣΗΣ ΓΙΑ ΤΟΝ ΙΟ COVID-19

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών: Πληροφοριακά Συστήματα και Ψηφιακή Καινοτομία.

στο Πανεπιστήμιο Νεάπολις.

ΝΙΚΟΛΑΟΣ ΒΑΡΔΑΡΗΣ

ΙΑΝΟΥΑΡΙΟΣ, 2021

Πνευματικά δικαιώματα

"ΣΕΛΙΔΑ ΕΓΚΥΡΟΤΗΤΑΣ" ("VALIDATION PAGE")

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: Νικόλαος Βαρδάρης

Τίτλος Μεταπτυχιακής Διατριβής: Σχεδιασμός και υλοποίηση εφαρμογής συλλογής και οπτικοποίησης επιδημιολογικών δεδομένων με χρήση τεχνολογιών προστασίας της ιδιωτικότητας: περίπτωση χρήσης για τον ιό COVID-19.

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …..…… από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος): ……

Μέλος Εξεταστικής Επιτροπής: ……

Μέλος Εξεταστικής Επιτροπής: ……

Ή ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Ο Νικόλαος Βαρδάρης, γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο Σχεδιασμός και υλοποίηση εφαρμογής συλλογής και οπτικοποίησης επιδημιολογικών δεδομένων με χρήση τεχνολογιών προστασίας της ιδιωτικότητας: περίπτωση χρήσης για τον ιό COVID-19, αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Ο Δηλών

Νικόλαος Βαρδάρης

Περίληψη

Η συλλογή δεδομένων σχετικά με την εμφάνιση συμπτωμάτων στον πληθυσμό, κατά τη διάρκεια επιδημιολογικών κρίσεων, μπορεί να παρέχει σημαντικές πληροφορίες για την εξέλιξη αλλά και την αντιμετώπιση μίας επιδημίας. Με αφορμή την εξάπλωση του ιού COVID-19, όπου υπάρχει μεγάλη διακύμανση στην σοβαρότητα και την ένταση των συμπτωμάτων που εμφανίζονται στον πληθυσμό, η καταγραφή και παρακολούθηση της εμφάνισης συμπτωμάτων καθίσταται ιδιαίτερα δύσκολη.

Η πληροφορία εμφάνισης συμπτωμάτων στον πληθυσμό μίας περιοχής, σε συνδυασμό με την καταγραφή των επιβεβαιωμένων κρουσμάτων μπορεί να παρέχει χρήσιμες πληροφορίες σχετικά με την εξάπλωση του ιού. Τα στοιχεία αυτά, σχετικά με την εμφάνιση συμπτωμάτων στον πληθυσμό, αποτελούν ευαίσθητη προσωπική πληροφορία και είναι απαραίτητο να προστατεύεται, τόσο από διαρροές όσο και από μη-εξουσιοδοτημένες χρήσεις.

Τα παραπάνω αποτέλεσαν το έναυσμα για την εκπόνηση της παρούσας εργασίας η οποία, αφορά το σχεδιασμό και υλοποίηση μιας web εφαρμογής η οποία έχει σκοπό την συλλογή κι οπτικοποίηση επιδημιολογικών δεδομένων σχετικά με την εμφάνιση συμπτωμάτων στον πληθυσμό μίας περιοχής. Ακολουθώντας την λογική της συμμετοχικής ανίχνευσης δεδομένων (participatory sensing) δημιουργούνται καμπάνιες καταγραφής συμπτωμάτων για συγκεκριμένες γεωγραφικές περιοχές. Τα δεδομένα που υποβάλλονται από τους συμμετέχοντες αποθηκεύονται σε κρυπτογραφημένη μορφή και παραμένουν κρυπτογραφημένα κατά την επεξεργασία τους για την εξαγωγή των αθροιστικών αποτελεσμάτων της καμπάνιας με τη χρήση ομομορφικών υπολογισμών. Με τον τρόπο αυτό διασφαλίζεται η προστασία των προσωπικών δεδομένων των συμμετεχόντων, χωρίς την απώλεια χρήσιμης πληροφορίας. Με χρήση σύγχρονων τεχνολογιών και μεθόδων ανάπτυξης εφαρμογών, αλλά και τεχνολογιών προστασίας της ιδιωτικότητας, αναπτύχθηκε σύστημα συλλογής, επεξεργασίας και οπτικοποίησης επιδημιολογικών δεδομένων, το οποίο χρησιμοποιήθηκε για την περίπτωση του ιού COVID-19. Η σχεδίαση και οι μέθοδοι που χρησιμοποιήθηκαν μπορούν να προσαρμοστούν για την μελέτη οποιασδήποτε περίπτωσης επιδημιολογικών δεδομένων.

Το σύστημα που αναπτύχθηκε επιτυγχάνει την αποτελεσματική συλλογή των δεδομένων από τους συμμετέχοντες, μέσω της ανάπτυξης κατάλληλης web εφαρμογής για την δημιουργία και διαχείριση καμπανιών συλλογής δεδομένων εμφάνισης συμπτωμάτων. Τα δεδομένα συλλέγονται κι αποθηκεύονται σε κρυπτογραφημένη μορφή, στο σύστημα backend

που αναπτύχθηκε, όπου και γίνεται η επεξεργασία τους για τη διεξαγωγή των συγκεντρωτικών αποτελεσμάτων ανά γεωγραφική περιοχή. Στη συνέχεια, τα αποτελέσματα των υπολογισμών οπτικοποιούνται μέσω κατάλληλης υλοποίησης δυναμικής απεικόνισης των δεδομένων, σε χάρτη και αλλά και πίνακες αναλυτικής παρουσίασης των δεδομένων.

Keywords: Ομομορφική κρυπτογραφία, συλλογή κι ανάλυση δεδομένων, επιδημιολογικά δεδομένα, κρυπτογραφημένοι υπολογισμοί, υπολογισμοί διατήρησης της ιδιωτικότητας, κρυπτοσύστημα Paillier.

Abstract

The collection of data on the occurrence of symptoms in the population, during epidemiological crises, can provide important information for the development and treatment of an epidemic. Due to the spread of COVID-19 virus, where there is a large variation in the severity and intensity of symptoms that appear in the population, recording and monitoring the onset of symptoms becomes particularly challenging.

Information about the appearance of symptoms in the population of an area, combined with the recording of confirmed cases can provide useful information about the spread of the virus. This data however, regarding the occurrence of symptoms in the population, constitute sensitive personal information and it is necessary to protect it, both from leaks and from unauthorized uses.

The above were the trigger for the elaboration of the present work, which concerns the design and implementation of a web application that aims to collect and visualize epidemiological data on the occurrence of symptoms in the population of an area. Following the logic of participatory sensing, symptom recording campaigns are created for specific geographical areas. The data submitted by the participants is stored in encrypted form and remains encrypted during their processing to extract the cumulative results of the campaign using homomorphic calculations. This ensures the protection of the personal data of the participants, without the loss of useful information. Using modern technologies and methods of application development, as well as privacy-preserving technologies, a system for collection, processing and visualization of epidemiological data is eveloped, which was applied to the use case of the COVID-19 virus. The design and methods used can be adapted to study any case of epidemiological data.

The developed system achieves the effective collection of data by the participants, through the development of a suitable web application for the creation and management of symptomatic data collection campaigns. The data is ollected and stored in encrypted form, in the backend system, where they are processed to calculate the aggregate results by geographical area. Then, the results of the calculations are visualized through appropriate implementation of dynamic display of the data on a map and additionally on tables containing detailed presentation of the data.

Keywords: Homomorphic encryption, data collection and analysis, epidemiological data, encrypted calculations, privacy-preserving calculations, Paillier cryptosystem

Ευχαριστίες:

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου, Δρ. Αιμιλία Τασίδου και το συνεπιβλέποντα Δρ. Γεώργιο Δροσάτο για τις συμβουλές, την τεχνική υποστήριξη, την καθοδήγηση που μου πρόσφεραν. καθώς, και την άριστη συνεργασία που είχαμε κατά τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας.

Τώρα που έφτασα στο τέλος της μεταπτυχιακής μου φοίτησης θα ήθελα να ευχαριστήσω τους ανθρώπους που με βοήθησαν και με στήριξαν στις δύσκολες στιγμές.

Περιεχόμενα

Περίληψη iv

Abstract vi

Περιεχόμενα ix

1^0 Κεφάλαιο: Εισαγωγή 1

1.1 Σκοπός και επί μέρους στόχοι: 1

1.2 Βασικά ερευνητικά ερωτήματα: 2

1.3 Αναγκαιότητα και σπουδαιότητα: 2

1.4 Δομή της εργασίας: 3

2^0 Κεφάλαιο: Υπόβαθρο (background) και βιβλιογραφική ανασκόπηση 4

2.1 Συνοπτική βιβλιογραφική ανασκόπηση, σχετικής με το θέμα υφιστάμενης κατάστασης: 4

2.2 Κρυπτογράφηση Paillier: 5

3^0 Κεφάλαιο: Σχεδιασμός και Υλοποίηση 8

3.1 Μεθοδολογία 8

3.2 Υλοποίηση 10

3.2.1 Μη σχεσιακή βάση δεδομένων: NoSQL 10

3.2.2 Βάση δεδομένων: MongoDB 12

3.2.3 Γλώσσα προγραμματισμού: C# 13

3.2.4 Διερμηνευμένη γλώσσα προγραμματισμού: JAVASCRIPT 13

3.2.5 Framework : ANGULAR 14

3.2.6 Πλοήγηση εντός εφαρμογής: Angular Router Ng Module 16

3.2.7 Πλατφόρμα ανάπτυξης λογισμικού: NODE . JS 16

4^0 Κεφάλαιο: Αποτελέσματα 18

4.1 Αρχική οθόνη - Home 18

4.2 Οθόνη Active campaigns 18

4.3 Οθόνη Campaign Management 20

4.4 Οθόνη Campaign Analysis 24

4.5 Οθόνη Calendar 26

4.6 Οθόνη Login/Logout 27

5^0 Κεφάλαιο: Συμπεράσματα 28

Βιβλιογραφία 29

Κατάλογος Γραφικών Παραστάσεων/Εικόνων/Διαγραμμάτων

Εικόνα 1 Home ……...… 18

Εικόνα 2 Active campaigns …… 19

Εικόνα 3 Data Entry…… 20

Εικόνα 4 MongoDB….……...…… 20

Εικόνα 5 Campaign management…… 21

Εικόνα 6 Campaign creation……... 22

Εικόνα 7 Public Keu – PrivateKey Key…….. 22

Εικόνα 8 Campaign lock……. 23

Εικόνα 9 Campaign Insert PrivateKey Key……... 24

Εικόνα 10 Map Analysis …… 25

Εικόνα 11 Analysis……. 26

Εικόνα 12 Calendar…… 27

Εικόνα 13 Login……. 27

1^0 Κεφάλαιο: Εισαγωγή

Αποτελεί κοινή παραδοχή το γεγονός ότι τόσο οι επιδημίες όσο και οι πανδημίες που κατά καιρούς πλήττουν πολλές χώρες του κόσμου, έχουν αναμφίβολα καταστροφικές συνέπειες για τα άτομα και την κοινωνία στην οποία ανήκουν. Σε αυτό το σημείο κρίνεται απαραίτητη μία εννοιολογική διασαφήνιση των όρων «επιδημία» και «πανδημία». Πιο συγκεκριμένα, η επιδημία θεωρείται ένας λοιμός και προσβάλει έναν συγκεκριμένο αριθμό ανθρώπων και για μια συγκεκριμένη χρονική περίοδο. Από την άλλη μεριά, η πανδημία (παν + δήμος), εξαπλώνεται με πολύ γρήγορους ρυθμούς σε μια μεγάλη περιοχή και απειλεί ένα πολύ μεγάλο μέρος του πληθυσμού.

Στο σημείο αυτό αξίζει να αναφερθούν ενδεικτικά και κάποιες από τις πιο γνωστές πανδημίες που έπληξαν την ανθρωπότητα, όπως χαρακτηριστικά ήταν ο λοιμός που ξέσπασε στην Αθήνα το 430 π.Χ., η πανδημία της χολέρας, η ελονοσία, η πανδημία της γρίπης το 2009 και τέλος η πανδημία της ασθένειας του κορδονιού που ξέσπασε αρχικά στην πόλη Γιουχάν της Κίνας και επηρέασε το μεγαλύτερο μέρος του πληθυσμού του κόσμου, συμπεριλαμβανομένης φυσικά και της Ελλάδας και της Κύπρου.

Όλα αυτά αποτέλεσαν το έναυσμα για την εκπόνηση της παρούσας εργασίας, με σκοπό των εντοπισμό των χαρακτηριστικών της εξάπλωσης του ιού, μέσω της συλλογής κι οργάνωση των επιδημιολογικών δεδομένων, γεγονός που θα συμβάλλει στην παρουσίαση μιας πιο ξεκάθαρης εικόνας της εμφάνισης συμπτωμάτων του κορονοϊού καθώς και του ποσοστού που πλήττεται από την πανδημία.

1.1 Σκοπός και επί μέρους στόχοι:

Η εργασία αυτή σκοπεύει στην εύρεση αποδοτικών τρόπων συλλογής, επεξεργασίας και οπτικοποίησης επιδημιολογικών δεδομένων, με στόχο την παροχή ενημέρωσης σχετικά με την πυκνότητα εμφάνισης συμπτωμάτων κατά γεωγραφική περιοχή.

Στόχο αποτελεί η εθελοντική συλλογή δεδομένων από τους συμμετέχοντες, εξασφαλίζοντας την προστασία της ιδιωτικότητας των δεδομένων των συμμετεχόντων. Η εφαρμογή στοχεύει στον υπολογισμό και την οπτικοποίηση συγκεντρωτικών (aggregate)

δεδομένων ανά γεωγραφική περιοχή, με σκοπό την παρακολούθηση εμφάνισης συμπτωμάτων που σχετίζονται με την υπό μελέτη επιδημία.

Η εργασία εφαρμόζεται στην περίπτωση του ιού COVID-19, η σχεδίαση και οι μέθοδοι που αναπτύχθηκαν μπορούν να προσαρμοστούν για την μελέτη οποιασδήποτε περίπτωσης επιδημιολογικών δεδομένων.

1.2 Βασικά ερευνητικά ερωτήματα:

Τα ερευνητικά ερωτήματα τα οποία στόχος είναι να απαντηθούν στα πλαίσια της εργασίας αυτής είναι τα παρακάτω:

- Εύρεση κατάλληλης μεθόδου συλλογής των δεδομένων από τους χρήστες, για την παράλληλη επίτευξη αποδοτικότητας των διεργασιών και προστασίας των δεδομένων.
- Εύρεση κατάλληλης μεθόδου οπτικοποίησης των δεδομένων για την χρηστική αναπαράσταση της πληροφορίας.
- Σχεδίασης κατάλληλης διεπαφής χρήστη, τόσο για την υποβολή των δεδομένων από τους συμμετέχοντες, όσο και για την αναπαράσταση των αποτελεσμάτων της επεξεργασίας.

1.3 Αναγκαιότητα και σπουδαιότητα:

Η συλλογή κι επεξεργασία επιδημιολογικών δεδομένων σε μεγάλη κλίματα, αποτελεί βήμα κρίσιμης σημασίας για την αξιολόγηση της κατάστασης εξάπλωσης μίας επιδημίας και την εξαγωγή συμπερασμάτων σχετικά με την αντιμετώπισή της. Η επεξεργασία των επιδημιολογικών δεδομένων παρέχει χρήσιμη πληροφορία, τόσο σχετικά με την αποτελεσματικότητα προηγούμενων δράσεων για το περιορισμό της εξάπλωσης μίας επιδημίας, όσο και σχετικά με την ανάγκη ενίσχυσης ή μη των δράσεων σε σχέση με την παρούσα κατάσταση.

Η δυνατότητα καταμέτρησης εμφάνισης συμπτωμάτων στον γενικό πληθυσμό, ανοίγει νέες δυνατότητες ανάλυσης και εξαγωγής συμπερασμάτων, καθώς μεγάλο ποσοστό

του πληθυσμού χωρίς έντονα συμπτώματα δεν προσμετράται από τις δομές υγείας, όμως μπορεί να συμβάλλει δραστικά στην μετάδοση της νόσου.

Ακόμη και η σύγκριση της συχνότητας εμφάνισης συμπτωμάτων σε μη-επιβεβαιωμένα κρούσματα μπορεί να καταδείξει ενδιαφέρουσες συσχετίσεις τόσο με άλλες νόσους που εξελίσσονται παράλληλα ή και με το ποσοστό εμφάνισης επιβεβαιωμένων κρουσμάτων της υπό εξέλιξη επιδημίας.

1.4 Δομή της εργασίας:

Η δομή της εργασίας αποτελείται από τα παρακάτω κεφάλαια: Στο δεύτερο κεφάλαιο παρουσιάζεται η σχετική βιβλιογραφία καθώς και παρουσιάζεται το υπόβαθρο σχετικά με τους ομομορφικούς υπολογισμούς και την κρυπτογραφία Paillier, μέσω των οποίων διασφαλίζεται η προστασία της ιδιωτικότητας των δεδομένων των συμμετεχόντων.

Στο τρίτο κεφάλαιο γίνεται περιγραφή του μοντέλου αρχιτεκτονικής ανάπτυξης λογισμικού της web εφαρμογής, κι αντίστοιχα περιγράφονται όλες οι γλώσσες προγραμματισμού και τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίησή της.

Στο τέταρτο κεφάλαιο παρουσιάζεται η εφαρμογή με βάση τις παραπάνω τεχνολογίες και γίνεται περιήγηση στις λειτουργίες της. Τέλος, στο πέμπτο κεφάλαιο περιγράφονται τα συμπεράσματα της εργασίας.

2^0 Κεφάλαιο: Υπόβαθρο (background) και βιβλιογραφική ανασκόπηση

2.1 Συνοπτική βιβλιογραφική ανασκόπηση, σχετικής με το θέμα υφιστάμενης κατάστασης:

Η εργασία αυτή βασίζεται στη λογική της συμμετοχικής ανίχνευσης (participatory sensing) (Shi, et al., 2010) (Drosatos, et al., 2017), η οποία επιτρέπει την απόκτηση δεδομένων σχετικά με τις συνθήκες στο περιβάλλον ή για τους ανθρώπους, χρησιμοποιώντας συνδεδεμένες συσκευές όπως κινητά τηλέφωνα ή αυτόνομους αισθητήρες.

Τα δεδομένα γεωγραφικής τοποθεσίας διαδραματίζουν σημαντικό ρόλο σε τέτοιες εφαρμογές, προκειμένου να οργανωθούν και να οπτικοποιηθούν τα δεδομένα που συλλέχθηκαν, για την παραγωγή σημαντικών μετρήσεων. Αυτό το γεγονός ωστόσο εισάγει βελτιωμένες απαιτήσεις προστασίας της ιδιωτικής ζωής σε οποιαδήποτε εφαρμογή που συγκεντρώνει τέτοια δεδομένα, ειδικά σε μεγάλη κλίμακα.

Στον πυρήνα της εφαρμογής υπάρχει ένα κρυπτογραφικό πρωτόκολλο διατήρησης της ιδιωτικής ζωής, το οποίο δέχεται ως είσοδο τα αρχεία συμπτωμάτων από τους χρήστες και εκτελεί ασφαλείς υπολογισμούς secure multi-party computations (Yao, 1982) (Bogetoft, et al., 2009) (Drosatos, et al., 2017) για τον υπολογισμό των συνολικών χαρτών συμπτωμάτων.

Ταυτόχρονα η εφαρμογή αυτή παρουσιάζει συνάφεια με πρωτόκολλα ηλεκτρονικής ψηφοφορίας (e-voting) (Damgård, et al., 2010) (Karlof, et al., 2005), ως προς τις απαιτήσεις λειτουργικότητας και τους στόχους προστασίας της ιδιωτικότητας των δεδομένων.

Η εργασία αυτή βασίζεται στις παραπάνω αρχές και τεχνικές για την παραγωγή μίας σύγχρονης εφαρμογής συλλογής, επεξεργασίας κι οπτικοποίησης επιδημιολογικών δεδομένων με ταυτόχρονη προστασία της ιδιωτικότητας των συμμετεχόντων.

2.2 Κρυπτογράφηση Paillier:

Αποτελεί κοινή παραδοχή το γεγονός ότι στις μέρες μας όλο και περισσότερες επιχειρήσεις και εταιρίες διαχειρίζονται πολύτιμες πληροφορίες αλλά και προσωπικά δεδομένα. Τα δεδομένα αυτά μπορούν μέσω της αποθήκευσής τους σε κρυπτογραφημένη μορφή να προστατευτούν από διαρροές και μη εξουσιοδοτημένες χρήσεις. Η επεξεργασία των κρυπτογραφημένων δεδομένων όμως συχνά απαιτεί την αποκρυπτογράφηση των δεδομένων αυτών, γεγονός που θέτει την ασφάλεια των δεδομένων σε κίνδυνο και εισάγει σημαντικές καθυστερήσεις στη διαδικασία της επεξεργασίας. . Μία σημαντική εξέλιξη της τεχνολογίας που παρέχει λύσεις σε αυτό το σύνθετο πρόβλημα είναι η ομομορφική κρυπτογραφία (homomorphic encryption), η οποία επιτρέπει την επεξεργασία των δεδομένων σε κρυπτογραφημένη μορφή

Ένα από τα πιο γνωστά κρυπτοσυστήματα είναι και το κρυπτοσύστημα Paillier και στο σημείο αυτό θα επισημανθούν κάποια βασικά χαρακτηριστικά του κρυπτοσυστήματος Paillier. Πιο συγκεκριμένα, το εν λόγω κρυπτοσύστημα αποτελεί έναν αλγόριθμο ο οποίος είναι ασύμμετρος με βασική αποστολή του την κρυπτογράφηση δημόσιου κλειδιού. (Αραμπατζής, 2020). Μία από τις πολύ βασικές ομομορφικές ιδιότητες που διαθέτει αυτό το κρυπτοσύστημα είναι ότι επιτρέπει δύο βασικούς τύπους υπολογισμού, οι οποίοι σχετίζονται με την προσθήκη δύο κρυπτογραφημένων κειμένων Αραμπατζής, 2020).

Στο σημείο αυτό θα αποτελούσε παράλειψη να μη γίνει μια εννοιολογική διασαφήνιση της έννοιας της ομομορφικής κρυπτογράφησης. Πιο συγκεκριμένα, η ομομορφική κρυπτογράφηση αποτελεί μια μορφή κρυπτογράφησης, η οποία δίνει τη δυνατότητα στους χρήστες της να πραγματοποιούν διάφορες λειτουργίες μαθηματικού ή λογικού τύπου στα κρυπτογραφικά δεδομένα (Αραμπατζής, 2020).

Τέλος, αξίζει να υπογραμμιστεί και το γεγονός ότι κατά καιρούς αρκετά σχήματα ομομορφικής κρυπτογράφησης έδιναν τη δυνατότητα να πραγματοποιηθεί σε κρυπτογραφημένα δεδομένα μόνο ένας συγκεκριμένος αριθμός λειτουργιών με χαρακτηριστικό παράδειγμα τον πολλαπλασιασμό και την προσθήκη. Παρόλα αυτά όμως τα τελευταία χρόνια έχουν γίνει προσπάθειες αναβάθμισης των σχημάτων κρυπτογράφησης, τα οποία μπορούν να υποστηρίζουν και αυθαίρετους υπολογισμούς σε κρυπτογραφημένα δεδομένα (Αραμπατζής, 2020).

Στο σημείο αυτό θα γίνει μία αναφορά στη χρησιμότητα της προσθετικής ιδιότητας του ομομορφισμού μέσα από ένα ενδεικτικό παράδειγμα. Πιο συγκεκριμένα, αξίζει να σημειωθεί το γεγονός ότι ο πρόσθετικός ομομορφισμός επιτρέπει να γίνει μια μέτρηση με ανωνυμία. Για να καταστεί αυτό κατανοητό, αρκεί κάποιος να σκεφτεί ένα σύστημα ψηφοφορίας έτσι όπως είναι διαμορφωμένο στις μέρες μας. Με βάση λοιπόν αυτό, έστω ότι ο χρήστης επιθυμεί να κρυπτογραφήσει όλα τα ψηφοδέλτια ενός εκλογικού συμβουλίου, χωρίς να επιτρέπει σε άλλους να μπορούν να διαβάσουν τις ψήφους. Επίσης, ο χρήστης ενδέχεται να επιθυμεί να μάθει το αποτέλεσμα των εκλογών από την εκλογική επιτροπή. Το όλο εγχείρημα βεβαίως δεν είναι εύκολη υπόθεση , καθώς το εκλογικό συμβούλιο δεν είναι σε θέση να γνωρίζει το αποτέλεσμα των εκλογών χωρίς να προβεί σε μια διαδικασία αποκρυπτογράφησης της κάθε ψήφου. Για τον λόγω αυτό, ο πρόσθετος ομομορφισμός επιτρέπει στον χρήστη να ξανασχεδιάσει το σύστημα ψηφοφορίας με τον παρακάτω τρόπο (CLARK, 2020).

Αρχικά, οι ψηφοφόροι μπορούν να κρυπτογραφήσουν τις ψήφους τους χρησιμοποιώντας το δημόσιο κλειδί της εκλογικής επιτροπής. Εν συνεχεία, ο κάθε ψηφοφόρος στέλνει τα κρυπτογραφημένα ψηφοδέλτια στον διακομιστή μέτρησης, ο οποίος με τη σειρά του δίνει την σκυτάλη σε έναν διακομιστή καταμέτρησης, ο οποίος θα προσθέσει όλα τα ψηφοδέλτια και θα αποστείλει το αθροιστικό αποτέλεσμα στην εκλογική επιτροπή. Τέλος, το εκλογικό συμβούλιο θα αποκρυπτογραφήσει το αποτέλεσμα και τελικά θα γνωστοποιήσει το πρόσωπο εκείνο που αναδείχτηκε νικητής στις εκλογές, χωρίς όμως νωρίτερα να διαβάσει την ψήφο κάθε ψηφοφόρου (CLARK, 2020).

Στο σημείο αυτό κρίνεται απαραίτητος ένας διαχωρισμός ανάμεσα στους τύπους της ομομορφικής κρυπτογράφησης. Πιο συγκεκριμένα, παρατηρούνται τρεις βασικοί τύποι ομομορφικής κρυπτογράφησης: η μερικώς ομομορφική κρυπτογράφηση, η κάπως ομομορφική κρυπτογράφηση και τέλος η πλήρης ομομορφική κρυπτογράφηση. Πέραν των κοινών χαρακτηριστικών που εντοπίζονται μεταξύ τους, η βασική διαφορά τους έχει σχέση τόσο με τους τύπους όσο και με την συχνότητα των μαθηματικών λειτουργιών σε σχέση με την εκτέλεση των κρυπτογραφημένων δεδομένων (Daylighting Society, 2017).

Αρχικά, η μερικώς ομομορφική κρυπτογράφηση δίνει τη δυνατότητα εκτέλεσης ορισμένων μαθηματικών συναρτήσεων σε κρυπτογραφημένες τιμές. Έτσι λοιπόν μια συγκεκριμένη λειτουργία εκτελείται απεριόριστα στα κρυπτογραφημένα δεδομένα. Από την άλλη μεριά, αυτό το είδος κρυπτογράφησης αποτελεί την βάση για την

κρυπτογράφηση RSA, που χρησιμοποιείται για να δημιουργηθούν ασφαλείς συνδέσεις μέσω SSL/TLS (Daylighting Society, 2017).

Επιπροσθέτως, η πλήρης ομομορφική κρυπτογράφηση διαθέτει πολλές δυνατότητες, προκειμένου ο χρήστης να διατηρήσει ασφαλείς όλες τις πληροφορίες που διαθέτει αλλά ταυτόχρονα να είναι και εύκολα προσβάσιμες σε αυτόν. Ο τύπος αυτός εξελίσσεται ραγδαία – παρόλο που βρίσκεται σε στάδιο ανάπτυξης – και χρησιμοποιεί και την πρόσθεση αλλά και τον πολλαπλασιασμό σε απεριόριστη μορφή, ενώ βασική του λειτουργία – μεταξύ άλλων – είναι να επιτρέπει την παράλληλη εκτέλεση διάφορων λειτουργιών πολλαπλών μερών. (Daylighting Society, 2017).

3^{0} Κεφάλαιο: Σχεδιασμός και Υλοποίηση

3.1 Μεθοδολογία

Στα πλαίσια ανάπτυξης του λογισμικού, χρησιμοποιηείται το μοντέλο αρχιτεκτονικής λογισμικού MVC (Model-View-Controller) για τη δημιουργία περιβαλλόντων αλληλεπίδρασης χρήστη. Το μοντέλο αυτό είναι πολύ διαδεδομένο την τελευταία 10ετία και χρησιμοποιείται από πολλές δημοφιλείς γλώσσες προγραμματισμού όπως οι JavaScript, Python, PHP, Java, c# κ.α..

Σύμφωνα με το μοντέλο MVC το Project χωρίζεται σε 3 μέρη όπου διασπάται η παρουσίαση της πληροφορίας στον χρήστη από την μορφή που έχει κατά την αποθήκευση και επεξεργασία της στο σύστημα.

Model: Είναι η διαχείριση ανάκτησης – αποθήκευσης των δεδομένων. Γίνεται ενημέρωση για τη γραφική απεικόνιση των κλάσεων που έχουμε ορίσει.

View: Χρησιμοποιείται κατά την παρουσίαση της πληροφορίας στον χρήστη. Απεικονίζει με γραφικό τρόπο την πληροφορία που περιέχει το Model δημιουργώντας γραφική παρουσίαση στον χρήστη. Στην παρούσα εργασία για View θα ακολουθήσουμε το framework της Angular, όπου κι αυτό με την σειρά του ακολουθεί το μοντέλο αρχιτεκτονικής λογισμικού MVC.

Controller: Είναι ένα κομβικό σημείο όπου δέχεται την είσοδο και ενημερώνει το αντικείμενο του Model και του View. Είναι η μηχανή του project για να μπορούμε να κάνουμε εγγραφές στην βάση ή να δείχνουμε διάφορες πληροφορίες στους χρήστες.

Το project αποτελείται από:

Το σύστημα Backend:

Είναι το σημείο όπου εκτελούνται το Model και το Controller. Ακόμα, για την εκτέλεση του controller χρησιμοποιήθηκε η γλώσσα προγραμματισμού Java.

Για βάση δεδομένων υλοποιείται η NoSQL, η οποία είναι κατάλληλη για συγκεκριμένες εφαρμογές που στοχεύουν στην ευελιξία των χρονοδιαγραμμάτων για κατασκευές σύγχρονων εφαρμογών. Η λειτουργία των βάσεων δεδομένων NoSQL βασίζεται σε ποικιλίες μοντέλων δεδομένων για καλύτερη πρόσβαση και διαχείριση στα δεδομένα, όπως έγγραφο, τιμή κλειδιού,

γράφημα, αναζήτηση και μνήμη. Οι δομές δεδομένων που χρησιμοποιούνται από βάσεις δεδομένων NoSQL είναι διαφορετικές από αυτές που χρησιμοποιούνται από προεπιλογή σε σχεσιακές βάσεις δεδομένων, κάνοντας κάποιες λειτουργίες γρηγορότερες στη NoSQL (Schaefer , 2020). Η καταλληλόλητα μιας συγκεκριμένης βάσης δεδομένων NoSQL εξαρτάται από το πρόβλημα προς επίλυση. Επίσης, οι βάσεις δεδομένων NoSQL είναι ευρέως γνωστές λόγω της λειτουργικότητας και της απόδοσής τους σε εφαρμογές Big Data, καθώς ο τρόπος ανάπτυξης τους είναι απλός. Ακόμη, οι βάσεις δεδομένων NoSQL είναι ενδεδειγμένες για σύγχρονες δυναμικές εφαρμογές (Mongo DB, 2020).

Το σύστημα Frontend:

Για την υλοποίηση του View χρησιμοποιείται το Framework της Angular, το οποίο αποτελεί σύγχρονο web framework βασισμένο σε JavaScript. Το Angular εκτελείται στον browser του υπολογιστή, δηλαδή επιτρέπει την εκτέλεση των εφαρμογών client side. Ουσιαστικά η Angular είναι ένα Framework που βασίζεται στην JavaScript και δημιουργεί ένα «αντικείμενο» ως μια σελίδα. Αυτό το αντικείμενο που δημιουργείται μπορεί να αλλάζει μέσα από τους controller για να μορφοποιεί τα services προσθέτοντας data (MDN, 2020).

Το Framework της Angular χρησιμοποιεί την αρχιτεκτονική του MVC, όπου:

- Model: Είναι οι τις κλάσεις που ορίζονται. Αυτό έχει σαν αποτέλεσμα την αποστολή συγκεκριμένων πεδίων στον server και παράλληλα τη λήψη συγκεκριμένων πεδίων από αυτόν.
- View: Είναι το σημείο όπου θα δείξουμε στον χρήστη την τελική οθόνη.
- Controller: Είναι το component που δημιουργείται κατά την δημιουργία μιας νέας σελίδας. Στο σημείο αυτό γίνεται η επικοινωνία με το service και αντίστοιχα το service επικοινωνεί με τον αντίστοιχο controller για να πάρει δεδομένα και να τα δώσει στο View ώστε να τα παρουσιάσει.

Ορισμένες βιβλιοθήκες που πρόκειται να χρησιμοποιηθούν είναι:

1. Για τα Input – Select – Checkbox - icons κ.α. θα χρησιμοποιηθούν τα κοντρόλ της Angular Material.
2. Για τη σχεδίαση της οθόνης θα χρησιμοποιηθεί το Bootstrap.
3. Για τους χάρτες θα χρησιμοποιηθεί το OpenStreetMap.

3.2 Υλοποίηση

Στο σημείο αυτό θα γίνει μια αναφορά όλων των σχετικών προγραμμάτων που χρησιμοποιήθηκαν προκειμένου να ολοκληρωθεί η παρούσα εργασία. Αξίζει να σημειωθεί ότι τα υπό μελέτη προγράμματα διαθέτουν πολύ βασικά χαρακτηριστικά, ενώ παρουσιάζουν πληθώρα πλεονεκτημάτων. Τα προγράμματα που χρησιμοποιήθηκαν για την εκπόνηση της παρούσας εργασίας είναι τα παρακάτω.

3.2.1 Μη σχεσιακή βάση δεδομένων: NoSQL

Αρχικά, το πρώτο πρόγραμμα που χρησιμοποιήθηκε είναι το NoSQL, το οποίο ουσιαστικά αποτελεί μια βάση δεδομένων που δεν βασίζεται σε πίνακες, ενώ βασικό χαρακτηριστικό του είναι ότι διαθέτουν τη δυνατότητα αποθήκευσης διαφορετικών δεδομένων σε σχέση με τους κλασικούς σχεσιακούς πίνακες. Αξίζει να σημειωθεί πως ανάλογα με το μοντέλο δεδομένων τους, περιλαμβάνουν διαφορετικούς τύπους όπως είναι τα έγγραφα, το γράφημα, καθώς επίσης και η ευρεία στήλη. Επιπλέον, δεν είναι λίγοι εκείνοι οι οποίοι συγκρίνουν αυτές τις βάσεις δεδομένων με τις βάσεις δεδομένων τύπου SQL, παρόλο που οι διαφορές μεταξύ τους είναι αρκετές. Πιο συγκεκριμένα, θεωρείται ότι οι βάσεις δεδομένων NoSQL είναι ευκολότερες στη χρήση συγκριτικά με τις βάσεις δεδομένων SQL, υπό την έννοια ότι τα σχετικά δεδομένα δεν είναι απαραίτητο να διαχωριστούν σε πίνακες (Schaefer, 2019).

Εάν επιχειρούσε κανείς να προβεί σε μια ιστορική αναδρομή των εν λόγω δεδομένων, θα τοποθετούσε χρονολογικά αυτές τις βάσεις στα τέλη του 2000, όταν και το κόστος της αποθήκευσης είχε μειωθεί σε σημαντικό βαθμό. Έτσι λοιπόν το βασικό κόστος ανάπτυξης του λογισμικού αφορούσε καθαρά τους προγραμματιστές, με αποτέλεσμα οι βάσεις δεδομένων NoSQL να αλλάξουν μορφή και να βελτιωθούν σημαντικά συμβάλλοντας με αυτόν τον τρόπο στην παραγωγικότητα του προγραμματιστή (Schaefer, 2019).

Όπως προαναφέρθηκε, οι τύποι βάσεων των δεδομένων NoSQL είναι τέσσερις και στη συνέχεια θα αναφερθούν αναλυτικά βάση των χαρακτηριστικών τους στοιχείων.

Αρχικά, ως πρώτος τύπος αναφέρονται οι βάσεις δεδομένων εγγράφων. Οι εν λόγω βάσεις έχουν τη δυνατότητα αποθήκευσης διάφορων δεδομένων σε έγγραφα, τα οποία θυμίζουν τα αντικείμενα JSON. Αναλυτικότερα, το κάθε έγγραφο περιλαμβάνει κάποια ζεύγη πεδίων και τιμών. Όσον αφορά στις τιμές, συνήθως πρόκειται για μια πληθώρα διάφορων τύπων όπως για παράδειγμα συμβολοσειρές, αντικείμενα, πίνακες ή και αριθμούς. Το πιο βασικό πλεονέκτημα αυτού του τύπου είναι ότι έχουν τη δυνατότητα αποθήκευσης πολύ μεγάλου όγκου δεδομένων. Τέλος, αναφέρεται χαρακτηριστικά ότι η πιο γνωστή βάση δεδομένων εγγράφων είναι το MongoDB, το οποίο διαθέτει τεράστιες δυνατότητες (Schaefer, 2019).

Επιπροσθέτως, ένας ακόμη βασικός τύπος βάσεων δεδομένων NoSQL είναι οι βάσεις δεδομένων κλειδιού - τιμής (Key-value), ο οποίος αποτελεί έναν πολύ απλό και εύχρηστο τύπο βάσης δεδομένων. Οι εν λόγω βάσεις επιτρέπουν την αποθήκευση και τη "φιλοξενία" μεγάλου όγκου δεδομένων με πολύ εύκολα ερωτήματα προς απάντηση. Αξίζει βεβαίως να τονιστεί και το γεγονός ότι οι βάσεις δεδομένων κλειδιού-τιμής είναι πολύ διαχωριστικές και προσφέρουν τη δυνατότητα οριζόντιας κλιμάκωσης σε κλίμακες που αδυνατούν να επιτύχουν άλλοι τύποι βάσεων δεδομένων. Εδώ, ο προγραμματιστής μπορεί να χρησιμοποιήσει περιπτώσεις όπως είναι τα παιχνίδια, η τεχνολογία διαφημίσεων, καθώς επίσης και τα IoT που προσφέρονται ιδιαίτερα στο μοντέλο δεδομένων κλειδί - τιμής. (Schaefer, 2019).

Συμπερασματικά, γίνεται εύκολα αντιληπτό το γεγονός ότι η βάση δεδομένων NoSQL αποτελεί μια πολύ χρήσιμη εφαρμογή και σχετίζεται με όλους σχεδόν τους τομείς της καθημερινότητας ενός σύγχρονου ανθρώπου. Είναι επίσης γεγονός ότι αυτές οι βάσεις δεδομένων χρησιμοποιούνται σε διάφορες καθημερινές εφαρμογές, όπως για παράδειγμα στα κινητά ή ακόμη και στα τυχερά παιχνίδια και διακρίνονται από πολλά πλεονεκτήματα καθώς, μεταξύ άλλων, προσφέρουν ευελιξία, υψηλή απόδοση, επεκτασιμότητα και διάφορους εξελιγμένους τύπους δεδομένων (Schaefer , 2020).

Συνοψίζοντας, η συγκεκριμένη τεχνολογία δίνει τη δυνατότητα τόσο στους χρήστες του όσο και στους προγραμματιστές να προβαίνουν σε προσωρινή αποθήκευση δεδομένων, ενώ παράλληλα διαθέτουν και την ικανότητα αναπαραγωγής δεδομένων. Με βάση λοιπόν τα παραπάνω, αντί ο χρήστης - προγραμματιστής να αποθηκεύει μόνο ξένα κλειδιά, μπορεί να αποθηκεύει πραγματικές ξένες τιμές σε συνδυασμό με τα δεδομένα του μοντέλου. Για παράδειγμα, κάθε σχόλιο ιστολογίου μπορεί να περιλαμβάνει το όνομα χρήστη εκτός από ένα αναγνωριστικό χρήστη, δίνοντας με αυτόν τον τρόπο εύκολη πρόσβαση στο όνομα

χρήστη χωρίς να χρειάζεται κάποια άλλη αναζήτηση. Όταν αλλάζει το όνομα ενός χρήστη, αυτό θα πρέπει να μεταβληθεί σε πολλά μέρη της βάσης δεδομένων. Έτσι, αυτή η προσέγγιση λειτουργεί ευκολότερα και φυσικά πιο αποτελεσματικά όταν οι αναγνώσεις είναι πολύ πιο συχνές από ό, τι γράφει (Schaefer , 2020).

3.2.2 Βάση δεδομένων: MongoDB

Συνεχίζοντας, ένα εξίσου σημαντικό πρόγραμμα που διαθέτει χρήσιμες δυνατότητες είναι το MongoDB. Το συγκεκριμένο πρόγραμμα επιτρέπει στους χρήστες του να αποθηκεύουν διάφορα δεδομένα σε έγγραφα τύπου JSON με δυνατότητα ευελιξίας. Αυτή η καινοτόμος δράση διαθέτει πολλές δυνατότητες, καθώς τα πεδία έχουν τη δυνατότητα να διαφέρουν ουσιαστικά από έγγραφο σε έγγραφο, ενώ η δομή των δεδομένων μπορεί να αλλάζει καθώς περνούν τα χρόνια. Ένα ακόμη πολύ βασικό πλεονέκτημα του εν λόγω προγράμματος είναι ότι προσφέρεται εντελώς δωρεάν για τη χρήση του, κάτι που δίνει τη δυνατότητα σε πάρα πολλούς χρήστες να το εντάξουν στα πλαίσια της εργασίας τους (Schaefer , 2020).

Στο σημείο αυτό υπογραμμίζεται ο τρόπος με τον οποίο μπορεί ο χρήστης του MongoDB να εκτελέσει το συγκεκριμένο πρόγραμμα, μέσα από κάποια βασικά χαρακτηριστικά λειτουργίας που διαθέτει. Πιο συγκεκριμένα, παρέχει υψηλή διαθεσιμότητα μέσω ενσωματωμένου αντιγράφου και ανακατεύθυνσης, καθώς επίσης και τη δυνατότητα οριζόντιας επεκτασιμότητας με φυσική θραύση. Επιπλέον, προσφέρει ασφάλεια από άκρο σε άκρο όπως επίσης και εγγενή επικύρωση εγγράφων και εξερεύνηση σχήματος με την πυξίδα. Τέλος, διαθέτει και διάφορα χρηστικά εργαλεία διαχείρισης με δυνατότητα για αυτοματοποίηση ή ακόμη και παρακολούθηση και δημιουργία αντιγράφων ασφαλείας, ενώ οι λειτουργίες του ολοκληρώνονται με μια πλήρως ελαστική βάση δεδομένων ως υπηρεσία με ενσωματωμένες πρακτικές που διενεργούνται με τον βέλτιστο τρόπο (Mongo DB, 2020).

Το εν λόγω πρόγραμμα βάσης δεδομένων αναπτύχθηκε το 2007, ενώ τον Οκτώβρη του 2019 συνεργάστηκε με την Alibaba Cloud (Rouse, 2020). Τέλος αξίζει να σημειωθεί πως το πρόγραμμα αυτό δίνει στους χρήστες του τη δυνατότητα ευρετηρίασης και μεγάλης αποθήκευσης αρχείων (Schaefer , 2020) .

3.2.3 Γλώσσα προγραμματισμού: C#

Ένα ακόμη πολύ εύχρηστο και ευέλικτο εργαλείο προγραμματισμού θεωρείται η γλώσσα C#. Η C# διακρίνεται λοιπόν για την ευελιξία της, ενώ παράλληλα είναι απλή στη χρήση της και με μοντέρνα χαρακτηριστικά. Ένα ακόμη βασικό πλεονέκτημα της C# πέραν των όσων αναφέρθηκαν παραπάνω, είναι ότι εξελίσσεται διαρκώς προσφέροντας απεριόριστες δυνατότητες στους χρήστες του. Η συγκεκριμένη γλώσσα δημιουργήθηκε για να καλύπτει τις ανάγκες των επιχειρήσεων, προκειμένου αυτές να μπορούν να δημιουργούν όλα τα είδη λογισμικού με τη χρήση μόνο μιας γλώσσα προγραμματισμού (Stackify, 2020). Η C# επίσης μπορεί και διαχειρίζεται ανάγκες, οι οποίες σχετίζονται με την ανάπτυξη κινητών, εφαρμογών αλλά και ιστού (Stackify, 2020).

Επιπλέον, μια ακόμη πολύ βασική λειτουργία της C# είναι ότι επιτρέπει τη δημιουργία διάφορων εφαρμογών .NET με δυνατότητα επέκτασης και ανάπτυξης σε πλατφόρμες Linux, Mac ή ακόμη και Windows. Επιπλέον, η C# απαγορεύει τις μετατροπές τύπου, οι οποίες ενδεχομένως να οδηγούν σε απώλεια χρήσιμων δεδομένων, επιτρέποντας ουσιαστικά με αυτόν τον τρόπο στους προγραμματιστές να χρησιμοποιούν έναν ασφαλή κώδικα και αποτελεσματικό κώδικα (Stackify, 2020).

Επιπροσθέτως, αξίζει να αναφερθεί και το γεγονός ότι η συγκεκριμένη γλώσσα εξελίσσεται διαρκώς, παρουσιάζοντας ακόμη πιο προηγμένα χαρακτηριστικά. Είναι γεγονός ότι το C# εξελίσσεται πολύ πιο γρήγορα από οποιαδήποτε άλλη γλώσσα, αφού διαθέτει επιπλέον και την ικανότητα να αναπτύσσει ακόμα και εφαρμογές cloud, όπως επίσης και σύγχρονο λογισμικό μηχανικής μάθησης (Stackify, 2020).

3.2.4 Διερμηνευμένη γλώσσα προγραμματισμού: JAVASCRIPT

Μια σημαντική και χρήσιμη γλώσσα προγραμματισμού είναι η JavaScript. Είναι μια δυναμική γλώσσα προγραμματισμού ηλεκτρονικών υπολογιστών. Η χρήση της είναι η συγγραφή σεναρίου. Το κάθε σενάριο αποτελείται από γραμμές κώδικα όπου μπορούν να διαβάζονται και να

εκτελούνται. Το βασικό πλεονέκτημα αυτού του προγράμματος είναι ότι δίνει τη δυνατότητα στους χρήστες να μπορούν να εφαρμόζουν σύνθετες λειτουργίες σε ιστοσελίδες. Επιπλέον, το περιεχόμενο που θα δημιουργήσει ο χρήστης του Javascript είναι ενημερωμένο με πολύ δυναμικό τρόπο και παράλληλα του δίνει τη δυνατότητα να ελέγχει διάφορα πολυμέσα ή ακόμη και να δημιουργεί αλλά και να ελέγχει με κινούμενες εικόνες (MDN, 2020)!

Πέρα από τις παραπάνω λειτουργίες που αναφέρθηκαν για το συγκεκριμένο πρόγραμμα, αναφέρονται στη συνέχεια και κάποια ακόμη βασικά πλεονεκτήματα της συγκεκριμένης γλώσσας, καθιστώντας την με αυτόν τον τρόπο ένα πολύ βασικό εργαλείο χρήσης. Πιο συγκεκριμένα, ο χρήστης του Javascript μπορεί να αποθηκεύει χρήσιμες τιμές μέσα στις μεταβλητές, ενώ παράλληλα διαθέτει και άλλες λειτουργίες που σχετίζονται με κομμάτια κειμένου τα οποία είναι η γλώσσα του προγραμματισμού. Τέλος, αξίζει να υπογραμμιστεί και το γεγονός ότι πολλοί διερμηνευτές στις μέρες μας χρησιμοποιούν την τεχνική "Just- in - time compilation", η οποία από τεχνικής πλευράς σχετίζεται με την Javascript, καθώς ο κώδικας της γλώσσας αυτής συγκεντρώνεται σε δυαδική μορφή κατά τη διάρκεια της χρήσης του σεναρίου, προκειμένου να εκτελεστεί πιο γρήγορα, γεγονός που εξηγεί τον λόγο που η Javascript θεωρείται ουσιαστικά μια ερμηνευμένη γλώσσα (MDN, 2020).

3.2.5 Framework : ANGULAR

Συνεχίζοντας, δεν θα μπορούσαμε να παραλείψουμε και τις τεράστιες δυνατότητες που προσφέρει η Angular. Το συγκεκριμένο πρόγραμμα αποτελεί μια πλατφόρμα με βασική αποστολή της τη δημιουργία εφαρμογών πελατών μιας σελίδας μέσα από τη χρήση του HTML και του TypeScript. Αξίζει να σημειωθεί επίσης πως το υπό μελέτη πρόγραμμα είναι γραμμένο σε μορφή Typescript, ενώ παράλληλα ένας από τους βασικούς του προσανατολισμούς είναι ότι διαθέτει τη δυνατότητα να εφαρμόζει λειτουργίες μέσα από ένα σύνολο βιβλιοθηκών Typescript, όπου ο κάθε χρήστης μπορεί να εισάγει τις εφαρμογές που επιθυμεί (Angular, 2020).

Επίσης, αξίζει να αναφερθεί και το γεγονός ότι η αρχιτεκτονική μιας γωνιακής εφαρμογής στηρίζεται σε κάποιες πολύ βασικές έννοιες. Τα βασικά δομικά στοιχεία του γωνιακού πλαισίου είναι γωνιακά στοιχεία που οργανώνονται σε NgModules . Τα NgModules συλλέγουν σχετικό κώδικα μέσα σε πλαίσια λειτουργικών συνόλων. Με βάση λοιπόν την ανωτέρω τοποθέτηση, μια γωνιακή εφαρμογή ορίζεται από ένα σύνολο

NgModules. Μια εφαρμογή διαθέτει πάντοτε τουλάχιστον μια ριζική λειτουργική μονάδα που δίνει τη δυνατότητα στο bootstrap να εκ κινηθεί και τις περισσότερες φορές διαθέτει περισσότερες λειτουργικές μονάδες (Krukowski, 2018).

Στο σημείο αυτό είναι αξιοσημείωτο το γεγονός ότι τα στοιχεία παίζουν πολύ σημαντικό ρόλο σε αυτό το πρόγραμμα, καθώς διαθέτουν πολύ σημαντικά γνωρίσματα λειτουργίας. Ειδικότερα, ρυθμίζουν τις προβολές , που αποτελούν σύνολα στοιχείων οθόνης που επιτρέπουν την επιλογή μεταξύ τους και μπορούν να μεταβληθούν ανάλογα με τη λογική αλλά και με τα δεδομένα του προγράμματος. Τέλος, τα στοιχεία χρησιμοποιούν υπηρεσίες , οι οποίες προσφέρουν συγκεκριμένη λειτουργικότητα που όμως δεν συνδέονται άμεσα με προβολές που αναφέρθηκαν νωρίτερα. Με τον τρόπο λοιπόν αυτόν, οι πάροχοι υπηρεσιών έχουν την ικανότητα να εισαχθούν σε εξαρτήματα ως εξαρτήσεις , καθιστώντας τον κώδικα που χρησιμοποιεί ο προγραμματιστής αρθρωτό, επαναχρησιμοποιήσιμο και φυσικά αποδοτικό (Krukowski, 2018).

Επιπροσθέτως, πρέπει να τονιστεί πως τόσο οι ενότητες όσο και τα εξαρτήματα αλλά και οι υπηρεσίες είναι τάξεις που χρησιμοποιούν διακοσμητές . Αυτοί οι διακοσμητές προσφέρουν επισήμανση του τύπου τους ενώ παράλληλα παρέχουν μεταδεδομένα τα οποία περιγράφουν στην Angular τον τρόπο με τον οποίο πρέπει να τα χρησιμοποιούν. Τα μεταδεδομένα αυτά για μια κλάση στοιχείων τα παρομοιάζουν με ένα πρότυπο που καθορίζει μια προβολή. Ένα πρότυπο συνδυάζει το συνηθισμένο HTML με τις γωνιακές οδηγίες και τη δέσμευση σήμανσης που δίνουν την δυνατότητα στο Angular να μεταβάλλει το HTML πριν το αποδώσει για προβολή. Επιπλέον, τα μεταδεδομένα για μια κατηγορία υπηρεσιών δίνουν τις πληροφορίες που χρειάζεται η Γωνιακή για τη διάθεσή της σε εξαρτήματα μέσα από την εξάρτηση (DI) (Angular, 2020).

Τέλος, μια πάρα πολύ σημαντική καινοτομία που προσφέρει το Angular είναι ότι μπορεί να προσφέρει την Router υπηρεσία για να βοηθήσει τους χρήστες του προκειμένου να ορίσουν και να διαμορφώσουν διαδρομές πλοήγησης ανάμεσα στις προβολές. Φυσικά αξίζει να τονιστεί ότι ο δρομολογητής προσφέρει προηγμένες δυνατότητες πλοήγησης στο πρόγραμμα περιήγησης. Οι καινοτομίες πάντως που προσφέρει προς αυτήν την κατεύθυνση το Angular θα παρουσιαστούν αναλυτικά αμέσως παρακάτω (Angular, 2020).

3.2.6 Πλοήγηση εντός εφαρμογής: Angular Router Ng Module

Επιπλέον, όπως αναφέρθηκε παραπάνω, πολύ μεγάλο ενδιαφέρον προκαλεί η περίπτωση του Angular Router Ng Module, όπου παρέχεται μια υπηρεσία που επιτρέπει στους χρήστες να δρομολογούν μια διαδρομή πλοήγησης που σχετίζονται με τις διάφορες καταστάσεις εφαρμογής. Πιο συγκεκριμένα, ο χρήστης εισάγει μια διεύθυνση URL στη γραμμή περιήγησης, ενώ παράλληλα το πρόγραμμα της περιήγησης κάνει μετάβαση σε μια σελίδα. Εν συνεχεία, ο χρήστης επιλέγει τον σύνδεσμο και τη σελίδα που επιθυμεί και αμέσως μετά το πρόγραμμα περιήγησης λαμβάνει εντολή και μεταβαίνει σε μια καινούργια σελίδα. Τέλος, ο χρήστης μπορεί να επιλέγει τα κουμπιά μπροστά και πίσω έτσι όπως αποτυπώνονται στο πρόγραμμα περιήγησης και αυτό στη συνέχεια πραγματοποιεί μια γρήγορη μετάβαση στο ιστορικό των σελίδων που έχει επισκεφτεί ο χρήστης επιλέγοντας "Πίσω" ή "Εμπρός" (Angular, 2020).

3.2.7 Πλατφόρμα ανάπτυξης λογισμικού: NODE . JS

Τέλος, ένα ακόμη πρόγραμμα που χρησιμοποιήθηκε στη συγκεκριμένη μελέτη και έχει σχέση με το Javascript είναι το Node.js, τα χαρακτηριστικά του οποίου καθώς και η λειτουργικότητά του εμφανίστηκαν έντονα το έτος 2009. Ουσιαστικά πρόκειται για έναν κόμβο, ο οποίος προσφέρει ένα τεράστιο πλεονέκτημα στους προγραμματιστές, καθώς τους δίνει τη δυνατότητα να γράφουν κώδικα Javascript, ο οποίος πραγματοποιείται αμέσως σε μια διαδικασία υπολογιστή, χωρίς να απαιτείται η χρήση ενός προγράμματος περιήγησης. Έτσι λοιπόν, από τα παραπάνω γίνεται εύκολα αντιληπτό το γεγονός ότι αυτός ο κόμβος χρησιμοποιείται για να εγγράψει διάφορες εφαρμογές από τον διακομιστή με πρόσβαση στο σύστημα λειτουργίας ή ακόμη και στο σύστημα αρχείων, προκειμένου να ολοκληρωθεί η διαδικασία της κατασκευής των λειτουργικών εφαρμογών. Όσον αφορά σε κάποια ακόμη χαρακτηριστικά αυτού του προγράμματος είναι ότι κόμβος διαθέτει πολλές ενσωματωμένες λειτουργικές μονάδες για την αλληλεπίδραση με τη γραμμή εντολών, το σύστημα αρχείων του υπολογιστή και το Διαδίκτυο. Τα στοιχεία που περιλαμβάνουν είναι το HTTP και το HTTPS που σχετίζονται με τη δημιουργία των διακομιστών ιστού. Επίσης, συναντάμε το σύστημα αρχείων, όπως επίσης και το λειτουργικό σύστημα καθώς και τη διαδρομή, που σχετίζονται με την αλληλεπίδραση που παρατηρείται ανάμεσα στο

σύστημα αρχείων, το λειτουργικό σύστημα και τις διαδρομές αρχείων / καταλόγων (Tutorial Spoint, 2020).

Επιπροσθέτως, στο σημείο αυτό θα γίνει μια προσπάθεια αξιολόγησης της επιλογής του συγκεκριμένου κόμβου. Πιο συγκεκριμένα, ο κόμβος διαθέτει ένα μοντέλο εισόδου και εξόδου το οποίο βασίζεται σε διάφορα συμβάντα χωρίς να παρατηρείται το ενδεχόμενο αποκλεισμού. Αυτό σημαίνει ότι ο κόμβος είναι καλά σχεδιασμένος για να χειρίζεται ασύγχρονο κώδικα JavaScript για να μπορεί να εκτελεί πολλές ασύγχρονες δραστηριότητες, όπως για παράδειγμα ανάγνωση και εγγραφή στο σύστημα αρχείων, χειρισμός συνδέσεων σε διακομιστές βάσης δεδομένων ή χειρισμός αιτημάτων ως διακομιστής ιστού (Tutorial Spoint, 2020).

Για να επιτευχθεί ο χειρισμός του ασύγχρονου κώδικα, το Node χρησιμοποιεί ένα σύστημα που βασίζεται σε επιστροφή κλήσεων. Ειδικότερα, οι λειτουργίες κόμβου αλλά και οι μέθοδοι που θα εφαρμόσουν την ασύγχρονη δραστηριότητα λαμβάνουν μια συνάρτηση επανάκτησης. Αυτή η επιστροφή κλήσης θα κληθεί όποτε έχει επιλυθεί η ασύγχρονη λειτουργία. Έτσι λοιπόν, το πρώτο επιχείρημα αυτής της επανάκτησης είναι ένα σύμβολο κράτησης θέσης σφάλματος. Εάν παρουσιαστεί σφάλμα στην ασύγχρονη λειτουργία τότε το όρισμα σφάλματος θα είναι αντικείμενο σφάλματος, αλλά θα συμβεί null εάν δεν παρουσιαστεί σφάλμα. Ενδεικτικά αναφέρεται το παράδειγμα στην περίπτωση που θα προσπαθήσει να διαβάσει μια μορφή αρχείου που ουσιαστικά δεν υπάρχει (Codecademy, 2019).

Τέλος, στο σημείο αυτό αξίζει να υπογραμμιστεί και το γεγονός ότι το Node.js είναι γραμμένο στη γλώσσα C ++, καθώς και στη Javascript, ενώ έχει ενσωματωθεί στη μηχανή Javascript ανοιχτού κώδικα V8, η οποία με τη σειρά της τροφοδοτεί το JS σε διάφορα προγράμματα περιήγησης, όπως για παράδειγμα το γνωστό σε όλους Google Chrome (Codecademy, 2019).

4^0 Κεφάλαιο: Αποτελέσματα

Όπως εύκολα μπορεί να παρατηρήσει κανείς, η συγκεκριμένη εφαρμογή αποτελείται από το κεντρικό μενού που περιέχει τις ακόλουθες επιλογές: Home, Active campaigns, Campaign Management, Calendar και Login.

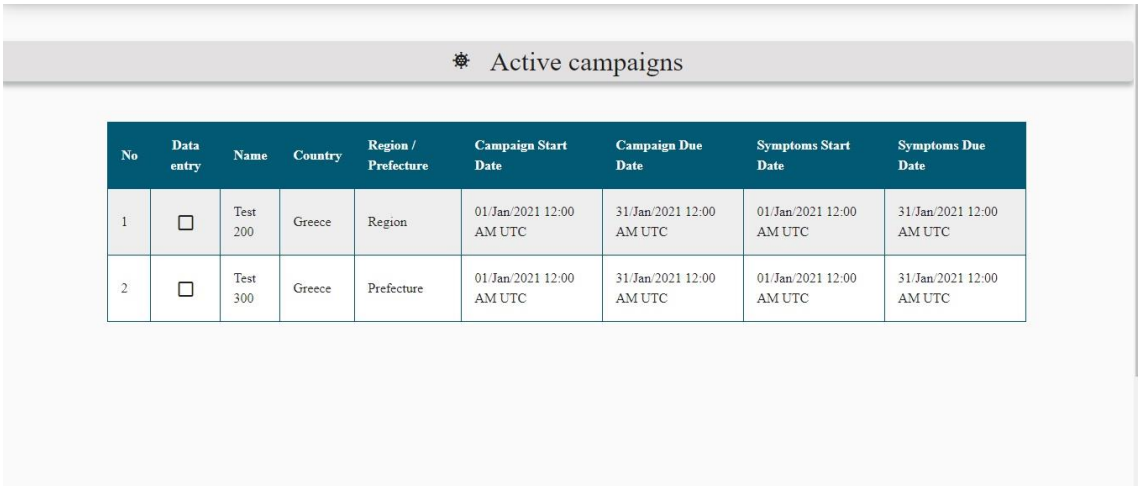
4.1 Αρχική οθόνη - Home

Στο κεντρικό μενού η πρώτη επιλογή είναι το Home (Εικόνα 1 Home), όπου είναι η πρώτη σελίδα εισαγωγή στην εφαρμογή, ενώ παράλληλα δίνεται η έναρξη πρόσβασης στην εφαρμογή.

Εικόνα 1 Home

4.2 Οθόνη Active campaigns

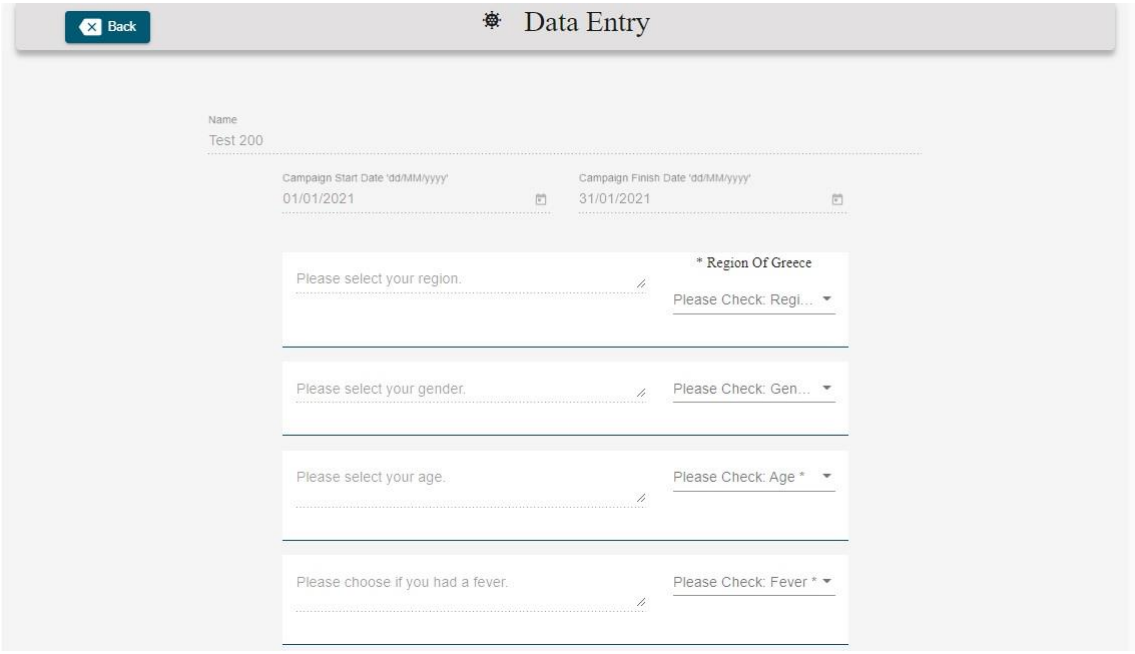
Στη συνέχεια ο χρήστης μπορεί να επισκεφτεί το δεύτερο σύνδεσμο της εφαρμογής που είναι το Active Campaigns (Εικόνα 2 Active campaigns). Η συγκεκριμένη επιλογή οδηγεί στην προβολή ενός πίνακα, ο οποίος περιλαμβάνει τα στοιχεία που σχετίζονται με τις ενεργές καμπάνιες συλλογής δεδομένων, τα διαστήματα που τρέχουν και τα διαστήματα που αφορά η συλλογή δεδομένων σε αυτές. Στο πίνακα με τις διαθέσιμες καμπάνιες υπάρχει επίσης σε κάθε καμπάνια το κουμπί Data entry που επιτρέπει στον χρήστη την συμμετοχή στην καμπάνια.



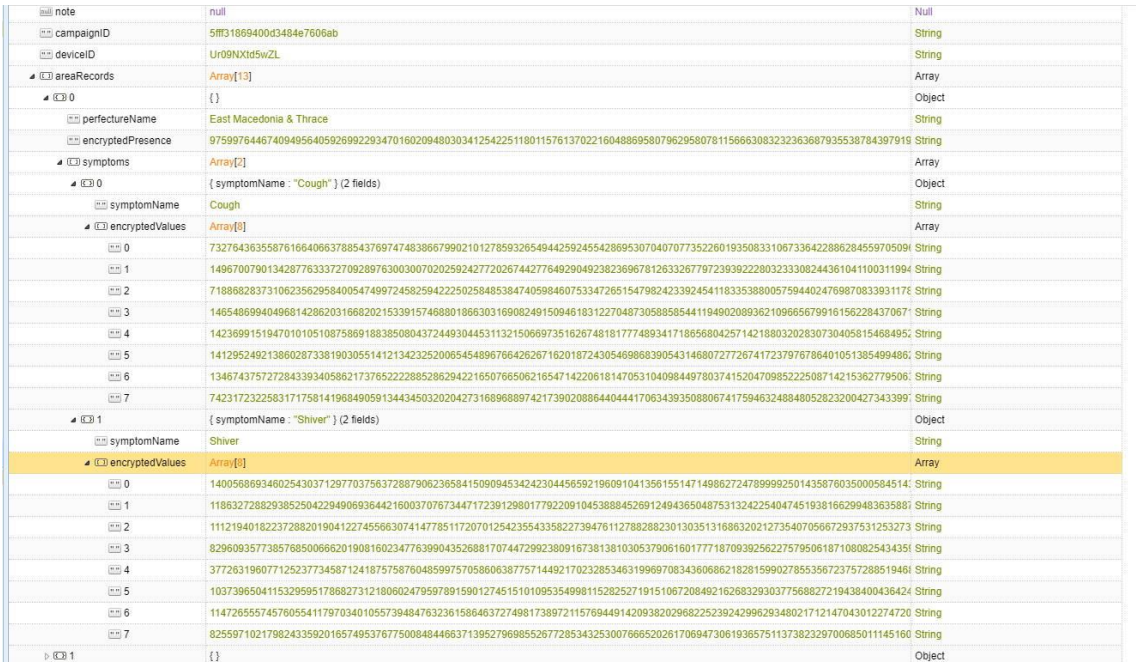
Εικόνα 2 Active campaigns

Επιλέγοντας αυτή την επιλογή (Εικόνα 3 Data Entry), ο χρήστης έχει την δυνατότητα να επιλέξει την περιοχή που βρισκόταν τις ημερομηνίες που αφορά η καμπάνια, το φύλο, την ηλικιακή ομάδα, και αν είχε τα συμπτώματα που αναφέρονται. Κατά την αποθήκευση της απάντησης για την κάθε καμπάνια, όλες οι τιμές που ο χρήστης έχει επιλέξει κωδικοποιούνται σε κατάλληλη διανυσματική μορφή, κρυπτογραφούνται και αποθηκεύονται σε κρυπτογραφημένη μορφή (Εικόνα 4 MongoDB). Με αυτό το τρόπο προστατεύονται τα προσωπικά δεδομένα των συμμετεχόντων.

Κατά την υποβολή των μετρήσεων από τους συμμετέχοντες, υποβάλλεται ένα κρυπτογραφημένο διάνυσμα ανά περιοχή που αφορά η καμπάνια, ώστε με τον τρόπο αυτό να μην αποκαλύπτεται για ποιά περιοχή υποβλήθηκαν τα στοιχεία από τον χρήστη. Το διάνυσμα αυτό αποτελείται από



Εικόνα 3 Data Entry

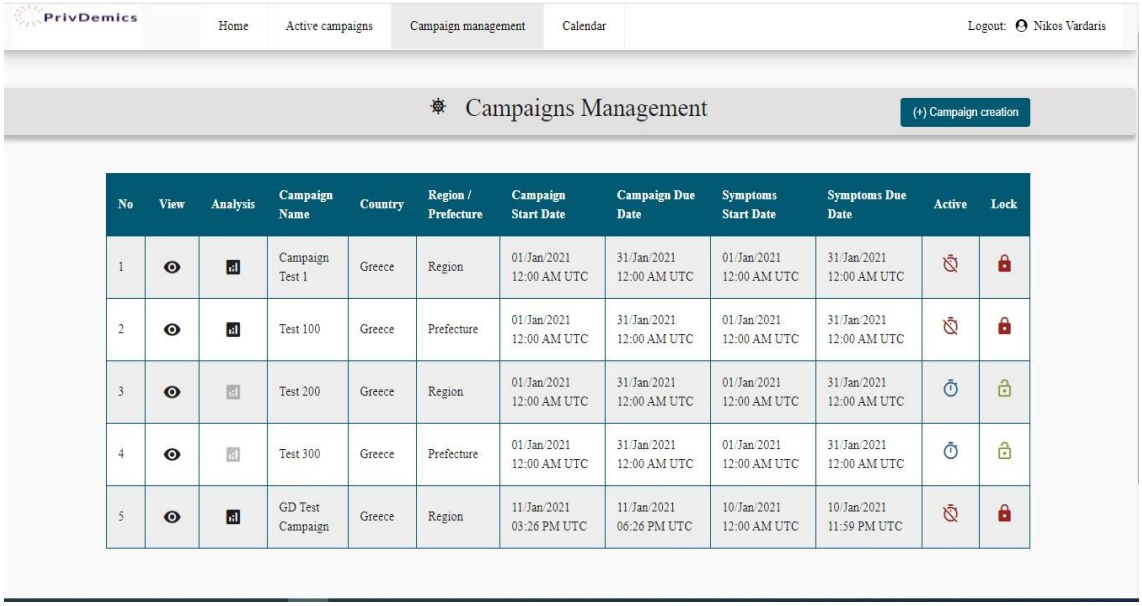


Εικόνα 4 MongoDB

4.3 Οθόνη Campaign Management

Επιπροσθέτως, στο μενού της εφαρμογής υπάρχει η επιλογή Campaign Management (Εικόνα 5 Campaign management). Στην προκειμένη περίπτωση καταγράφονται στοιχεία που δηλώνουν όλες τις διαθέσιμες καμπάνιες που είναι ενεργές. Πιο συγκεκριμένα, αναφέρεται το όνομα της κάθε καμπάνιας, όπως επίσης και η χώρα. Επίσης, η συγκεκριμένη σελίδα περιλαμβάνει και επιλογές οι οποίες σχετίζονται με την ημερομηνία έναρξης και λήξης των συμπτωμάτων από τον ιό όπου μελετάμε. Τέλος, στο δεξί μέρος της εικόνας μπορεί κανείς να αντικρίσει την επιλογή «Lock», όπου το σύμβολο της κόκκινης κλειδαριάς δηλώνει ότι η καμπάνια είναι κλειδωμένη, ενώ το σύμβολο της πράσινης ανοιχτής κλειδαριάς δηλώνει ότι η συγκεκριμένη επιλογή είναι διαθέσιμη από τους χρήστες της εφαρμογής.

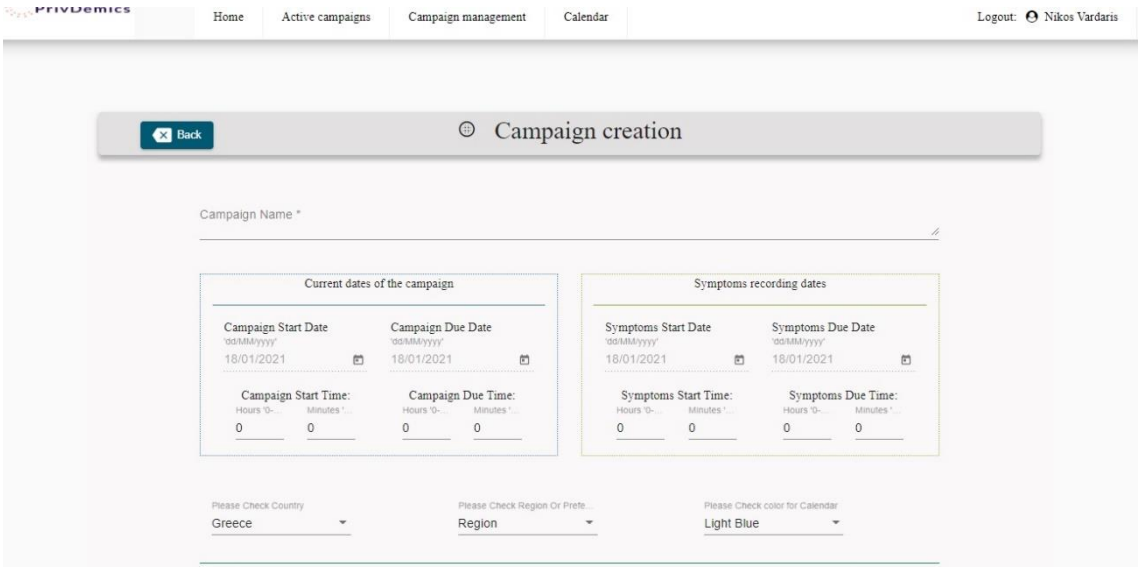
Επιπροσθέτως, ο χρήστης της συγκεκριμένης οθόνης μπορεί να προβεί σε μια επιλογή, η οποία βρίσκεται επάνω και δεξιά και πιο συγκεκριμένα στον σύνδεσμο Campaign creation.



Εικόνα 5 Campaign management

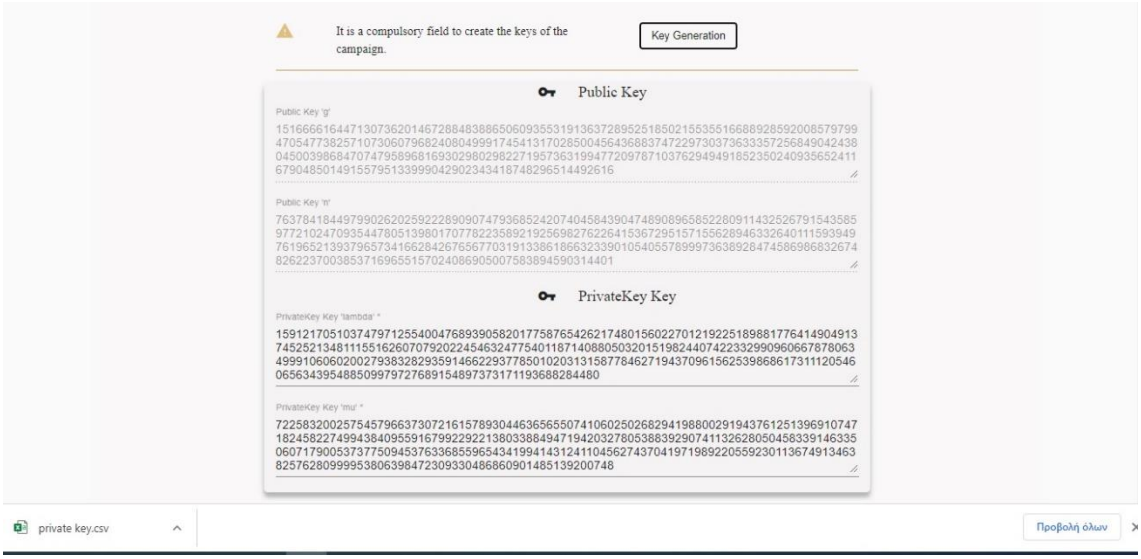
Η συγκεκριμένη επιλογή επιτρέπει τη δημιουργία μιας καμπάνιας (Εικόνα 6 Campaign creation), η οποία αποτελείται από αρκετά στοιχεία που σχετίζονται με ημερομηνία έναρξης και λήξης της καμπάνια αλλά και την έναρξη και λήξη για το συγκεκριμένο διάστημα όπου μελετάμε. Υπάρχει η δυνατότητα να επιλέξει για ποια χώρα θέλουμε να τρέξει η καμπάνια, για το αν θα αναφέρεται σε περιφέρεια ή νομό και τέλος,

μπορεί να επιλέξει τουλάχιστον ένα σύμπτωμα από τα έξι που υπάρχουν ή και όλα μαζί όπου θα πάρει μέρος για την έρευνα που θα πραγματοποιηθεί.



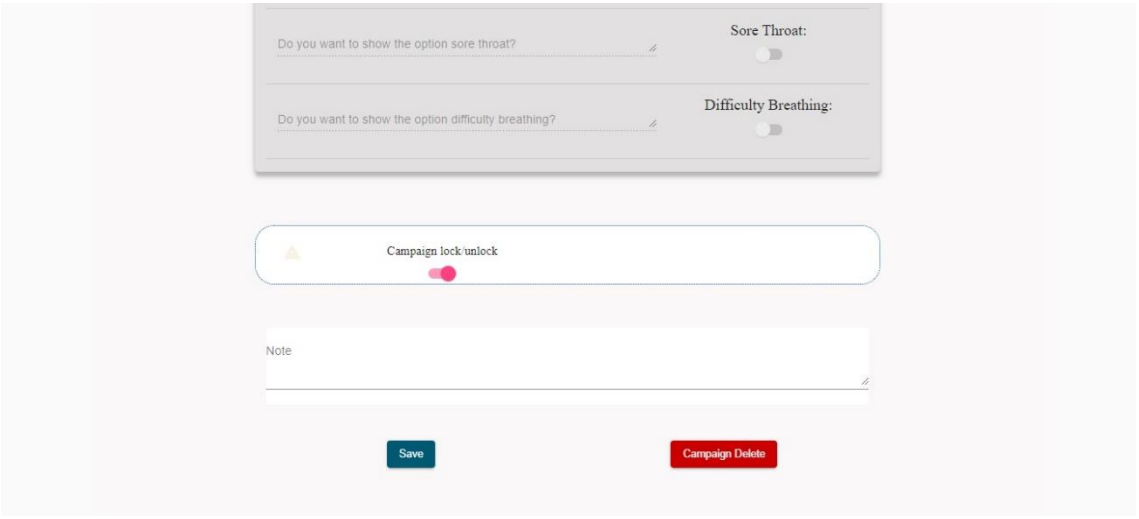
Εικόνα 6 Campaign creation

Αμέσως πιο κάτω υπάρχει ένα κουμπί με όνομα «Key Generetion» (Εικόνα 7 Public Keu – PrivateKey Key) όπου επιλέγοντας το κουμπί δημιουργείται τυχαία το Public Key – PrivateKey Key για το κρυπτοσύστημα Paillier και αμέσως γίνεται λήψη ένα αρχείο τύπου csv όπου μέσα περιέχει το όνομα της καμπάνιας και το Private Key. Επιλέγοντας Save τότε η καμπάνια που έχουμε δημιουργήσει κρατάει μόνο το Public Key.



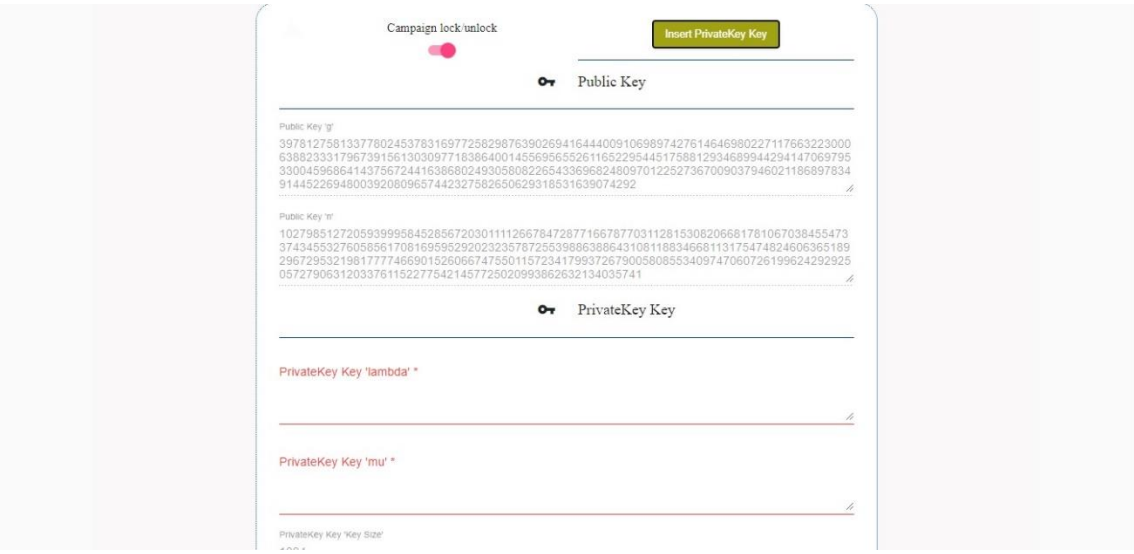
Εικόνα 7 Public Keu – PrivateKey Key

Επιπλέον, αν ο χρήστης επιθυμεί να κλειδώσει την καμπάνια τότε επιλέγει την επιλογή View. Στην σελίδα που θα μας ανοίξει υπάρχει η επιλογή Campaign lock/unlock (Εικόνα 8 Campaign lock), με αυτό το τρόπο κλειδώνει η καμπάνια και αφού επιλέξουμε Save ο χρήστης μεταφέρεται στη λίστα με τις διαθέσιμες καμπάνιες.



Εικόνα 8 Campaign lock

Αφού έχει κλειδωθεί η καμπάνια τότε ο χρήστης έχει τη δυνατότητα να προχωρήσει στην ανάλυση των αποτελεσμάτων. Αυτή η διαδικασία πραγματοποιείται μέσα από την επιλογή View η οποία φορτώνει τα στοιχεία της συγκεκριμένης καμπάνιας. Στο κάτω μέρος της οθόνης υπάρχει ένα κουμπί με όνομα Insert Private Key (Εικόνα 9 Campaign Insert PrivateKey Key). Σε αυτό το σημείο ο χρήστης εισάγει το PrivateKey της συγκεκριμένης καμπάνιας και στη συνέχεια επιλέγει το κουμπί Start the calculations. Επιλέγοντας το κουμπί αυτό πραγματοποιείται η άθροιση των κρυπτογραφημένων διανυσμάτων που έχουν καταχωρηθεί για τη συγκεκριμένη καμπάνια και η αποκρυπτογράφηση των συγκεντρωτικών αποτελεσμάτων.

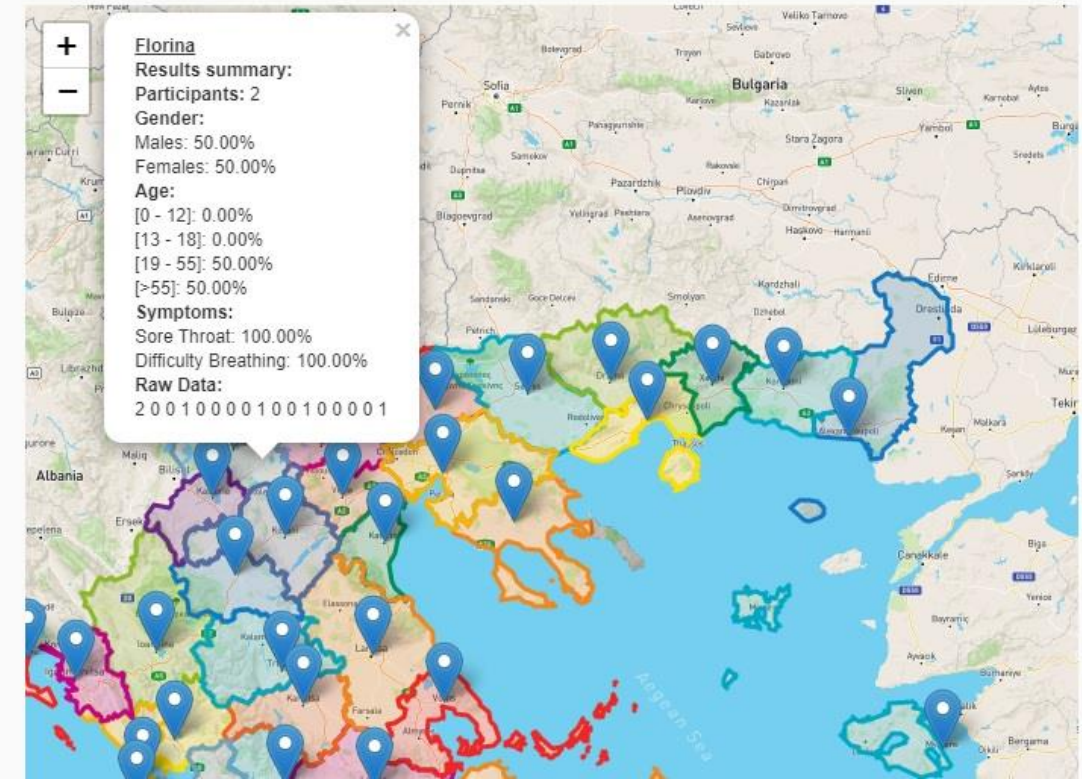


Εικόνα 9 Campaign Insert Private Key

4.4 Οθόνη Campaign Analysis

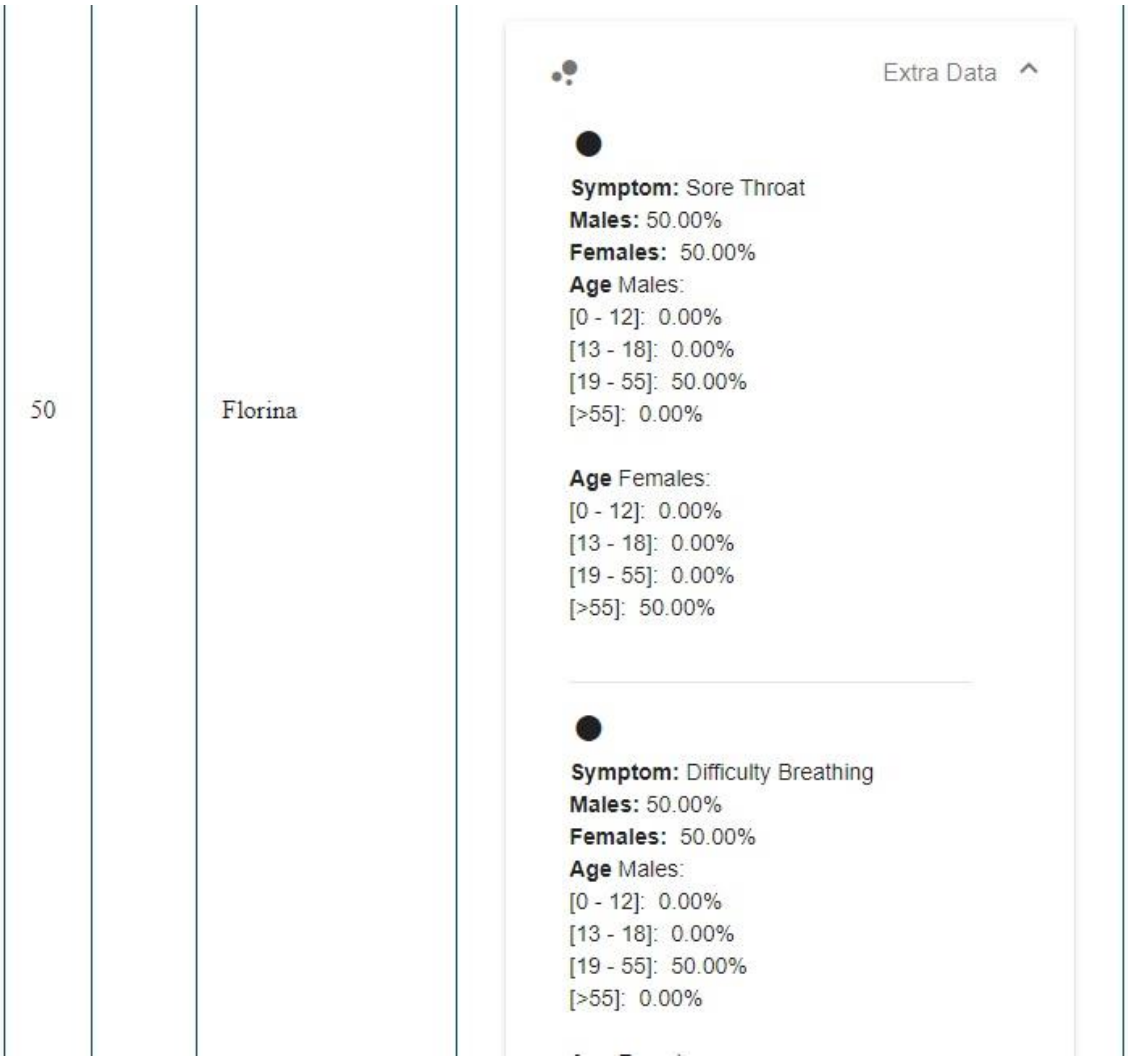
Αφού ολοκληρωθεί η διεργασία του υπολογισμού των αποτελεσμάτων, ενεργοποιείται στο μενού Campaign Management το κουμπί Analysis. Αυτή η επιλογή εμφανίζει τη σελίδα της ανάλυσης αποτελεσμάτων της καμπάνιας, όπου τα υπολογισμένα συγκεντρωτικά αποτελέσματα εμφανίζονται δυναμικά σε χάρτη (Εικόνα 10 Map Analysis). Κάνοντας κλικ σε ένα νομό ή περιφέρεια εμφανίζονται τα στατιστικά δεδομένα για την επιλεγμένη περιοχή.

Date	Date	Date	Date
01/Jan/2021 12:00 AM UTC	31/Jan/2021 12:00 AM UTC	01/Jan/2021 12:00 AM UTC	31/Jan/2021 12:00 AM UT



Εικόνα 10 Map Analysis

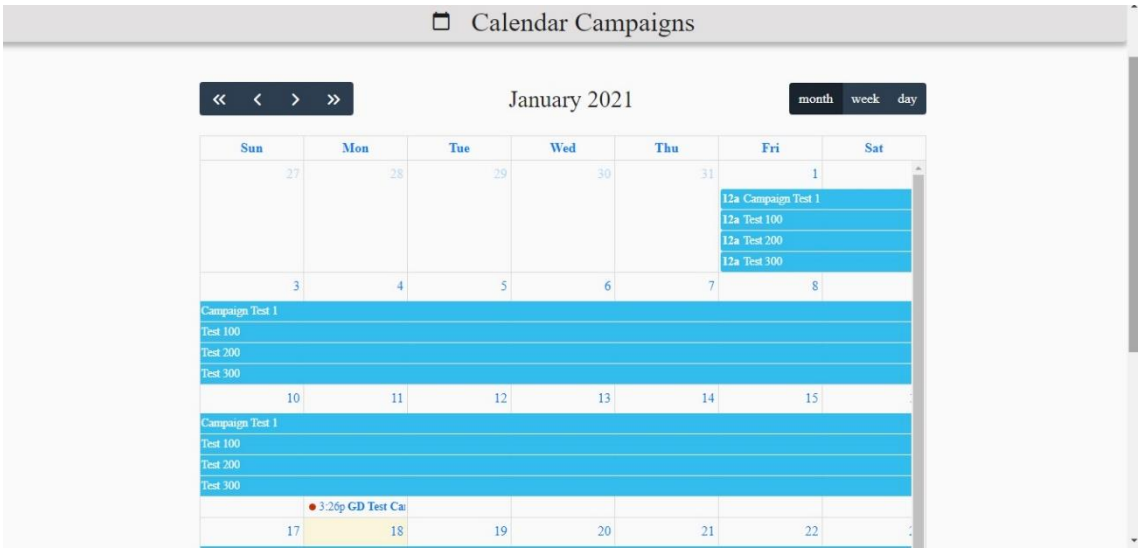
Κάτω από την εμφάνιση του χάρτη υπάρχει ένας πίνακας (Εικόνα 11 Analysis) που έχει όλες τις περιοχές της καμπάνιας και όλα τα στατιστικά δεδομένα ξεχωριστά, σε συνοπτική και αναλυτική μορφή.



Εικόνα 11 Analysis

4.5 Οθόνη Calendar

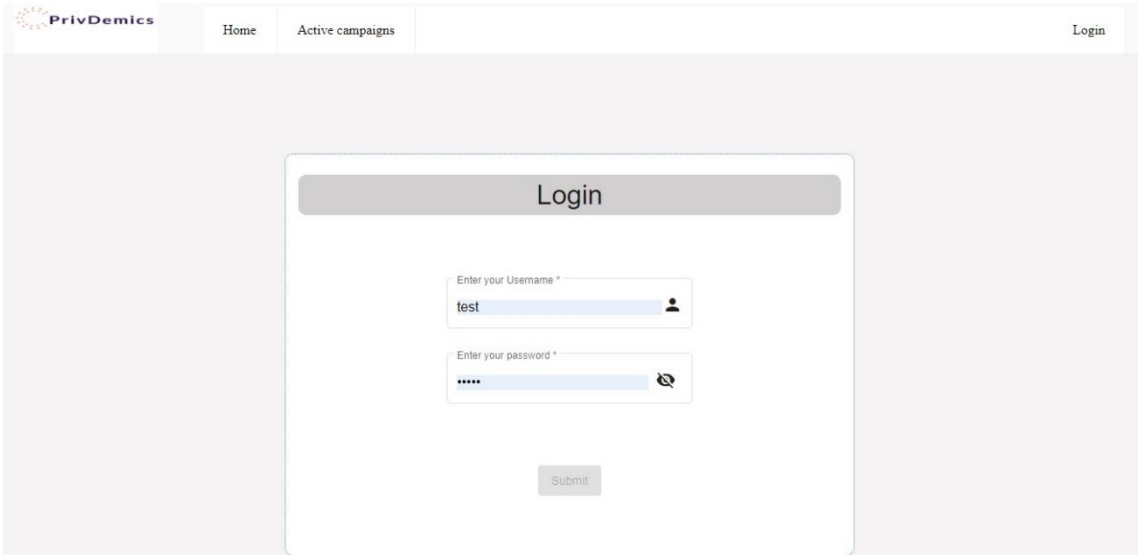
Στην οθόνη Calendar (Εικόνα 12 Calendar) εμφανίζονται οι καμπάνιες σε ημορολόγιο με επιλογή μορφής μήνα ή εβδομάδας ή ημέρας, όπου εμφανίζεται η αρχή και το τέλος από τις καμπάνιες.



Εικόνα 12 Calendar

4.6 Οθόνη Login/Logout

Τέλος, στο κεντρικό μενού υπάρχει η επιλογή σύνδεσης στο σύστημα Login (Εικόνα 13 Login) όπου αν κάποιος έχει δικαιώματα σύνδεσης στο σύστημα μπορεί να διαχειριστεί τις καμπάνιες.



Εικόνα 13 Login

5^0 Κεφάλαιο: Συμπεράσματα

Στην εργασία αυτή, με χρήση σύγχρονών μεθόδων ανάπτυξης λογισμικού και τεχνολογιών προστασίας προσωπικών δεδομένων, αναπτύχθηκε διαδικτυακή πλατφόρμα – εφαρμογή η οποία έδωσε τη δυνατότητα συλλογής δεδομένων εμφάνισης συμπτωμάτων από συμμετέχοντες-εθελοντές, με σκοπό την επεξεργασία των δεδομένων αυτών για την εξαγωγή συμπερασμάτων σχετικά με την εξέλιξη μίας επιδημίας ή πανδημίας, με εφαρμογή στην περίπτωση του ιού COVID-19. Η εν λόγω εφαρμογή αποτελεί ένα πολύ χρήσιμο εργαλείο, διότι μέσα από τις καινοτόμες επιλογές της, δίνει τη δυνατότητα στους χρήστες της να παρακολουθήσουν τη γεωγραφική διασπορά των συμπτωμάτων που σχετίζονται με την εκάστοτε επιδημία, προστατεύοντας ταυτόχρονα την ιδιωτικότητα των συμμετεχόντων. Με αυτόν λοιπόν τον τρόπο παρέχεται η δυνατότητα της άμεση καταγραφής και απεικόνισης των επιδημιολογικών δεδομένων και την εξαγωγή συμπερασμάτων για την αποτελεσματικότερη αντιμετώπιση των εξελίξεων.

Βιβλιογραφία

Αραμπατζής, Α., 2020. Διαθέσιμο σε: https://www.homodigitalis.gr/posts/5200 (Ανακτήθηκε 12 Μάρτιος 2020).

Angular, 2020. *Angular.* Διαθέσιμο σε: https://angular.io/guide/architecture (Ανακτήθηκε 3 Δεκέμβριος 2020).

Bogetoft, P. και συν., 2009. *'Secure multiparty computation goeslive,' in Financial Cryptography and Data Security.* Berlin: Heidelberg: Springer-Verlag.

CLARK, W., 2020. *Open Mined.* Διαθέσιμο σε: https://blog.openmined.org/the-paillier-cryptosystem/
(Ανακτήθηκε 9 ιούλιος 2020).

Codecademy, 2019. *Codecademy.* Διαθέσιμο σε: https://www.codecademy.com/articles/what-is-node
(Ανακτήθηκε 11 Δεκέμβριος 2020).

Damgård, I., Jurik, M. & Nielsen, J. B., 2010. A generalization of Paillier's public-key system with applications to electronic voting. *International Journal of Information Security volume*, 9 Ιούλιος, p. 371–385.

Daylighting Society, 2017. *Daylighting Society.* Διαθέσιμο σε: https://paillier.daylightingsociety.org/about
(Ανακτήθηκε 10 Δεκέμβριος 2020).

Drosatos, G., Efraimidis, P. S., Athanasiadis, I. N. & Stevens, M., 2017. 'Privacy-preserving computation of participatory noisemaps in the cloud,' Journal of Systems and Software. Τόμος 92, p. 170–183.

Drosatos, G., Tasidou, A. & Efraimidis, P. S., 2017. 'Privacy-enhancedtelevision audience measurements', ACM Transactions on Internet Technolog. Τόμος 17.

Karlof, C., Sastry, N. & Wagner, D., 2005. *Cryptographic Voting Protocols: A Systems Perspective.* USA Berkeley: USENIX.

Krukowski, B., 2018. *Sitepoint.* Διαθέσιμο σε: https://www.sitepoint.com/angular-introduction/
(Ανακτήθηκε 10 Δεκέμβριος 2020).

MDN, C., 2020. *Developer Mozilla.* Διαθέσιμο σε: https://developer.mozilla.org/en-US/docs/Learn/JavaScript/First_steps/What_is_JavaScript
(Ανακτήθηκε 10 Δεκέμβριος 2020).

Mongo DB, 2020. *Mongo DB.* Διαθέσιμο σε: https://www.mongodb.com/what-is-mongodb
(Ανακτήθηκε 2 Δεκέμβριος 2020).

Rouse, M., 2020. *SearchDataManagement - TechTarget.* Διαθέσιμο σε: https://searchdatamanagement.techtarget.com/definition/MongoDB
(Ανακτήθηκε 5 Δεκέμβριος 2020).

Schaefer , L., 2020. *Mongo DB.* Διαθέσιμο σε: https://www.mongodb.com/nosql-explained
(Ανακτήθηκε 28 Νοέμβριος 2020).

Schaefer, L., 2019. *Mongo DB.* Διαθέσιμο σε: https://www.mongodb.com/nosql-explained/nosql-vs-sql
(Ανακτήθηκε 29 Νοέμβριος 2020).

Shi, J., Zhang, R., Liu, Y. & Zhang, Y., 2010. *'PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems', in Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM '10).* USA: IEEE.

Stackify, 2020. *Stackify.* Διαθέσιμο σε: https://stackify.com/what-is-c-used-for/
(Ανακτήθηκε 14 Δεκέμβριος 2020).

Tutorial Spoint, 2020. *Tutorial Spoint.* Διαθέσιμο σε: https://www.tutorialspoint.com/nodejs/nodejs_introduction.htm
(Ανακτήθηκε 9 Δεκέμβριος 2020).

Yao, A. C., 1982. *"Protocols for secure computations," in IEEE 54th AnnualSymposium on Foundations of Computer Science.IEEE.* USA: IEEE.