ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΓΕΣ ΣΤΗ ΒΙΟΪΑΤΡΙΚΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΒΕΛΤΙΩΣΗ ΤΗΣ ΠΡΟΒΛΕΨΗΣ ΤΗΣ ΠΙΘΑΝΟΤΗΤΑΣ ΑΣΘΕΝΕΙΑΣ ΜΕ ΤΗ ΧΡΗΣΗ WEARABLE SENSORS ΚΑΙ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΜΕΤΡΗΣΕΩΝ, ΜΕΣΩ SECURE MULTI-PARTY COMPUTATION

ΕΜΜΑΝΟΥΗΛΙΑ ΒΑΣΙΛΕΙΑΔΟΥ

ΛΑΜΙΑ

ΜΑΪΟΣ 2018

ΠΤΥΧΙΑΚΗΕΡΓΑΣΙΑ

Βελτίωση της πρόβλεψης της πιθανότητας ασθένειας με τη χρήση wearable sensors και την ανταλλαγή μετρήσεων, μέσω Secure Multi-party Computation

Εμμανουηλία Βασιλειάδου

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

Γεώργιος Σπαθούλας

Μέλος ΕΔΙΠ, Πανεπιστήμιο Θεσσαλίας

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

Γεώργιος Σπαθούλας

Μέλος ΕΔΙΠ, Πανεπιστήμιο Θεσσαλίας

Αθανάσιος Κακαρούντας

Επίκουρος Καθηγητής, Πανεπιστήμιο Θεσσαλίας

Ιωάννης Τριανταφύλλου

Επίκουρος Καθηγητής, Πανεπιστήμιο Θεσσαλίας

Ημερομηνία Εξέτασης: 23 Μαΐου 2018

ΠΕΡΙΛΗΨΗ

Οι φορητές συσκευές μέτρησης βιοσημάτων αποτελούν ένα σημαντικό εργαλείο τόσο για την αξιολόγηση της φυσικής κατάστασης, όσο και για την πρόβλεψη κλινικών επεισοδίων. Επίσης, ορισμένες λειτουργίες που παρέχουν οι φορητές συσκευές σχετίζονται με την αναγνώριση και την ασφάλεια. Η συγκεκριμένη εργασία προτείνει μια εφαρμογή, με σκοπό τη βελτίωση της πρόβλεψης της πιθανότητας ασθένειας. Για την επίτευξη του σκοπού αυτού κρίνεται αναγκαία η χρήση φορητών συσκευών με αισθητήρες από μια ομάδα ανθρώπων. Η κάθε συσκευή θα πραγματοποιεί μετρήσεις, τις οποίες οι χρήστες θα ανταλλάσσουν μεταξύ τους, μέσω Secure Multi-party Computation προστατεύοντας έτσι τα προσωπικά τους δεδομένα.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Φορητές Συσκευές, Παρακολούθηση Υγείας, Ασφαλείς Υπολογισμοί.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Δίκτυο Πραγμάτων, Αισθητήρες, BITalino, Πρόβλεψη Ασθένειας, Προστασία Δεδομένων.

ABSTRACT

Wearable devices that measure biosignals are an important tool not only to assess physical fitness, but also to prevent clinical episodes. Also, some additional capabilities of wearable devices are related to identification and security. This work proposes an application to improve the prediction of the possibility of illness. In order to achieve this goal, it is necessary the use of portable sensing devices from a group of people. Each device will perform measurements that users will transmit through Secure Multi-Party Computation, thereby protecting their personal data.

SUBJECT AREA: Wearable Devices, Health Monitoring, Secure Multi-party Computation.

KEYWORDS: Internet of Things, Sensors, BITalino, Predicting Illness, Data Security.

Στην οικογένειά μου.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον επιβλέποντα της πτυχιακής μου εργασίας, διδάσκοντα κ. Γεώργιο Σπαθούλα κυρίως για την εμπιστοσύνη που μου έδειξε, αλλά και το χρόνο που διέθεσε για τη διεκπεραίωση της πτυχιακής εργασίας. Οι προτάσεις του βελτίωσαν με ακρίβεια το περιεχόμενο, την οργάνωση, την αναγνωσιμότητα και τη συνολική ποιότητα αυτής της εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική που είχα όλα αυτά τα χρόνια της ακαδημαϊκής μου ζωής, για τις γνώσεις που μου μετέδωσαν και τα κατάλληλα κίνητρα που μου έδωσαν για να φθάσω σε αυτό το στάδιο παρουσίασης της πτυχιακής μου εργασίας.

Ευχαριστώ τους συμφοιτητές και τις συμφοιτήτριές μου, για την αλληλοϋποστήριξη και τη συμπαράσταση τους σε αυτό το κοινό ταξίδι.

Και τέλος, θέλω να εκφράσω ένα τεράστιο ευχαριστώ στην οικογένειά μου, για όλα όσα μου πρόσφεραν και μου προσφέρουν, για την αγάπη τους και την πίστη τους σε εμένα, δίνοντάς μου κουράγιο να φτάσω στο στόχο μου.

Βασιλειάδου Εμμανουηλία

ΥΠΕΥΘΗΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΛΟΓΟΚΛΟΠΗΣ

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Ακόμα δηλώνω ότι αυτή η γραπτή εργασία προετοιμάστηκε από εμένα προσωπικά και αποκλειστικά και ειδικά για την συγκεκριμένη πτυχιακή εργασία και ότι θα αναλάβω πλήρως τις συνέπειες εάν η εργασία αυτή αποδειχθεί ότι δεν μου ανήκει.

Εμμανουηλία

Βασιλειάδου

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Η παρούσα πτυχιακή εργασία αφορά τη βελτίωση της πρόβλεψης της πιθανότητας ασθένειας με τη χρήση wearable sensors και την ανταλλαγή μετρήσεων, μέσω Secure Multi-party Computation. Η ανάπτυξη της εφαρμογής έγινε με τη χρήση της γλώσσας Java και της πλακέτας βιοσημάτων BITalino.

Το θέμα της συγκεκριμένης εργασίας συζητήθηκε και αναπτύχθηκε μαζί με τον επιβλέποντα καθηγητή κ. Γεώργιο Σπαθούλα. Στα παρακάτω κεφάλαια θα παρουσιαστεί λεπτομερώς η ανάπτυξη της εφαρμογής, θα αναλυθεί ο κώδικας και η χρήση του SMC με σκοπό τη σωστή χρήση και την προστασία των προσωπικών πληροφοριών.

Σαφώς, η μελέτη και η συγγραφή της πτυχιακής μου εργασίας στηρίχθηκε σε επιστημονικά κείμενα, άρθρα και εργασίες. Ωστόσο, οποιαδήποτε χρήση πηγών και πληροφοριών έχει αναφερθεί στη βιβλιογραφία.

1.ΕΙΣΑΓΩΓΗ

Η μέτρηση των βιολογικών σημάτων είναι ένα σημαντικό εργαλείο όχι μόνο για την αξιολόγηση της φυσικής κατάστασης, αλλά και για την πρόληψη ή/και την πρόβλεψη κλινικών επεισοδίων [1]. Τα τελευταία χρόνια, λοιπόν, η κοινότητα Do-It-Yourself (DIY), δηλαδή καν' το-μόνος-σου, συνέβαλε στην ανάπτυξη πλατφορμών χαμηλού κόστους και εύχρηστων εφαρμογών [2] που συλλέγουν -με τη βοήθεια αισθητήρων- βιοσήματα από το χρήστη, με στόχο τη μέτρηση και την αξιολόγηση των ζωτικών στοιχείων (όπως η πίεση του αίματος, οι παλμοί ή ο καρδιακός ρυθμός).

Ένας από τους σημαντικότερους λόγους για τη συχνή μέτρηση των ζωτικών στοιχείων σε ένα υγιές άτομο, είναι ότι καθίσταται δυνατή η αξιολόγηση των φυσιολογικών παραμέτρων [1]. Με τον τρόπο αυτό, εντοπίζονται και αντιμετωπίζονται έγκαιρα τυχών ανωμαλίες.

Μία άλλη οπτική, είναι ότι η παρακολούθηση των βιοσημάτων είναι επίσης ένα σημαντικό εργαλείο για την εκτίμηση της φυσικής κατάστασης. Για παράδειγμα, ένας αθλητής μπορεί να χρησιμοποιήσει μια τέτοια εφαρμογή ή συσκευή, ώστε να βελτιώσει και να κάνει πιο αποδοτική την εκπαίδευσή του, σύμφωνα πάντα με τις προσωπικές του αναλύσεις [1].

Παράλληλα, οι απαιτήσεις των αθλητών των θαλάσσιων σπορ, προκάλεσαν τους ερευνητές και τους μηχανικούς και τους οδήγησαν στην κατασκευή μικρών φορητών συσκευών (και αντίστοιχων εφαρμογών) ανθεκτικών στο νερό. Έχοντας ως στόχο -πάντα- την απόκτηση, τη μετάδοση και την αποθήκευση δεδομένων που αφορούν τα βιολογικά σήματα του κάθε αθλητή [1].

Άλλες πιθανές εφαρμογές είναι η αναγνώριση και η αξιολόγηση των συναισθηματικών καταστάσεων, η παρακολούθηση δραστηριοτήτων ή η παρακολούθηση της αποκατάστασης από έναν τραυματισμό, καθώς και η ανάπτυξη φορητών συσκευών που αποσκοπούν στην ευημερία και στην ευεξία του ανθρώπου.

Η τεχνολογία των φορητών συσκευών (wearables) αναφέρεται συχνά ως μια από τις μεγαλύτερες εφαρμογές του Δικτύου των Πραγμάτων (Internet of Things IoT) [3]. Το Internet of Things είναι μία έννοια που αφορά τα αντικείμενα της καθημερινότητας μας (από βιομηχανικές μηχανές μέχρι wearable συσκευές) που χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και την ανάληψη κάποιας δράσης από αυτά μέσα σε ένα δίκτυο. Κάπως έτσι λειτουργεί ένα κτίριο που χρησιμοποιεί αισθητήρες (sensors) για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού. Άλλο παράδειγμα είναι ο ένας εξοπλισμός παραγωγής που προειδοποιεί το προσωπικό συντήρησης για μία επικείμενη βλάβη. Με απλά λόγια το Internet of Things είναι το τεχνολογικό μέλλον που θα κάνει τη ζωή μας πιο εύκολη [4].

Ορισμένες λειτουργίες που παρέχουν οι φορητές συσκευές σχετίζονται με την αναγνώριση και την ασφάλεια. Ένα πολύ καλό παράδειγμα είναι οι κάρτες εργασίας, οι οποίες παρέχουν χαρακτηριστικά αναγνώρισης και ασφάλειας (όπως είναι το όνομα και το επίθετο του εργαζόμενου ή ο τομέας στον οποίο απασχολείται) που είναι χρήσιμα για το εργασιακό περιβάλλον. Ορισμένες προηγμένες κάρτες περιλαμβάνουν ακόμα και κάποιες βιομετρικές δυνατότητες (όπως είναι η ενεργοποίηση δακτυλικών αποτυπωμάτων, που μόνο ο κάτοχος της κάρτας μπορεί να χρησιμοποιήσει για να ανοίξει π.χ. μια κλειδωμένη πόρτα) με σκοπό τη βελτίωση της ασφάλειας. Επιπλέον, οι κάρτες εργασίας μπορούν να περιλαμβάνουν δυνατότητες εντοπισμού θέσης, που είναι χρήσιμες σε καταστάσεις έκτακτης ανάγκης για να είναι σίγουρο, παραδείγματος χάριν, ότι το κτίριο έχει εκκενωθεί με επιτυχία [5].

Η ιστορία όμως των wearables ξεκινάει το 1961 από τους καθηγητές μαθηματικών του MIT Edward O. Thorp και Claude Shannon. Σχεδίασαν μια συσκευή χρονισμού, η οποία χωρούσε μέσα στα παπούτσια τους, για να προβλέψουν με ακρίβεια πού θα σταματήσει η μπάλα σε τροχό ρουλέτας και στη συνέχεια να μεταδώσουν τον αριθμό μέσω ραδιοκυμάτων στον παίκτη στο τραπέζι. Ο Thorp ανέφερε αύξηση κατά 44% στα νικητήρια στοιχήματα στο βιβλίο του Beat The Dealer. Στην πραγματικότητα, η στρατηγική ήταν τόσο επιτυχής που η Νεβάδα ψήφισε ένα νόμο που απαγόρευε τέτοιες μηχανές το 1985. Αρκετά χρόνια αργότερα ήρθε ο Steve Mann, ο οποίος θα ήταν πρωτοπόρος για πολλές φορητές συσκευές στην εποχή του. Το 1994 ο Mann δημιούργησε το Wearable Wireless Webcam, το οποίο χρησιμοποιούσε για να ανεβάζει εικόνες στο Διαδίκτυο. Το 2000 έφθασαν στην αγορά τα πρώτα ακουστικά Bluetooth και το 2006 η Nike και η Apple ένωσαν τις δυνάμεις τους για να δημιουργήσουν το

κατάλληλο όνομα Nike + iPod. Μια συσκευή που επιτρέπει στους δρομείς να συγχρονίζουν τις κινήσεις τους στο iPod. Το Μάιο του 2014 η Google κυκλοφόρησε τη συσκευή Google Glass, ενώ το 2015 η Fitbit κυκλοφόρησε μια δωδεκάδα φορητών συσκευών. Τέλος, η Apple, ο παγκόσμιος βασιλιάς της τεχνολογίας, κυκλοφόρησε το Apple Watch στις 24 Απριλίου 2015 [3].

Σήμερα, οι εταιρείες παράγουν μαζικές ποσότητες φορητής τεχνολογίας, αλλά παρόλα αυτά η αγορά δεν είναι υπερκορεσμένη. Η Apple έχει δημιουργήσει τρία ρολόγια, εκ των οποίων το ένα είναι σε συνεργασία με τη Nike. Τα Fitbit Blaze και Fitbit Alta έχουν λάβει θετικές κριτικές, τόσο από τους καταναλωτές όσο και από τους κριτικούς. Και τέλος, υπάρχουν τα wearables που μοιάζουν με τα παραδοσιακά ρολόγια συνδυάζοντας στιλ και λειτουργικότητα, όπως είναι το Samsung Gear S2 και το Huawei Watch.

Εκτιμάται ότι μέχρι τα τέλη του 2020 η αγορά των φορητών συσκευών θα αυξηθεί στα 162.9 εκατομμύρια μονάδες, σύμφωνα με την κορυφαία ερευνητική υπηρεσία του Business Insider. Καταλυτικό ρόλο στην αύξηση των πωλήσεων θα παίξει ο τομέας της υγειονομικής περίθαλψης. Οι ανιχνευτές άσκησης, συγκεκριμένα, χρησιμοποιούνται από τους καταναλωτές, με σκοπό την καταγραφή στατιστικών της άσκησής τους, της υγείας τους και της προόδου τους. Από την άλλη μεριά, τέτοιες συσκευές έχουν αρχίσει να χρησιμοποιούνται και από νοσοκομεία, φαρμακευτικές εταιρείες και ασφαλιστικές εταιρείες.

Παρ' όλη τη διάδοση και την εξέλιξη των συσκευών αυτών, η ακρίβεια θα παραμείνει το κορυφαίο εμπόδιο, καθώς οι κατασκευαστές θα πρέπει να εξασφαλίσουν ότι οι συσκευές αυτές μεταδίδουν σωστά δεδομένα. Και όπως πάντα, εξαιρετικά σημαντικές είναι οι ανησυχίες για την προστασία της ιδιωτικής ζωής.

Άλλα δευτερεύοντα προβλήματα που αφορούν τα smartwatches είναι ότι:

- **a.** Οι διεπαφές των Smartwatches είναι αργές. Ενώ μια γρήγορη ματιά στον καρπό είναι ένας πολύ καλός τρόπος για να ελέγξεις ποιος σε καλεί, στην πραγματικότητα η ευκολία του ρολογιού αντισταθμίζεται από την αποτελεσματικότητα του Smartphone.
- **b.** Η εξέλιξη των υλικών είναι αργή για τα wearables. Ενώ οι περισσότεροι άνθρωποι αλλάζουν το κινητό τους κάθε 1-2 χρόνια, μέχρι στιγμής η αγορές

Smartwatch έδειξαν ότι ο χρήστης μπορεί να περιμένει περισσότερο για να αλλάξει το ρολόι του. Ένα σύνηθες παράπονο είναι ότι τα ρολόγια είναι πολύ ογκώδη και μεγάλα (το εντελώς αντίθετο με τα κινητά τηλέφωνα) και οι κατασκευαστές δεν μπορούν να δημιουργήσουν τα μικρότερα και πιο λεπτά ρολόγια που οι χρήστες ζητούν.

c. Οι τιμές κατά την έναρξη της αγοράς ήταν υψηλές και οι περισσότερες προσφορές παρέμειναν πολύ ακριβές για τον τυπικό καταναλωτή. Το γεγονός αυτό έχει ως αποτέλεσμα οι άνθρωποι να βλέπουν το προϊόν αυτό ως πολυτέλεια κι όχι ως αναγκαιότητα. Η σπατάλη εκατοντάδων ευρώ σε ένα προϊόν που κάνει ότι και το κινητό τηλέφωνο (στην πραγματικότητα κάνει λιγότερα), καθιστά τους δυνητικούς καταναλωτές να μη δουν την αξία του ρολογιού [6].

Η υπόσχεση του IoT βασίζεται στη διαδεδομένη συνδεσιμότητα και όταν συνδυάζεται με μεγάλες συλλογές συνδεδεμένων συσκευών, μπορούν να προκύψουν σημαντικά οφέλη. Για παράδειγμα, θα μπορούσαν οι φορητές συσκευές να αλληλεπιδρούν με τις συσκευές άλλων. Θέλει κάποιος να μάθει αν αυτός που κάθεται κοντά του στο τρένο έχει υψηλό πυρετό; Είναι λογικό να θέλει κανείς να το γνωρίζει αυτό, αλλά και το άτομο που πάσχει από πυρετό ίσως να μη θέλει να το μεταδώσει. Ωστόσο, εάν και οι δύο χρησιμοποιούν τον ίδιο πάροχο υγειονομικής περίθαλψης ίσως αυτές οι πληροφορίες να μοιράζονται ή ίσως να ελέγχονται μέσω ενός φίλτρου έξυπνων τηλεφώνων. Τα ζητήματα ιδιωτικού απορρήτου θα εξακολουθήσουν να αποτελούν μεγάλη ανησυχία για τα επόμενα χρόνια, αλλά θα υπάρξουν τομείς όπου κάποια διαδεδομένη ανταλλαγή βιομετρικών στοιχείων θα ήταν χρήσιμη [5].

Η παρούσα πτυχιακή εργασία πραγματεύεται την ανάπτυξη μιας εφαρμογής, η οποία θα κάνει χρήση μιας τέτοιας συσκευής σε μια ομάδα ατόμων σε πραγματικό χρόνο. Το πλάνο στο οποίο βασίστηκε η υλοποίηση έχει ως εξής:

a. Οι χρήστες βρίσκονται σε κοινό χώρο.
b. Έχουν όλοι πρόσβαση σε μία όμοια πλατφόρμα και στην εφαρμογή που σχεδιάστηκε.
c. Συνδέονται με τον αισθητήρα ηλεκτροκαρδιογραφίας.
d. Πραγματοποιείται η εκκίνηση της εφαρμογής.
e. Η πλατφόρμα συλλέγει δεδομένα από τους χρήστες (καρδιακοί παλμοί).

f. Επιτυγχάνεται η σύνδεση μέσω Bluetooth της πλατφόρμας με τη συσκευή που διαθέτει την εφαρμογή.

g. Πραγματοποιείται αποστολή των δεδομένων που συλλέχθηκαν, ενώ παράλληλα τα πραγματικά δεδομένα παραμένουν κρυφά.

h. Τα δεδομένα επεξεργάζονται και αποστέλλονται σειριακά από χρήστη σε χρήστη.

i. Το τελικό επεξεργασμένο αποτέλεσμα επιστρέφεται στον πρώτο χρήστη του κύκλου.

j. Η διαδικασία επαναλαμβάνεται, με σκοπό την εξαγωγή ενός αντιπροσωπευτικού αποτελέσματος σχετικά με την κατάσταση των καρδιακών παλμών των χρηστών.

Το αποτέλεσμα μπορεί να ερμηνευθεί είτε με κλινικά αίτια είτε με συναισθηματικά. Αυτό εξαρτάται και από την παρακολούθηση της κατάστασης ή του περιβάλλοντος που βρισκόταν η ομάδα των χρηστών τη δεδομένη στιγμή. Για παράδειγμα αν οι χρήστες βρίσκονταν σε κατάσταση άγχους, οι παλμοί τους θα ανέβαιναν, με αποτέλεσμα να αναμένεται η υψηλή τελική τιμή.

Ο στόχος της παρούσας πτυχιακής είναι η πρότυπη υλοποίηση ενός συνεργατικού συστήματος, αποτελούμενο από κόμβους (wearable συσκευές) που χρησιμοποιούνται από διαφορετικούς χρήστες και βασική του λειτουργικότητα είναι η παραγωγή ασφαλέστερων εκτιμήσεων της φυσιολογικής κατάστασης των χρηστών. Σημαντικό χαρακτηριστικό του προτεινόμενου συστήματος είναι η διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων των χρηστών.

Για την ανάπτυξη του προτεινόμενου συστήματος, χρησιμοποιήθηκε το BITalino. Το BITalino είναι μία πλατφόρμα με ενσωματωμένους αισθητήρες βιομετρικών σημάτων και τα αντίστοιχα αναλογικά κανάλια τους (EMG, EDA, ECG, ACC, LUX). Για την προτεινόμενη υλοποίηση, έγινε χρήση της μέτρησης των καρδιακών παλμών, οπότε και χρησιμοποιήθηκε ο αισθητήρας ηλεκτροκαρδιογραφίας (ECG).

Καθώς δεν ήταν εφικτή η απόκτηση περισσότερων από μίας όμοιων συσκευών για την πραγματοποίηση του αρχικού πλάνου, κρίθηκε απαραίτητη η προσομοίωση της συνεργατικής λειτουργίας του συστήματος. Κατά τη διάρκεια των πειραματικών δοκιμών του συστήματος χρησιμοποιήθηκε ένας κανονικός κόμβος όπου ο χρήστης συνδέεται με το BITalino, ενώ για τους υπόλοιπους κόμβους οι τιμές του ρυθμού

των καρδιακών παλμών προσομοιώθηκαν βάση κανονικών κατανομών και των τυπικών χαρακτηριστικών του κάθε χρήστη (ηλικία και φύλλο).

Τέλος, απαραίτητο είναι να σημειωθεί και ο τρόπος με τον οποίο πραγματοποιείται η δικτυακή μετάδοση των αποτελεσμάτων μεταξύ των χρηστών. Ο σχεδιασμός και η υλοποίηση βασίστηκε στα χαρακτηριστικά της αρχιτεκτονικής Διακομιστή-Πελάτη (Server-Client). Ο κάθε κόμβος συμπεριφέρεται όπως και ένας Διακομιστής, οι υπόλοιποι κόμβοι μπορούν να του αποστείλουν ένα μήνυμα ως πελάτες ανά πάσα στιγμή.

2.ΣΧΕΤΙΚΗ ΕΡΕΥΝΑ

Στο κεφάλαιο αυτό θα παρουσιαστούν θέματα εργασιών και ερευνών που χρησιμοποιούν wearables συσκευές για την αποθήκευση, αξιολόγηση και χρήση των βιομετρικών μετρήσεων του ανθρώπου.

Το περιεχόμενο της κάθε σχετικής έρευνας που θα παρουσιαστεί, θα κατηγοριοποιηθεί σε μία από τις παρακάτω τρεις υποενότητες:

1. Η πρώτη υποενότητα αφορά το **health monitoring**. Είναι μια τεχνολογία που επιτρέπει την παρακολούθηση των φυσιολογικών παραμέτρων του ανθρώπου.
2. Στη δεύτερη υποενότητα θα παρουσιαστούν έρευνες και εργασίες σχετικές με το **biometric authentication**. Ο βιομετρικός έλεγχος ταυτότητας είναι μια διαδικασία ασφαλείας που βασίζεται στα μοναδικά βιολογικά χαρακτηριστικά ενός ατόμου για να επιβεβαιώσει την ταυτότητά του [7].
3. Και τέλος, η τρίτη υποενότητα αφορά την **ανίχνευση κίνησης/δραστηριότητας χρήστη**.

Επομένως, και τα θέματα που θα αναφερθούν, θα έχουν παρόμοιο περιεχόμενο με αυτό της παρούσας πτυχιακής εργασίας.

2.1 Health monitoring

Υπάρχουν πολλές διαθέσιμες πλατφόρμες και συσκευές, εφοδιασμένες με τους κατάλληλους αισθητήρες, οι οποίες χρησιμοποιούνται σε εφαρμογές που σχετίζονται με την παρακολούθηση της κατάστασης (είτε σωματικής είτε ψυχολογικής) του χρήστη. Παρακάτω θα παρουσιαστεί ένα δείγμα αυτών.

Η ομάδα των **Ιπποκράτης Αποστολίδης**, **Άννα Παρασκευά**, **Κωνσταντίνα Καραγκιόζη**, **Θρασύβουλος Τσιάτσος**, **Μαγδαληνή Τσολάκη** δημιούργησαν μια πρωτότυπη συσκευή βιο-ανάδρασης, η οποία αξιολογήθηκε ως προς την ευχρηστία της και τη χρησιμότητά της στη διαχείριση του άγχους των φοιτητών [8]. Όπως αναφέρεται στην εργασία, η συσκευή (Εικόνα 1) περιλαμβάνει μια πλακέτα Arduino συνδεδεμένη με δύο κυκλώματα: το κύκλωμα εφίδρωσης και το κύκλωμα καρδιακών παλμών, καθώς σε καταστάσεις άγχους παρατηρείται αύξηση της υγρασίας στο ανθρώπινο σώμα και ταχυπαλμία. Στόχος της ομάδας, λοιπόν, είναι ο εκπαιδευτής, λαμβάνοντας τις πληροφορίες από τη συσκευή, να ρυθμίσει τη συμπεριφορά του με σκοπό την ελάττωση της ανησυχίας του φοιτητή.

Ο **Τσίτογλου Κυριάκος** χρησιμοποίησε το καρδιοσυχνόμετρο Polar RS800CX (Εικόνα 2) σε καταστάσεις ηρεμίας, άσκησης και αποκατάστασης [9]. Σκοπός της έρευνάς του ήταν η αξιολόγηση της αξιοπιστίας της συσκευής. Τα συμπεράσματα στα οποία κατέληξε ήταν ότι: σε καταστάσεις ηρεμίας το Polar RS800CX αποτελεί έμπιστο εργαλείο, αλλά σε καταστάσεις άσκησης και αποκατάστασης είναι ανεπαρκές

Οι **André G. Pinto**, **Gil Dias**, **Virginie Felizardo** χρησιμοποίησαν μία συσκευή BITalino για να συλλέξουν βιοσήματα σε υγρό περιβάλλον [1]. Πιο συγκεκριμένα, συγκεντρώθηκαν τρία διαφορετικά σήματα από το αξελερόμετρο και από τους αισθητήρες ηλεκτροκαρδιογραφίας και ηλεκτρομυογραφίας κατά τη διάρκεια κολύμβησης.

Οι **Sreedhar Vineel R. Kaipu**, **Joyline G. D'sa** και **Divyesh Sachan** σχεδίασαν και κατασκεύασαν έναν εύκαμπτο αισθητήρα αγωγιμότητας δέρματος [10]. Η απόδοση του αισθητήρα επαληθεύτηκε πειραματικά με τη χρήση του BITalino. Αυτοί οι αισθητήρες είναι χρήσιμοι για την ανίχνευση της συναισθηματικής δραστηριότητας και της παρακολούθησης του ανθρώπινου άγχους στην καθημερινή ζωή.

Οι **Benny P.L. Lo, Surapa Thiemjarus, Rachel King** και **Guang-Zhong Yang** παρουσίασαν μία μικροσκοπική συσκευή, τον κόμβο δικτύου αισθητήρων σώματος (node Body Sensor Networks (BSN), Εικόνα 3) με σκοπό την παρακολούθησης της υγείας. Εκτός από την παροχή συνεχούς παρακολούθησης και ανάλυσης φυσιολογικών παραμέτρων, τα πρόσφατα προτεινόμενα δίκτυα αισθητήρων σώματος (BSN) ενσωματώνουν διαίσθηση του περιβάλλοντος για αυξημένη ευαισθησία και ειδικότητα. Για τη διευκόλυνση της έρευνας και της εξέλιξης στη σύντηξη δεδομένων

από το BSN και τους πολλαπλούς αισθητήρες, παρουσιάζεται μια πλατφόρμα ανάπτυξης υλικού BSN. Με τη χαμηλή ισχύ, τον εύκαμπτο και συμπαγή σχεδιασμό, οι κόμβοι BSN παρέχουν ένα ευπροσάρμοστο περιβάλλον για την έρευνα και την ανάπτυξη ασύρματης ανίχνευσης [11].

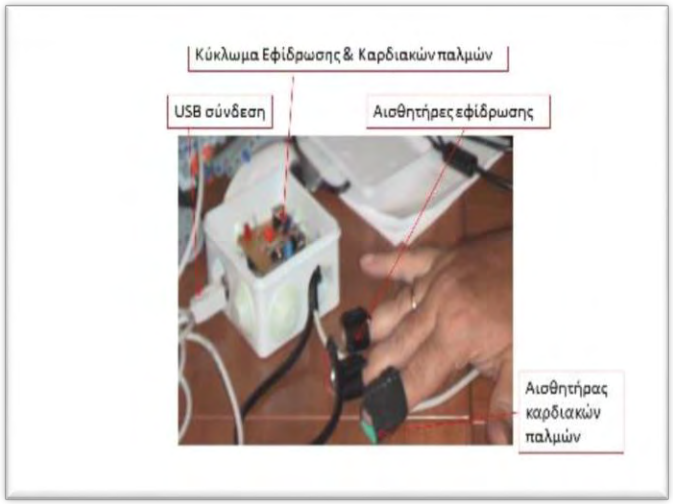
Στη μελέτη των **Y. M. Huang**, **M. Y. Hsieh** και **H. C. Chao** παρουσιάστηκε μια αρχιτεκτονική παρακολούθησης της υγειονομικής περίθαλψης με φορητά συστήματα αισθητήρων και ένα δίκτυο περιβαλλοντικών αισθητήρων για την παρακολούθηση ηλικιωμένων ή χρόνιων ασθενών στην κατοικία τους. Το φορητό σύστημα αισθητήρων, ενσωματωμένο σε μια υφασμάτινη ζών, αποτελείται από διάφορους ιατρικούς αισθητήρες που συλλέγουν ένα έγκαιρο σύνολο φυσιολογικών δεικτών υγείας που μεταδίδονται μέσω ασύρματης επικοινωνίας χαμηλής ενέργειας σε κινητές συσκευές πληροφορικής. Προσαρμοσμένα ζητήματα ασφάλειας για τη μετάδοση δεδομένων εκτελούνται με βάση διαφορετικές ασύρματες δυνατότητες. Τα εφαρμοζόμενα συστήματα ελέγχθηκαν ως αποδοτικά και γρήγορα στην προτεινόμενη αρχιτεκτονική δικτύου [12].

Σκοπός της έρευνας των **Ashraf Darwish** και **Aboul Ella Hassanien** είναι να εξηγήσουν το σημαντικό ρόλο των δικτύων αισθητήρων σώματος και των εμφυτεύσιμων συσκευών στην ιατρική, με σκοπό την ελαχιστοποίηση ανάγκης φροντιστών στους χρόνιους άρρωστους και ηλικιωμένους ανθρώπους και στη δυνατότητα μιας ανεξάρτητης ζωής. Το έγγραφο παρέχει αρκετά παραδείγματα τεχνολογίας αιχμής, μαζί με τις εκτιμήσεις σχεδιασμού όπως η διακριτικότητα, η δυνατότητα κλιμάκωσης, η ενεργειακή απόδοση, η ασφάλεια και παρέχει επίσης μια ολοκληρωμένη ανάλυση των διαφόρων πλεονεκτημάτων και μειονεκτημάτων αυτών των συστημάτων [13].

Η εργασία των **Wan-Young Chung**, **Young-Dong Lee** και **Sang-Joong Jung** παρουσιάζει το σχεδιασμό και την ανάπτυξη ενός φορητού συστήματος παρακολούθησης της υγειονομικής περίθαλψης με χρήση ενσωματωμένων αισθητήρων ηλεκτροκαρδιογραφήματος (ECG), επιταχυνσιόμετρου και κορεσμού οξυγόνου (SpO2). Το σύστημα αυτό σχεδιάστηκε με βάση το ασύρματο δίκτυο αισθητήρων (WSN), για κάλυψη ευρείας περιοχής με ελάχιστη ισχύ μπαταρίας για τη στήριξη της μετάδοσης RF. Το φορητό σύστημα ελέγχου παρακολούθησης υγείας επιτρέπει τη μετάδοση φυσιολογικών δεδομένων σε ασύρματο δίκτυο αισθητήρων σε

έναν σταθμό βάσης, ο οποίος είναι συνδεδεμένος σε ένα υπολογιστή. Τα φυσιολογικά δεδομένα μπορούν να εμφανίζονται και να αποθηκεύονται συνεχώς στον υπολογιστή [14].

Οι **Changzhi Li**, **Victor M. Lubecke** και **Olga Boric-Lubecke** εξέτασαν τις πρόσφατες εξελίξεις στις εφαρμογές βιοϊατρικής και υγειονομικής περίθαλψης του ραντάρ Doppler, που ανιχνεύει εξ αποστάσεως τον καρδιακό παλμό και την αναπνοή ενός ανθρώπου. Τα πλεονεκτήματα της ανίχνευσης χωρίς επαφή έχουν προκαλέσει ενδιαφέρον για διάφορες εφαρμογές, όπως το έξυπνο σπίτι ενέργειας, η παρακολούθηση μωρού, η αξιολόγηση καρδιοπνευμονικής δραστηριότητας και η παρακολούθηση όγκων. Αυτό το έγγραφο εξετάζει διαφορετικές αρχιτεκτονικές, την επεξεργασία σήματος βάσης και τις υλοποιήσεις του συστήματος [15].



Εικόνα 1. Κύκλωμα Arduino

Εικόνα 2. Polar RS800CX.

Εικόνα 3. BSN node.

2.2 Biometric authentication

Σε αυτή την υποενότητα θα γίνει μια σύντομη ανάλυση ερευνών και εργασιών που σχετίζονται με τον βιομετρικό έλεγχο ταυτότητας.

Οι **R. Snelick**, **U. Uludag** και **A. Mink** εξέτασαν την απόδοση συστημάτων πολυτροπικών βιομετρικών στοιχείων ελέγχου ταυτότητας, με τη χρήση ψηφιακών δακτυλικών αποτυπωμάτων (COTS) τελευταίας τεχνολογίας και βιομετρικών συστημάτων προσώπου σε πληθυσμό που προσεγγίζει τα 1.000 άτομα. Ήταν οι πρώτοι που απέδειξαν ότι τα πολυτροπικά βιομετρικά συστήματα δακτυλικών αποτυπωμάτων και προσώπου, μπορούν να επιτύχουν σημαντικά οφέλη ακρίβειας σε σχέση με τα απλά βιομετρικά συστήματα. Εκτός από την εξέταση πολύ γνωστών πολυτροπικών μεθόδων, εισήγαγαν νέες μεθόδους εξομάλυνσης και σύντηξης που βελτιώνουν περαιτέρω την ακρίβεια[16].

Στην εργασία τους, οι **Pim Tuyls**, **Anton H. M. Akkermans**, **Tom A. M. Kevenaar**, **Geert-Jan Schrijen**, **Asker M. Bazen** και **Raimond N. J. Veldhuis,** παρουσίασαν τη σκοπιμότητα της προστασίας των βιομετρικών συστημάτων ελέγχου ταυτότητας. Συγκεκριμένα, εφάρμοσαν συστήματα προστασίας προτύπων σε δεδομένα δακτυλικών αποτυπωμάτων [17].

Οι **Dario Maio**, **Davide Maltoni**, **Raffaele Cappelli**, **Jim L. Wayman** και **Anil K. Jain** οργάνωσαν μια νέα τεχνολογική αξιολόγηση των αλγορίθμων επαλήθευσης δακτυλικών αποτυπωμάτων, ακολουθώντας την προσέγγιση των προηγούμενων αξιολογήσεων FVC2000 και FVC2002, με στόχο την παρακολούθηση των ταχέως εξελισσόμενων συστημάτων τεχνολογίας αναγνώρισης δακτυλικών αποτυπωμάτων [18].

Ο **Paul M. Burger** εφηύρε ένα βιομετρικό σύστημα ελέγχου ταυτότητας, το οποίο περιλαμβάνει έναν αναγνώστη διπλής εισόδου. Οι είσοδοι αποτελούνται από αποθηκευμένα φυσιολογικά δεδομένα ενός χρήστη σε ένα τσιπ που διατίθεται σε μια έξυπνη κάρτα, και ένα σαρωτή δακτυλικών αποτυπωμάτων για σύγκριση με τα αποθηκευμένα δεδομένα. Η εφεύρεση εμποδίζει, επίσης, την επικοινωνία με εξωτερικές πηγές πριν από την επιβεβαίωση της γνησιότητας του χρήστη, έτσι ώστε να αποτραπεί η κλοπή ή η αλλοίωση των δεδομένων των χρηστών [19].

Οι **Noel D. Matchett** και **Brian D. Kehoe** δημιούργησαν ένα σύστημα που ενεργοποιεί και αναλύει τα βιομετρικά δεδομένα από μια πλειάδα βιομετρικά προσανατολισμένων συσκευών προσωπικής αναγνώρισης σε διακοπτόμενα διαστήματα. Το σύστημα αυτό επιτρέπει ή εμποδίζει, επιλεκτικά, τη συνεχή χρήση ενός συγκεκριμένου προστατευμένου συστήματος ή συσκευής από ένα συγκεκριμένο άτομο. Το όριο αποδοχής/απόρριψης για μεμονωμένες συσκευές βιομετρικών αισθητήρων είναι ρυθμιζόμενο, όπως και το όριο αποδοχής/απόρριψης για το συνολικό συνδυασμό βιομετρικών αισθητήρων [20].

Οι **Adams Wai-Kin Kong** και **David Zhang** προτείνουν μια προσέγγιση σύντηξης, σε επίπεδο χαρακτηριστικών, για τη βελτίωση της αποτελεσματικότητας της αναγνώρισης των παλαμών. Χρησιμοποιείται μια βάση δεδομένων που περιέχει 7.752 εικόνες παλάμης από 386 διαφορετικές παλάμες για την επικύρωση της απόδοσης της προτεινόμενης μεθόδου. Η εμπειρική σύγκριση της προηγούμενης προσέγγισης μη σύντηξης και της προτεινόμενης μεθόδου εξασφαλίζει τη βελτίωση της επαλήθευσης [21].

Στην εργασία τους, οι **Pim Tuyls** και **Jasper Goseling**, διατύπωσαν με ακρίβεια τις απαιτήσεις για την προστασία της ιδιωτικότητας των βιομετρικών συστημάτων ελέγχου ταυτότητας. Επιπλέον, παρουσίασαν έναν γενικό αλγόριθμο που ικανοποιεί τις απαιτήσεις και επιτυγχάνει την ικανότητα απορρήτου καθώς και την ικανότητα

αναγνώρισης. Τέλος, παρουσίασαν κάποιες πρακτικές κατασκευές του γενικού αλγορίθμου και ανέλυσαν τις ιδιότητές τους [22].

Οι **Yuan-Pin Yu**, **Stephen Wong** και **Mark B. Hoffberg** είναι οι εφευρέτες ενός συστήματος και μιας μεθόδου ελέγχου ταυτότητας βασισμένη στο ίντερνετ. Το σύστημα περιλαμβάνει τουλάχιστον έναν σταθμό πελάτη Web, τουλάχιστον έναν σταθμό διακομιστή Web και ένα κέντρο ελέγχου ταυτότητας. Πραγματοποιείται εξακρίβωση της ταυτότητας του ατόμου που επιδιώκει την πρόσβαση στο σταθμού του διακομιστή, η οποία είναι συνήθως πρόσβαση σε πληροφορίες, υπηρεσίες και άλλους πόρους που παρέχονται από έναν ή περισσότερους διακομιστές εφαρμογών που σχετίζονται με το σταθμό του διακομιστή Web [23].

2.3 Ανίχνευση κίνησης/δραστηριότητας χρήστη

Με τη διαθεσιμότητα οικονομικά προσιτών αισθητήρων και δικτύων αισθητήρων, η αναγνώριση ανθρώπινης δραστηριότητας βασισμένη σε αισθητήρες έχει προσελκύσει μεγάλη προσοχή στην τεχνητή νοημοσύνη και στην πανταχού παρούσα πληροφορική. Παρακάτω θα γίνει αναφορά σε μερικές σχετικές εφαρμογές.

Οι **Artemiy Oleinikov**, **Berdakh Abibullaev** και **Almas Shintemirov** χρησιμοποίησαν το κανάλι ηλεκτρομυογραφίας του BITalino για την αναγνώριση διαφορετικών θέσεων και κινήσεων των χεριών μέσω τεχνητών νευρωνικών δικτύων. Με τον τρόπο αυτό, πέτυχαν 82% ακρίβεια για οκτώ κινήσεις χεριού και 91% ακρίβεια για έξι κινήσεις χεριού, με στόχο την επανένταξη ατόμων με ακρωτηριασμούς ή αναπηρίες των άνω άκρων στην κοινωνία μας. Πρόσθεσαν, λοιπόν, ένα ακόμα λιθαράκι στις έρευνες στον τομέα της πρόσθεσης ενεργού βραχίονα [24].

Η εργασία των **Jan Meyer**, **Paul Lukowicz** και **Gerhard Troster** παρουσιάζει έναν υφασμάτινο αισθητήρα χωρητικής πίεσης, σχεδιασμένο με σκοπό την ενσωμάτωσή του σε ρούχα για τη μέτρηση της πίεσης στο ανθρώπινο σώμα. Τα πεδία εφαρμογής καλύπτουν όλους τους τομείς όπου απαιτείται ένας μαλακός και εύκαμπτος αισθητήρας

με υψηλή τοπική ανάλυση, π.χ. στην αποκατάσταση, στην πρόληψη τραυματισμού λόγω πίεσης ή στην ανίχνευση κίνησης λόγω μυϊκών δραστηριοτήτων [25].

Η ομάδα των **Jaeyong Sung**, **Colin Ponce** και **Bart Selman** πραγματοποίησαν ανίχνευση και αναγνώριση της μη δομημένης ανθρώπινης δραστηριότητας σε μη δομημένα περιβάλλοντα. Χρησιμοποίησαν έναν αισθητήρα RGBD (Microsoft Kinect) ως αισθητήρα εισόδου και υπολόγισαν ένα σύνολο από λειτουργίες που βασίζονται στην ανθρώπινη στάση και κίνηση. Δοκίμασαν τον αλγόριθμό τους για την ανίχνευση και αναγνώριση δώδεκα διαφορετικών δραστηριοτήτων που εκτελούνται από τέσσερα άτομα σε διαφορετικά περιβάλλοντα, όπως κουζίνα, σαλόνι, γραφείο κλπ., και επιτυγχάνουν καλές επιδόσεις ακόμη και όταν το άτομο δεν είχε ανιχνευθεί αρχικά στο εκπαιδευτικό σετ [26].

Στην εργασία τους, οι **Daphney-Stavroula Zois**, **Marco Levorato** και **Urbashi Mitra**, αντιμετώπισαν το πρόβλημα της αποτελεσματικής λειτουργίας ενός ενεργειακά περιορισμένου, ετερογενούς Wireless Body Area Netawork (WBAN) για τη βελτιστοποίηση μιας εφαρμογής εντοπισμού δραστηριότητας. Ένα τυπικό WBAN αποτελείται από μερικούς, ετερογενείς αισθητήρες ασύρματα συνδεδεμένους με ένα ενεργειακά περιορισμένο κέντρο σύντηξης, το οποίο επιβάλλει σημαντικούς περιορισμούς στη διάρκεια ζωής του συστήματος. Για να αντιμετωπίσουν αυτό το ζήτημα, εισήγαγαν ένα νέο στοχαστικό πλαίσιο ελέγχου, το οποίο λαμβάνει υπόψη τόσο την ετερογένεια των αισθητήρων όσο και τις απαιτήσεις της εφαρμογής, για την επίτευξη του διττού στόχου: εξοικονόμηση ενέργειας με ικανοποιητική απόδοση ανίχνευσης. Επίσης, δημιούργησαν ένα δυναμικό αλγόριθμο προγραμματισμού για το πρόβλημα επιλογής αισθητήρα [27].

Ο **N. Noury** ασχολήθηκε με την ανίχνευση της πτώσης των ηλικιωμένων. Ο απώτερος στόχος του ήταν να επιτευχθεί ένας καλός συμβιβασμός μεταξύ ανίχνευσης σε πραγματικό χρόνο, ευαισθησίας και εξειδίκευσης. Παρουσίασε μια ακριβέστερη περιγραφή της αρχής του έξυπνου αισθητήρα πτώσης, με τα αποτελέσματά της και την πρόταση μιας νέας ευέλικτης έκδοσης, που ο ίδιος υλοποίησε, και μπορεί να ενσωματωθεί σε ένδυμα [28].

Οι **Mark W. Kroll**, **Chris Sorensen** και **Gene A. Bornzin** εφηύραν μια εμφυτεύσιμη συσκευή καρδιακής διέγερσης, εφοδιασμένη με έναν αισθητήρα -που βασίζεται σε επιταχυνσιόμετρο- για να ανιχνεύει την κίνηση ενός ασθενούς και να παράγει ένα

στοιχείο κατακόρυφης επιτάχυνσης, ενδεικτικό της επιτάχυνσης του ασθενούς σε κάθετη κατεύθυνση. Σε συνδυασμό με διάφορους αισθητήρες αποτελεί έναν επεξεργαστή, που προγραμματίζεται για τον προσδιορισμό της θέσης και της κατάστασης της δραστηριότητας του ασθενούς, όπως εάν ο ασθενής ανεβαίνει/κατέρχεται ή σκαρφαλώνει. Από την κατάσταση του ασθενούς αποφασίζεται εάν θα χορηγηθεί θεραπεία καρδιακού βηματοδότη και το είδος της θεραπείας που θα εφαρμοστεί [29].

Οι **Kaustubh Kalgaonkar**, **Rongquiang Hu** και **Bhiksha Raj** ανέπτυξαν και παρουσίασαν μια απλή, αλλά ισχυρή μέθοδο εξαγωγής πληροφοριών φωνητικής δραστηριότητας, από το υπερηχητικό σήμα Doppler. Μία υπερηχητική δέσμη προσπίπτει στο πρόσωπο του συνομιλητή. Οι κινήσεις του προσώπου μετατρέπονται σε μεταβολές συχνότητας Doppler, οι οποίες ανιχνεύονται από τον αισθητήρα υπερήχων. Οι κινήσεις του προσώπου, που σχετίζονται με το λόγο, μετατρέπονται σε αναγνωρίσιμα μοτίβα που μπορούν να χρησιμοποιηθούν για την αναγνώριση της ομιλίας. Ο αλγόριθμός τους είναι πολύ αποτελεσματικός και ανθεκτικός στον θόρυβο και μπορεί να εφαρμοστεί σε πραγματικό χρόνο [30].

Οι **Seon-Woo Lee** και **K. Mase** πρότειναν μια αποτελεσματική μέθοδο υπολογισμού της θέσης του χρήστη, η οποία έχει τη δυνατότητα να ανιχνεύει τις μεταβάσεις μεταξύ προεπιλεγμένων θέσεων και να αναγνωρίζει και να ταξινομεί τις συμπεριφορές του χρήστη (αν κάθεται, στέκεται ή περπατάει). Αυτό επιτυγχάνεται χρησιμοποιώντας δεδομένα επιτάχυνσης και γωνιακής ταχύτητας που συγκεντρώθηκαν μέσω φτηνών, wearable αισθητήρων [31].

3.SECURE MULTIPARTY COMPUTATION

3.1 Σωστή και κακή χρήση ιδιωτικών πληροφοριών

Σε μια σύγχρονη κοινωνία που βασίζεται στην πληροφόρηση, η καθημερινή ζωή των ατόμων και των εταιρειών είναι γεμάτη από περιπτώσεις όπου διάφοροι τύποι ιδιωτικών πληροφοριών αποτελούν σημαντικούς πόρους. Ενώ ένας κρυπτογράφος μπορεί να σκεφτεί κωδικούς PIN και κλειδιά, αυτά τα είδη των μυστικών δεν είναι το κύριο στοιχείο που θα μελετηθεί. Αντίθετα, θα γίνει ανάλυση των πληροφοριών που είναι πιο κοντά στην κύρια δραστηριότητα ενός ατόμου ή μιας εταιρείας. Για έναν ιδιώτη, αυτό μπορεί να είναι δεδομένα σχετικά με την οικονομική του κατάσταση, όπως το εισόδημα, τα δάνεια και τα φορολογικά στοιχεία ή πληροφορίες σχετικά με την υγεία του, όπως οι ασθένειες και η χρήση της ιατρικής. Για μια εταιρεία, μπορεί να είναι η βάση δεδομένων πελατών ή πληροφορίες σχετικά με τον τρόπο λειτουργίας της επιχείρησης, όπως ο κύκλος εργασιών, τα κέρδη και οι μισθοί.

Χρησιμοποιώντας τα ηλεκτρονικά μέσα, στη σύγχρονη κοινωνία, υπάρχει αλληλεπίδραση και συνεργασία μεταξύ των μελών μικρών ή μεγάλων ομάδων. Στις πιο πολλές από αυτές τα μέλη δεν γνωρίζονται και συχνά ενδέχεται να έχουν αντικρουόμενα συμφέροντα. Επομένως, η χρήση των ιδιωτικών δεδομένων καθίσταται εξαιρετικά δύσκολη, αν δε βεβαιωθεί ότι οι ομάδες με τις οποίες αλληλοεπιδρά μια εταιρεία είναι αξιόπιστες.

Θα μπορούσε να γίνει αποθήκευση των ευαίσθητων δεδομένων σε μια πολύ ασφαλή τοποθεσία που να μην επιτρέπεται η πρόσβαση, αλλά αυτό είναι, φυσικά, παράλογο. Τα προσωπικά δεδομένα έχουν –συνήθως- αξία επειδή χρησιμοποιούνται για κάτι. Με άλλα λόγια, πρέπει να υπάρχουν τρόποι ελέγχου της διαρροής εμπιστευτικών δεδομένων, ενώ αυτά τα δεδομένα αποθηκεύονται, διαβιβάζονται ή υπολογίζονται, ακόμη και σε περιπτώσεις όπου ο κάτοχος των δεδομένων δεν εμπιστεύεται τα μέρη με τα οποία επικοινωνεί [32].

Οι περισσότεροι χρήστες ηλεκτρονικών υπολογιστών διατρέχουν σημαντικούς κινδύνους ασφαλείας. Η ύπαρξη κινδύνου δεν σημαίνει ότι θα πρέπει να σταματήσει η χρήση των υπολογιστών.

Οι χρήστες και οι διαχειριστές των μεγάλων υπολογιστικών συστημάτων κεντρικών υπολογιστών της δεκαετίας του 1960 και του 1970, ανέπτυξαν τεχνικές ασφάλειας υπολογιστών που ήταν λογικά αποτελεσματικές κατά τη διάρκεια αυτής της εποχής. Ωστόσο, δύο παράγοντες έχουν καταστήσει ξεπερασμένες αυτές τις διαδικασίες ασφαλείας [33]:

1. **Η χρήση προσωπικών υπολογιστών.** Μεγάλος αριθμός ανθρώπων έχουν γίνει χρήστες συστημάτων προσωπικών υπολογιστών, τόσο για δουλειές όσο και για ευχαρίστηση. Κατασκευάζονται εφαρμογές "φιλικές προς το χρήστη" έτσι ώστε οι υπολογιστές να μπορούν να χρησιμοποιηθούν από ανθρώπους που δεν γνωρίζουν τίποτα για υλικό ή προγραμματισμό. Οι χρήστες ενδέχεται να μην είναι ιδιαίτερα συνειδητοί για τις απειλές κατά της ασφάλειας που σχετίζονται με τη χρήση του υπολογιστή· ακόμη και οι χρήστες που γνωρίζουν μπορεί να μην ξέρουν τι να κάνουν για να μειώσουν τον κίνδυνο τους.
2. **Συστήματα δικτύου απομακρυσμένης πρόσβασης.** Τα μηχανήματα συνδέονται σε μεγάλους αριθμούς. Το Διαδίκτυο και ο Παγκόσμιος Ιστός, μοιάζουν να διπλασιάζονται κάθε χρόνο σε αριθμό χρηστών. Ένας χρήστης ενός κεντρικού υπολογιστή μπορεί να μην συνειδητοποιήσει ότι η πρόσβαση στο ίδιο μηχάνημα επιτρέπεται στους ανθρώπους σε όλο τον κόσμο από έναν σχεδόν αμέτρητο αριθμό υπολογιστικών συστημάτων.

3.2 Secure multiparty computation

Η μεθοδολογία Secure Multiparty Computation συνίσταται στον υπολογισμό μίας συνάρτησης βάσει ιδιωτικών τιμών που κατέχουν τα μέλη μίας ομάδας. Η βασική προσέγγιση εγγυάται τον υπολογισμό αυτό χωρίς το κάθε μέλος να αποκαλύπτει την ιδιωτική τιμή (είσοδο στην συνάρτηση) που διαθέτει. Υπάρχουν διάφορα μοντέλα για

ασφαλή υπολογισμό πολλών μελών, αναλόγως με τον τύπο των μελών που κάθε μοντέλο θεωρείται ότι προστατεύει, συμπεριλαμβανομένων των κακόβουλων συμπεριφορών και των κρυφών αντιπάλων. Το μοντέλο μπορεί να θεωρηθεί και ως μια έμπιστη βάση με τη χρήση της δομής δημόσιου κλειδιού ή χρησιμοποιώντας μια συμβολοακολουθία ως κοινή αναφορά. Η μέθοδος Secure Multiparty Computation έχει πολλές εφαρμογές συμπεριλαμβανομένων των scientific computation, data mining και data base querying.

Γενικά, ένα πρόβλημα ασφαλούς υπολογισμού πολλών μελών ασχολείται με τον υπολογισμό οποιασδήποτε συνάρτησης σε ένα διανεμημένο δίκτυο όπου ο κάθε συμμετέχων κατέχει ένα από τα ορίσματα, εξασφαλίζοντας έτσι την ανεξαρτησία των ορισμάτων, την ορθότητα του υπολογισμού, και ότι δε θα αποκαλυφθεί καμιά επιπλέον πληροφορία σε κάποιον συμμετέχοντα, η οποία μπορεί να εξαχθεί από το όρισμά του και το αποτέλεσμα του υπολογισμού. Μια κοινή στρατηγική είναι να θεωρηθεί σίγουρη η αξιοπιστία των παρόχων της υπηρεσίας, ή να θεωρηθεί η ύπαρξη ενός τρίτου μέρους, που είναι ριψοκίνδυνο στο σημερινό δυναμικό και κακόβουλο περιβάλλον.

Το κοινό χαρακτηριστικό αυτών των προβλημάτων είναι ότι δύο ή περισσότερα μέλη θέλουν να διεξάγουν έναν υπολογισμό με βάση τα δικά τους ιδιωτικά ορίσματα, αλλά κανένα μέλος δεν επιθυμεί να αποκαλύψει το δικό του όρισμα σε κάποιο άλλο. Το πρόβλημα είναι με ποιον τρόπο μπορεί να διεξαχθεί ένας τέτοιος υπολογισμός, διατηρώντας την ιδιωτικότητα των ορισμάτων. Το πρόβλημα αυτό αναφέρεται ως Secure Multiparty Computation.

3.3 Παρουσίαση ενός μοντέλου SMC

Αναλυτικά, τα μέρη ή οι παίκτες που συμμετέχουν ονομάζονται $\mathbf{P_1,\ldots, P_n}$. Κάθε παίκτης $\mathbf{P_i}$ κατέχει μυστική είσοδο $\mathbf{x_i}$ και οι παίκτες συμφωνούν σε μια συνάρτηση **f** που λαμβάνει **n** εισόδους. Στόχος τους είναι να υπολογίζουν το $\mathbf{y = f(x_1,\ldots,x_n)}$ μεριμνώντας για την ικανοποίηση των ακόλουθων δύο προϋποθέσεων:

i. Ορθότητα: σωστός υπολογισμός της τιμής του **y**, και

ii. Απόρρητο: το **y** είναι η μόνη νέα πληροφορία που ανακοινώνεται.

Όσον αφορά την τελευταία προϋπόθεση, επισημαίνεται ότι επειδή ο σκοπός της όλης άσκησης είναι να γίνει γνωστό το **y**, από την άποψη της ιδιωτικότητας είναι ότι δεν πρέπει να διαφεύγει τίποτα άλλο παρά μόνο το **y**. Ο υπολογισμός της **f** έτσι ώστε να επιτυγχάνονται η ιδιωτικότητα και η ορθότητα αναφέρεται ως υπολογισμός της **f** με ασφάλεια. Μπορεί κανείς να εξετάσει μια πιο γενική περίπτωση, όπου κάθε παίκτης παίρνει το δικό του ιδιωτικό αποτέλεσμα.

Ως παράδειγμα του τρόπου με τον οποίο αυτό συνδέεται με τα σενάρια που παρουσιάστηκαν στις προηγούμενες παραγράφους, μπορεί κανείς να σκεφτεί το $\mathbf{x_i}$ ως αριθμό, και πιο συγκεκριμένα ως την προσφορά του $\mathbf{P_i}$ σε μια δημοπρασία και

$$\mathbf{f(x_1,\ldots,x_n) = (z,j)} \text{ , όπου } \mathbf{x_j = z} \text{ και } \mathbf{z \geq x_i,\ i = 1,\ldots,n}$$

το **f** εξάγει την υψηλότερη προσφορά και την ταυτότητα του αντίστοιχου πλειοδότη. Αν ο νικητής δε θέλει να πληρώσει τη δική του προσφορά αλλά την προσφορά του δεύτερου υψηλότερου πλειοδότη, απλώς γίνεται αλλαγή στο **z** ώστε να είναι ίσο με την τιμή αυτή, η οποία είναι και πάλι μια καλά καθορισμένη συνάρτηση των εισόδων. Αυτό θα αποτελέσει μια συνάρτηση που θα υλοποιεί τη λεγόμενη δημοπρασία δεύτερης τιμής.

Σε αυτή την ενότητα δίνεται μια πρώτη διαίσθηση σχετικά με τον τρόπο με τον οποίο κάποιος θα μπορούσε να υπολογίσει μια λειτουργία με ασφάλεια, χωρίς να στηρίζεται σε αξιόπιστα μέρη. Αυτό απαιτεί να καθοριστεί ένα πρωτόκολλο, δηλαδή ένα σύνολο οδηγιών που οι παίκτες πρέπει να ακολουθήσουν για να αποκτήσουν το επιθυμητό αποτέλεσμα. Για ευκολία, θεωρείται ότι οι παίκτες ακολουθούν πάντα το πρωτόκολλο. Στη συνέχεια θα εξεταστεί η περίπτωση κατά την οποία ορισμένα μέρη ενδέχεται να παρεκκλίνουν από το πρωτόκολλο, προκειμένου να λάβουν περισσότερες πληροφορίες από ό, τι πρέπει ή να προκαλέσουν λάθος αποτέλεσμα. Έστω ότι οποιοδήποτε ζευγάρι παικτών μπορεί να επικοινωνήσει με ασφάλεια. Δηλαδή, είναι δυνατόν για τον $\mathbf{P_i}$ να στείλει ένα μήνυμα **m** στο $\mathbf{P_j}$ έτσι ώστε να μην βλέπει κάποιος τρίτος το **m**, και ο $\mathbf{P_j}$ ξέρει ότι το **m** ήρθε από τον $\mathbf{P_i}$. Θα παρουσιαστεί αργότερα πώς μπορεί να γίνει αυτό στην πράξη.

3.3.1 Ασφαλής πρόσθεση και ψηφοφορία

Θα μελετηθεί πρώτα μια απλή ειδική περίπτωση, όπου κάθε $\mathbf{x_i}$ είναι ένας φυσικός αριθμός και $\mathbf{f}(\mathbf{x_i}, \dots, \mathbf{x_n}) = \sum_{i=1}^{n} \mathbf{x_i}$. Ο ασφαλής υπολογισμός ακόμη και μιας τέτοιας απλής λειτουργίας μπορεί να έχει πολύ σημαντικές εφαρμογές. Η περίπτωση, για παράδειγμα, όπου οι $\mathbf{P_1,\dots,P_n}$ θέλουν να ψηφίσουν ναι/όχι για κάποια απόφαση. Στη συνέχεια, το $\mathbf{x_i}$ αντιπροσωπεύει την ψήφο του $\mathbf{P_i}$, όπου $\mathbf{x_i=0}$ σημαίνει "όχι" και $\mathbf{x_i=1}$ σημαίνει "ναι". Αν μπορεί να υπολογιστεί το άθροισμα του $\mathbf{x_i}$ με ασφάλεια, αυτό σημαίνει ότι υπάρχει ένας τρόπος να πραγματοποιηθεί η ψηφοφορία με τις ιδιότητες που συνήθως αναμένονται: το αποτέλεσμα $\sum_{i=1}^{n} \mathbf{x_i}$ να είναι πράγματι το αποτέλεσμα της ψηφοφορίας, δηλαδή ο αριθμός των θετικών ψήφων. Και επιπλέον, ο υπολογισμός να είναι ασφαλής, δηλαδή να μη διαχέονται πληροφορίες πέρα από το $\sum_{i=1}^{n} \mathbf{x_i}$, και ειδικότερα να μην αποκαλύπτονται πληροφορίες σχετικά με τον τρόπο με τον οποίο ψήφισε ο $\mathbf{P_i}$. Θα παρουσιαστεί ένα πρωτόκολλο για την εφαρμογή ψηφοφορίας. Για λόγους συνέπειας ορίζεται το $\mathbf{n=3}$ για το επόμενο παράδειγμα.

3.3.2 Secret Sharing

Πριν λυθεί το πρόβλημα, πρέπει να εξεταστεί ένα σημαντικό εργαλείο που είναι γνωστό ως secret sharing (κρυφή ανταλλαγή). Ο όρος μπορεί να φανεί από μόνος του αντιφατικός: πώς μπορεί κάτι να είναι μυστικό εάν μοιράζεται με άλλους; Παρ' όλα αυτά, το όνομα έχει νόημα: το θέμα είναι ότι η κρυφή ανταλλαγή παρέχει έναν τρόπο για ένα μέλος, ας πούμε το $\mathbf{P_1}$, να διαδίδει την πληροφορία ενός κρυφού αριθμού $\mathbf{x}$ σε όλους τους παίκτες, ώστε μαζί να κατέχουν την πλήρη ενημέρωση για το $\mathbf{x}$, παράλληλα κανένα μέλος (εκτός, φυσικά του $\mathbf{P_1}$) έχει οποιαδήποτε πληροφορία για το $\mathbf{x}$. Πρώτα, επιλέγουμε ένα αρχικό $\mathbf{p}$, και ορίζουμε το $\mathbf{Z_p}$ ως $\mathbf{Z_p = \{0,1,\dots,p-1\}}$ και στη συνέχεια το κρυφό $\mathbf{x}$ αποτελεί έναν αριθμό που ανήκει στο $\mathbf{Z_p}$.

Προκειμένου να σταλεί το κρυφό **x**, ο $\mathbf{P_1}$ επιλέγει ομοιόμορφα τους τυχαίους αριθμούς $\mathbf{r_1}$, $\mathbf{r_2}$ από το $\mathbf{Z_p}$ και θέτει:

$$\mathbf{r_3 = x - r_1 - r_2 \bmod p}$$

Διαφορετικά, ο $\mathbf{P_1}$ επιλέγει τυχαία τα $\mathbf{r_1}$, $\mathbf{r_2}$, $\mathbf{r_3}$ από το $\mathbf{Z_p}$, βάση του περιορισμού:

$$\mathbf{x = r_1 + r_2 + r_3 \bmod p}$$

Ο τρόπος επιλογής των $\mathbf{r_1}$, $\mathbf{r_2}$, $\mathbf{r_3}$ σημαίνει ότι ο καθένας από τους τρεις αριθμούς επιλέγεται ομοιόμορφα από το $\mathbf{Z_p}$: για κάθε έναν από αυτούς, όλες οι τιμές στο $\mathbf{Z_p}$ είναι δυνατές και εξίσου πιθανές να επιλεχθούν. Τώρα, το $\mathbf{P_1}$ στέλνει ιδιωτικά τα $\mathbf{r_1}$, $\mathbf{r_3}$ στο $\mathbf{P_2}$, τα $\mathbf{r_1}$, $\mathbf{r_2}$ στο $\mathbf{P_3}$, και κρατά τα $\mathbf{r_2}$, $\mathbf{r_3}$ για τον εαυτό του. Τα $\mathbf{r_j}$ ονομάζονται «μέρη του μυστικού **x**».

Η διαδικασία που παρουσιάστηκε ικανοποιεί δύο βασικές ιδιότητες: Πρώτον, το μυστικό **x** παραμένει ιδιωτικό, με την έννοια ότι ούτε ο $\mathbf{P_2}$ ούτε ο $\mathbf{P_3}$ γνωρίζουν κάτι για το μυστικό αυτό. Με αποτέλεσμα, αν κάποιος χάκερ παραβιάσει το $\mathbf{P_2}$ ή το $\mathbf{P_3}$ (αλλά όχι και τα δύο), δε θα μάθει τίποτα για το **x**. Δεύτερον, το **x** μπορεί να ανακατασκευαστεί αν είναι διαθέσιμα τα μέρη από τουλάχιστον δύο παίκτες. Έστω ότι αυτό ισχύει με έναν πιο συγκεκριμένο τρόπο:

i. **Ιδιωτικότητα**. Παρόλο που ο $\mathbf{P_1}$ έχει διανείμει μέρη του μυστικού **x** στους άλλους παίκτες, ούτε ο $\mathbf{P_2}$ ούτε ο $\mathbf{P_3}$ έχουν ιδέα τι είναι το **x**. Για τον $\mathbf{P_2}$, υποστηρίζονται τα εξής: αυτός ξέρει τα $\mathbf{r_1}$, $\mathbf{r_3}$ (αλλά όχι το $\mathbf{r_2}$) και ότι ισχύει: $\mathbf{x = r_1 + r_2 + r_3 \bmod p}$. Από τη μεριά του P_2 θα μπορούσε να ισχύει $x = x_0$, για οποιοδήποτε x_0 ανήκει στο Z_p. Σε αυτή την περίπτωση:

   $$\mathbf{r_2 = x_0 - r_1 - r_3 \bmod p}$$

   από τη στιγμή που το $\mathbf{r_2}$ επιλέγεται ομοιόμορφα από το $\mathbf{Z_p}$ και όλες οι τιμές του είναι πιθανές. Ωστόσο, οποιαδήποτε άλλη επιλογή, π.χ. $\mathbf{x = x_0' \neq x_0}$ είναι επίσης πιθανή και τότε: $\mathbf{r_2 = x_0' - r_1 - r_3 \bmod p}$, που αποτελεί διαφορετική τιμή από το $\mathbf{x_0 - r_1 - r_3 \bmod p}$, αλλά εξίσου πιθανή. Καταλήγοντας, το συμπέρασμα είναι ότι αυτό που έχει σταλεί στο $\mathbf{P_2}$ δεν αποκαλύπτει τίποτα νέο για το **x**. Ομοίως ισχύει και για το $\mathbf{P_3}$.

ii. **Ορθότητα**. Εάν δύο από τα τρία μέλη συγκεντρώσουν τις πληροφορίες τους, το μυστικό μπορεί να ανακατασκευαστεί γιατί τότε και τα τρία μέρη (r_1,r_2,r_3) θα είναι γνωστά και μπορεί κάποιος απλά να τους προσθέσει το **modulo p**.

Αξίζει να σημειωθεί ότι η ιδιωτικότητα αποτελεί θεωρητική πληροφορία. Όσο ένα συμβαλλόμενο μέλος δε γνωρίζει και τους τρεις αριθμούς (r_1,r_2,r_3), κανένα ποσό υπολογιστικής δύναμης δε μπορεί να δώσει σε αυτό το μέλος οποιαδήποτε νέα πληροφορία σχετικά με το αντίστοιχο κρυφό **x**.

3.3.3 Πρωτόκολλο ασφαλής πρόσθεσης

Η βασική ιδέα για μια ασφαλή πρόσθεση είναι ότι όλα τα μέλη $\mathbf{P_1}$, $\mathbf{P_2}$ και $\mathbf{P_3}$ θα διανείμουν τα μερίδια των ιδιωτικών τους τιμών $\mathbf{x_1}$, $\mathbf{x_2}$ και $\mathbf{x_3}$ ακριβώς όπως και προηγουμένως. Αποδεικνύεται ότι κάποιος μπορεί τώρα να υπολογίσει το ποσό με ασφάλεια, προσθέτοντας τοπικά τα μέρη και ανακοινώνοντας το αποτέλεσμα. Το πλήρες πρωτόκολλο έχει ως εξής:

Τα $\mathbf{P_1}$,$\mathbf{P_2}$,$\mathbf{P_3}$ είναι οι συμμετέχοντες. Το όρισμα για το $\mathbf{P_i}$ είναι το $\mathbf{x_i}$ που ανήκει στο $\mathbf{Z_p}$, ενώ το **p** είναι μια αρχική σταθερή τιμή.

1. Κάθε $\mathbf{P_i}$ υπολογίζει και διανέμει μέρη του κρυφού του $\mathbf{x_i}$ όπως αναλύθηκε παραπάνω: επιλέγει ομοιόμορφα με τυχαίο τρόπο από το $\mathbf{Z_p}$ τα $\mathbf{r_{i,1}}$ και $\mathbf{r_{i,2}}$ και θέτει $\mathbf{r_{i,3} = x_i - r_{i,1} - r_{i,2} \bmod p}$.
2. Κάθε $\mathbf{P_i}$ στέλνει ιδιωτικά τα $\mathbf{r_{i,2}}$, $\mathbf{r_{i,3}}$ στο $\mathbf{P_1}$, τα $\mathbf{r_{i,1}}$, $\mathbf{r_{i,3}}$ στο $\mathbf{P_2}$ και τα $\mathbf{r_{i,1}}$, $\mathbf{r_{i,2}}$ στο $\mathbf{P_3}$ (αυτό συμπεριλαμβάνει ότι το $\mathbf{P_i}$ στέλνει και στον εαυτό του). Έτσι το $\mathbf{P_1}$, για παράδειγμα, κατέχει τώρα τα $\mathbf{r_{1,2}}$, $\mathbf{r_{1,3}}$, $\mathbf{r_{2,2}}$, $\mathbf{r_{2,3}}$ και τα $\mathbf{r_{3,2}}$ $\mathbf{r_{3,3}}$.
3. Κάθε $\mathbf{P_j}$ προσθέτει τα αντίστοιχα μέρη των κρυφών τιμών (x_1,x_2,x_3). Ποιο συγκεκριμένα υπολογίζει $\mathbf{s_m = r_{1,m} + r_{2,m} + r_{3,m} \bmod p}$ για $\mathbf{m \neq j}$ και ανακοινώνει το $\mathbf{s_m}$ σε όλα τα μέλη. Κάθε μέλος υπολογίζει και ανακοινώνει δύο τιμές.
4. Όλα τα μέλη υπολογίζουν το αποτέλεσμα $\mathbf{v = s_1 + s_2 + s_3 \bmod p}$.

Για να αναλυθεί το πρωτόκολλο ασφαλής πρόσθεσης, ας εξηγηθεί πρώτα γιατί το αποτέλεσμα **v** αποτελεί το σωστό αποτέλεσμα. Ισχύει:

$$\mathbf{V = \sum_j s_j \bmod p = \sum_j \sum_i r_{i,j} \bmod p = \sum_i \sum_j r_{i,j} \bmod p = \sum_i x_i \bmod p}$$

Αυτό δείχνει ότι το πρωτόκολλο υπολογίζει το άθροισμα **modulo p** των εισόδων, ανεξάρτητα από το πώς επιλέγονται τα $\mathbf{x_i}$. Ωστόσο, αν τα μέρη επιλέξουν $\mathbf{x_i=1}$ για "ναι" και $\mathbf{x_i=0}$ για "όχι" και ισχύει ότι $\mathbf{p>3}$, τότε:

$$\sum_i \mathbf{x_i} \bmod \mathbf{p} = \sum_i \mathbf{x_i}$$

επειδή όλα τα $\mathbf{x_i}$ είναι 0 ή 1 και έτσι το άθροισμά τους δεν μπορεί να είναι μεγαλύτερο από το **p**. Έτσι, στην περίπτωση αυτή, το **v** είναι πράγματι ο αριθμός των θετικών ψήφων.

Τώρα, γιατί δεν υπάρχει καμία άλλη πληροφορία εκτός από το αποτέλεσμα **v** που διαρρέει σε οποιοδήποτε μέλος; Ας χρησιμοποιηθεί το $\mathbf{P_1}$ για παράδειγμα. Στο βήμα 1, τα $\mathbf{x_1}$, $\mathbf{x_2}$ και $\mathbf{x_3}$ διανέμονται κρυφά και έχει ήδη αποδειχθεί ότι αυτό δε γνωστοποιεί στο $\mathbf{P_1}$ τίποτα για τα $\mathbf{x_2}$, $\mathbf{x_3}$. Στο τελευταίο βήμα ανακοινώνονται τα $\mathbf{s_1}$, $\mathbf{s_2}$, $\mathbf{s_3}$. Σημειώνεται ότι το $\mathbf{P_1}$ γνωρίζει ήδη τα $\mathbf{s_2}$, $\mathbf{s_3}$, έτσι ώστε το $\mathbf{s_1}$ να είναι το μοναδικό νέο κομμάτι πληροφοριών. Ωστόσο, βλέποντας το $\mathbf{s_1}$ θα γνωστοποιηθεί στο $\mathbf{P_1}$ τι είναι το **v** και τίποτα περισσότερο. Ο λόγος για αυτό είναι ότι αν σε κάποιον δοθούν τα $\mathbf{s_2}$, $\mathbf{s_3}$, και **v**, μπορεί να υπολογίσει το $\mathbf{s_1 = v - s_2 - s_3 \bmod p}$. Με άλλα λόγια, δεδομένου του τι πρέπει να γνωρίζει το $\mathbf{P_1}$, δηλαδή το **v**, είναι εφικτό να υπολογιστεί ήδη τι θα του γνωστοποιηθεί από το πρωτόκολλο, δηλαδή το $\mathbf{s_1}$, και επομένως να μη γνωρίζει κάτι πέρα από το **v**.

Δεδομένου του αποτελέσματος, το $\mathbf{P_1}$ είναι στην πραγματικότητα ικανό να υπολογίσει κάποιες πληροφορίες σχετικά με τις ψήφους των άλλων. Ειδικότερα, αυτός μπορεί να υπολογίσει το $\mathbf{v - x_1 = x_2 + x_3}$, δηλαδή το άθροισμα των ψήφων των άλλων μελών. Είναι εύκολο να μπερδευτεί κανείς και να σκεφτεί ότι εξαιτίας αυτού, κάτι πρέπει να είναι λάθος στο πρωτόκολλο, αλλά στην πραγματικότητα δεν υπάρχει πρόβλημα: είναι αλήθεια ότι το $\mathbf{P_1}$ μπορεί να υπολογίσει το άθροισμα των ψήφων των $\mathbf{P_2}$ και $\mathbf{P_3}$, αλλά αυτό πηγάζει από τις πληροφορίες που το $\mathbf{P_1}$ πρέπει να γνωρίζει, δηλαδή το αποτέλεσμα και τα δικά του ορίσματα. Δεν υπάρχει τίποτα που μπορεί να κάνει το πρωτόκολλο για να στερήσει το $\mathbf{P_1}$ από αυτές τις πληροφορίες. Με άλλα λόγια, το καλύτερο που μπορεί να κάνει ένα πρωτόκολλο είναι να διασφαλίσει ότι τα μέλη μαθαίνουν μόνο ό, τι πρέπει να μάθουν και αυτό περιλαμβάνει οτιδήποτε μπορεί να αντληθεί από το όρισμα του ίδιου του μέλους και το επιδιωκόμενο αποτέλεσμα.

3.3.4 Ασφαλής πολλαπλασιασμός και matchmaking

Για να πραγματοποιηθούν γενικοί ασφαλείς υπολογισμοί, θα χρειαστεί να γίνουν περισσότερα από μια ασφαλή πρόσθεση. Αποδεικνύεται ότι το σχέδιο ασφαλής μετάδοσης, από την προηγούμενη υποενότητα, επιτρέπει ήδη να επιτευχθούν περισσότερα: είναι εφικτό επίσης να πραγματοποιηθεί ασφαλής πολλαπλασιασμός.

Έστω δύο αριθμοί **a**,**b** που ανήκουν στο $\mathbf{Z_p}$ έχουν μεταδοθεί κρυφά, όπως αναλύθηκε προηγουμένως, έτσι ώστε $\mathbf{a=a_1+a_2+a_3 \bmod p}$ και $\mathbf{b=b_1+b_2+b_3 \bmod p}$, και πρέπει να υπολογιστεί με ασφάλεια το **ab mod p**. Επομένως:

$$\mathbf{ab = a_1b_1 + a_1b_2 + a_1b_3 + a_2b_1 + a_2b_2 + a_2b_2 + a_3b_1 + a_3b_2 + a_3b_3 \bmod p}$$

Είναι εύκολο να καταλάβει κανείς τώρα αν τα $\mathbf{a_i}$ και $\mathbf{b_i}$ έχουν διανεμηθεί όπως περιγράφηκε προηγουμένως. Είναι γεγονός ότι για κάθε προϊόν $\mathbf{a_ib_j}$, υπάρχει τουλάχιστον ένα μέλος μεταξύ των τριών που γνωρίζει τα $\mathbf{a_i}$ και $\mathbf{b_j}$ και συνεπώς μπορεί να υπολογίσει το $\mathbf{a_ib_j}$. Για παράδειγμα, το $\mathbf{P_1}$ έχει λάβει τα $\mathbf{a_2}$, $\mathbf{a_3}$, $\mathbf{b_2}$, $\mathbf{b_3}$ και μπορεί επομένως να υπολογίσει τα $\mathbf{a_2b_2}$, $\mathbf{a_2b_3}$, $\mathbf{a_3b_2}$ και $\mathbf{a_3b_3}$. Η κατάσταση επομένως έχει ως εξής: το επιθυμητό αποτέλεσμα **ab** είναι το άθροισμα ορισμένων αριθμών, όπου κάθε επιμέρους άθροισμα μπορεί να υπολογιστεί από τουλάχιστον ένα από τα μέλη. Και το τελευταίο βήμα είναι ήδη γνωστό από το πρωτόκολλο ασφαλής πρόσθεσης! Ακολουθεί το πρωτόκολλο που προκύπτει από αυτές τις παρατηρήσεις.

Τα μέλη είναι τα $\mathbf{P_1}$, $\mathbf{P_2}$ και $\mathbf{P_3}$. Το όρισμα του $\mathbf{P_1}$ είναι το **a** που ανήκει στο $\mathbf{Z_p}$. Το όρισμα του $\mathbf{P_2}$ είναι το **b** που ανήκει -κι αυτό- στο $\mathbf{Z_P}$, όπου το **p** είναι μια αρχικοποιημένη σταθερή τιμή. Το $\mathbf{P_3}$ δεν έχει όρισμα.

1. Το $\mathbf{P_1}$ διανέμει τα $\mathbf{a_1}$, $\mathbf{a_2}$, $\mathbf{a_3}$ που αποτελούν κομμάτια του **a**, ενώ το $\mathbf{P_2}$ διανέμει τα $\mathbf{b_1}$, $\mathbf{b_2}$, $\mathbf{b_3}$ αντίστοιχα.
2. Το $\mathbf{P_1}$ υπολογίζει τοπικά το $\mathbf{u_1 = a_2b_2 + a_2b_3 + a_3b_2 \bmod p}$, το $\mathbf{P_2}$ υπολογίζει το $\mathbf{u_2 = a_3b_3 + a_1b_3 + a_3b_1 \bmod p}$ και το $\mathbf{P_3}$ υπολογίζει το $\mathbf{u_3 = a_1b_1 + a_1b_2 + a_2b_1 \bmod p}$.
3. Τα μέλη χρησιμοποιούν το πρωτόκολλο ασφαλής πρόσθεσης για τον ασφαλή υπολογισμό του αθροίσματος $\mathbf{u_1 + u_2 + u_3 \bmod p}$, όπου το $\mathbf{P_i}$ χρησιμοποιεί σαν όρισμα το $\mathbf{u_i}$.

Για να υποστηρίξει κάποιος ότι λειτουργεί, πρέπει να προσέξει πρώτα ότι η ορθότητα, δηλαδή το $\mathbf{ab = u_1 + u_2 + u_3 \bmod p}$, προκύπτει από τα προηγούμενα. Για να αποδειχθεί ότι δεν αποκαλύπτεται τίποτα εκτός από το **ab mod p**, παρατηρείται ότι τίποτα καινούργιο για τα **a**, **b** δεν αποκαλύπτεται στο πρώτο βήμα. Και επειδή το πρωτόκολλο ασφαλής πρόσθεσης είναι ιδιωτικό, δεν αποκαλύπτεται κάτι στο τελευταίο βήμα, εκτός από το άθροισμα των ορισμάτων και αυτό το ποσό ισούται πάντα με **ab mod p**.

Επιπλέον, ακόμη και σε μια πολύ απλή περίπτωση όπου και το **a** και το **b** είναι είτε 0 είτε 1, ο ασφαλής πολλαπλασιασμός έχει μια σημαντική εφαρμογή: έστω δύο μέλη, η **Alice** και ο **Bob**. Η **Alice** αναρωτιέται αν ο **Bob** θέλει να βγει μαζί της και ο **Bob** αναρωτιέται αν η **Alice** ενδιαφέρεται για αυτόν. Θα ήθελαν πάρα πολύ να μάθουν αν υπάρχει αμοιβαίο ενδιαφέρον, αλλά χωρίς να διατρέχουν τον κίνδυνο της αμηχανίας που θα προέκυπτε αν, για παράδειγμα, ο **Bob** πει στην **Alice** ότι ενδιαφέρεται και εκείνη τον απορρίψει. Το πρόβλημα μπορεί να λυθεί αν η **Alice** επιλέξει ένα **a** από το $\mathbf{Z_p}$, όπου ισχύει **a=1** αν ενδιαφέρεται για τον **Bob**, αλλιώς **a=0**. Με τον ίδιο τρόπο, ο **Bob** επιλέγει το **b** να είναι 0 ή 1. Κατόπιν, υπολογίζεται τη συνάρτηση **f(a,b) = ab mod p** με ασφάλεια. Είναι σαφές ότι το αποτέλεσμα είναι 1 αν και μόνο αν υπάρχει αμοιβαίο ενδιαφέρον. Ωστόσο, εάν, για παράδειγμα, η **Alice** δεν ενδιαφέρεται, θα επιλέξει **a=0**, και στην περίπτωση αυτή, δεν μαθαίνει τίποτα καινούργιο από το πρωτόκολλο. Με αυτόν τον τρόπο η ασφάλεια του πρωτοκόλλου υπονοεί ότι η μόνη (πιθανώς) νέα πληροφορία που θα μάθει η **Alice** είναι το αποτέλεσμα **ab mod p**. Αλλά ξέρει ήδη ότι το αποτέλεσμα θα είναι 0! Συγκεκριμένα, δε μαθαίνει αν ο **Bob** ενδιαφερόταν ή όχι, οπότε ο **Bob** είναι ασφαλής από την αμηχανία. Ομοίως, αυτό ισχύει και για την **Alice**. Αυτό το επιχείρημα προϋποθέτει, βεβαία, ότι και οι δύο παίκτες επιλέγουν τα ορίσματά τους ειλικρινά, σύμφωνα με τα πραγματικά τους συμφέροντα.

Από τον πρωτόκολλο του ασφαλή πολλαπλασιασμού, γίνεται σαφές ότι αν η **Alice** και ο **Bob** διαδραματίσουν τους ρόλους των $\mathbf{P_1}$ και $\mathbf{P_2}$ αντίστοιχα, πρέπει απλώς να βρουν ένα τρίτο μέλος για να τους βοηθήσει να κάνουν τον πολλαπλασιασμό με ασφάλεια. Είναι πιθανό αυτό το τρίτο μέλος να μην αποτελεί ένα απόλυτα αξιόπιστο τρίτο μέλος του είδους που συζητήσαμε νωρίτερα: δεν πρέπει να μάθει τίποτα για το **a** ή το **b** εκτός από **ab mod p**. Η **Alice** και ο **Bob** πρέπει να εμπιστευτούν ότι ο τρίτος δε μοιράζεται τις πληροφορίες του ούτε με τον **Bob** ούτε με την **Alice**.

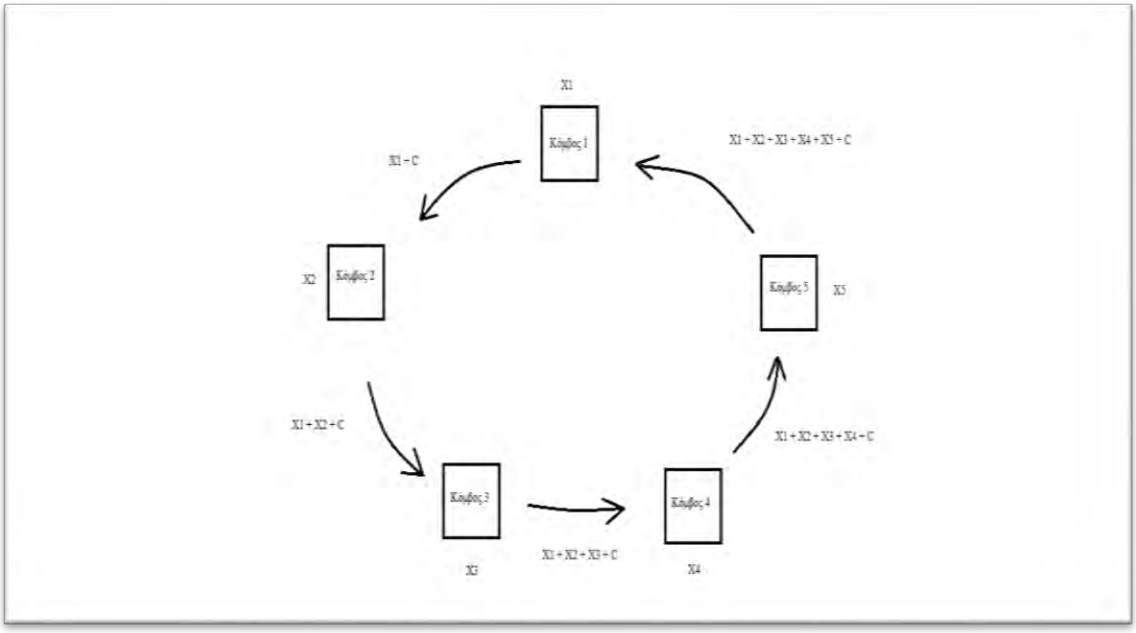
Ένα προφανές ερώτημα είναι εάν μπορεί κανείς να κάνει ασφαλές πολλαπλασιασμό μόνο με τη συμμετοχή της **Alice** και του **Bob**. Η απάντηση αποδεικνύεται να είναι θετική, αλλά τότε η θεωρητική πληροφορία της ασφάλειας δεν είναι δυνατή. Αντ' αυτού, πρέπει να χρησιμοποιηθούν λύσεις βασισμένες στην κρυπτογραφία. Τέτοιες λύσεις μπορούν πάντοτε να παραβιαστούν εάν ένα μέρος έχει αρκετή υπολογιστική ισχύ.

Για λόγους πληρότητας, υπογραμμίζεται ότι το πρόβλημα της **Alice** και του **Bob** είναι μια ειδική περίπτωση του λεγόμενου προβλήματος **"matchmaking"** που έχει κάπως πιο σοβαρές εφαρμογές. Στην περίπτωση μιας σειράς εταιρειών όπου κάθε εταιρεία έχει μια σειρά από άλλες εταιρείες που θα προτιμούσε να συνεργάζεται, πρέπει σε κάθε ζεύγος εταιρειών να γίνεται γνωστό αν υπάρχει αμοιβαίο ενδιαφέρον, αλλά χωρίς να υποχρεώνουν τις εταιρείες να αποκαλύπτουν τη στρατηγική τους, ανακοινώνοντας δημόσια τα συμφέροντά τους.

4.ΥΛΟΠΟΙΗΣΗ

4.1 Αρχιτεκτονική του συστήματος

Η γενική ιδέα της παρούσας πτυχιακής εργασίας, είναι η επικοινωνία μεταξύ κόμβων/χρηστών συνδεδεμένων σε μια κοινή πλατφόρμα. Πραγματοποιείται η καταμέτρηση των παλμών που είχε ο κάθε κόμβος/χρήστης σε ένα λεπτό. Οι κόμβοι αυτοί θα ανταλλάσσουν, σειριακά και κατ' επανάληψη, την απόκλιση του καρδιακού τους παλμού από μια μέση τιμή (Εικόνα 3). Η μέση τιμή αντιπροσωπεύει τον καρδιακό παλμό που αναμένεται να έχει ο χρήστης, σύμφωνα με την ηλικία και το φύλο του. Με αυτό τον τρόπο, γνωστοποιείται αν υπάρχει μεγάλη απόκλιση στους παλμούς, στο σύνολο των κόμβων/χρηστών, από την αναμενόμενη. Παραδείγματος χάριν, μια μεγάλη απόκλιση μπορεί να ερμηνευθεί ως αύξηση της καρδιακής λειτουργίας, η οποία οφείλεται σε κάποιο ερέθισμα ή σε σωματική άσκηση.



Εικόνα 3. Παράδειγμα με πέντε κόμβους/χρήστες.

Ο κάθε κόμβος, λοιπόν, αναλογεί σε ένα χρήστη του προγράμματος. Αναλυτικά, ο πρώτος κόμβος λειτουργεί λίγο διαφορετικά από τους υπόλοιπους, διότι έχει την ιδιότητα του εκκινητή της διαδικασίας. Έγινε χρήση μιας πλακέτας, του BITalino (Εικόνα 4), η οποία έχει σχεδιαστεί, ειδικά, για να καλύπτει τις απαιτήσεις των σημάτων του ανθρώπινου σώματος. Στη συγκεκριμένη περίπτωση, χρησιμοποιήθηκε ο αισθητήρας ηλεκτροκαρδιογραφίας και τα κατάλληλα ηλεκτρόδια, που συνδέονται στις παλάμες του χρήστη και πραγματοποιείται η καταγραφή των παλμών του. Ζητείται η καταχώρηση της ηλικίας και του φύλου του χρήστη, με σκοπό να υπολογιστεί ο αντιπροσωπευτικός καρδιακός παλμός. Το σύνολο, δηλαδή, των παλμών που αναμένεται να έχει σε ένα λεπτό ένας άνθρωπος με την αντίστοιχη ηλικία και φύλο. Στη συνέχεια, με διαίρεση υπολογίζεται η απόκλιση του πραγματικού παλμού από τον αντιπροσωπευτικό. Η τιμή αυτή θα αποτελέσει το μήνυμα που θα σταλεί στον επόμενο κόμβο/χρήστη, αφού πρώτα προστεθεί και ένας τυχαίος αριθμός, γνωστός μόνο στον πρώτο χρήστη, ώστε να διασφαλιστεί το απόρρητο των προσωπικών δεδομένων.

Εικόνα 4. BITalino.

Ο επόμενος, και κάθε επόμενος κόμβος/χρήστης, υπολογίζει την απόκλιση του καρδιακού παλμού του και την προσθέτει στην τιμή που έλαβε από τον προηγούμενο. Το τελικό άθροισμα θα σταλεί στον επόμενο κόμβο. Η διαδικασία αυτή θα συνεχιστεί μέχρι να φτάσουμε στον τελευταίο χρήστη, ο οποίος θα προσθέσει και αυτός με τη σειρά του την απόκλιση του καρδιακού του παλμού στην τιμή που έλαβε και θα τη στείλει στον πρώτο κόμβο. Ο πρώτος κόμβος θα αφαιρέσει τον τυχαίο αριθμό, που είχε –αρχικά- προσθέσει (για να προστατέψει το προσωπικό του δεδομένο), και θα του απομείνει το άθροισμα των αποκλίσεων όλων των χρηστών. Με τη μέθοδο αυτή διαφυλάσσονται οι προσωπικές τιμές του κάθε χρήστη και το μόνο που γίνεται γνωστό είναι το άθροισμα όλων των αποκλίσεων, χωρίς να διαφεύγει κάποια επιπλέον πληροφορία. Θα επαναληφθεί η διαδικασία μερικές φορές ακόμα, ώστε από τη μεταβολή της τελικής τιμής, που λαμβάνει κάθε φορά ο πρώτος κόμβος, να γίνει γνωστό και αν υπήρξε κάποια αξιοσημείωτη διαφοροποίηση στους καρδιακούς παλμούς των χρηστών.

Στην υποενότητα που ακολουθεί, θα γίνει αναφορά στο πιο πρακτικό κομμάτι της πτυχιακής εργασίας. Δηλαδή, θα αναλυθεί η χρήση και ο κώδικας του BITalino, οι δυσκολίες που προέκυψαν και πως ξεπεράστηκαν, καθώς και ο υπόλοιπος κώδικας υλοποίησης.

Σε αυτό το σημείο, πρέπει να αναφερθεί ότι χρησιμοποιήθηκαν υλοποιημένοι κώδικες για τις λειτουργίες του BITalino, τους οποίους έχουν δημιουργήσει οι Svein Petter Gjøby και Paulo Pires [34]. Οι κώδικες αυτοί παρέχονται ελεύθερα στο GitHub και διευκόλυναν πολύ στην υλοποίηση της εργασίας.

4.2 Εργαλεία και βιβλιοθήκες

4.2.1 Δημιουργία διαγραμμάτων

Μέσω της κλάσης **ChartMatrix** και με τη βοήθεια των βιβλιοθηκών org.knowm.xchart.* και org.knowm.xchart.style.markers.SeriesMarkers δημιουργούνται τα απαραίτητα διαγράμματα. Η μέθοδος **Matrix** δέχεται ως όρισμα έναν πίνακα τύπου double με περιεχόμενο τις τιμές που θα απεικονιστούν στο διάγραμμα.

4.2.2 Μετατροπή δειγμάτων από αναλογικά σε ψηφιακά

Η κλάση **SensorDataConverter** περιέχει τις μεθόδους που λαμβάνουν τα δείγματα από τους αισθητήρες σε αναλογική μορφή και τα μετατρέπουν στην ψηφιακή τους μορφή. Αυτό επιτυγχάνεται με μία μαθηματική εξίσωση, ξεχωριστή για κάθε αισθητήρα. Στην εργασία αυτή χρησιμοποιήθηκε ο αισθητήρας ηλεκτροκαρδιογραφίας (ECG) και η αντίστοιχη μέθοδος μετατροπής των δεδομένων.

Η μαθηματική εξίσωση που χρησιμοποιείται είναι:

$$\left(\frac{\left(\frac{raw}{2^{10}} - 0.5\right) 3.3}{1100}\right) 1000$$

Όπου raw τα δείγματα από τον αισθητήρα ECG.

4.2.3 Εύρεση μεγίστου

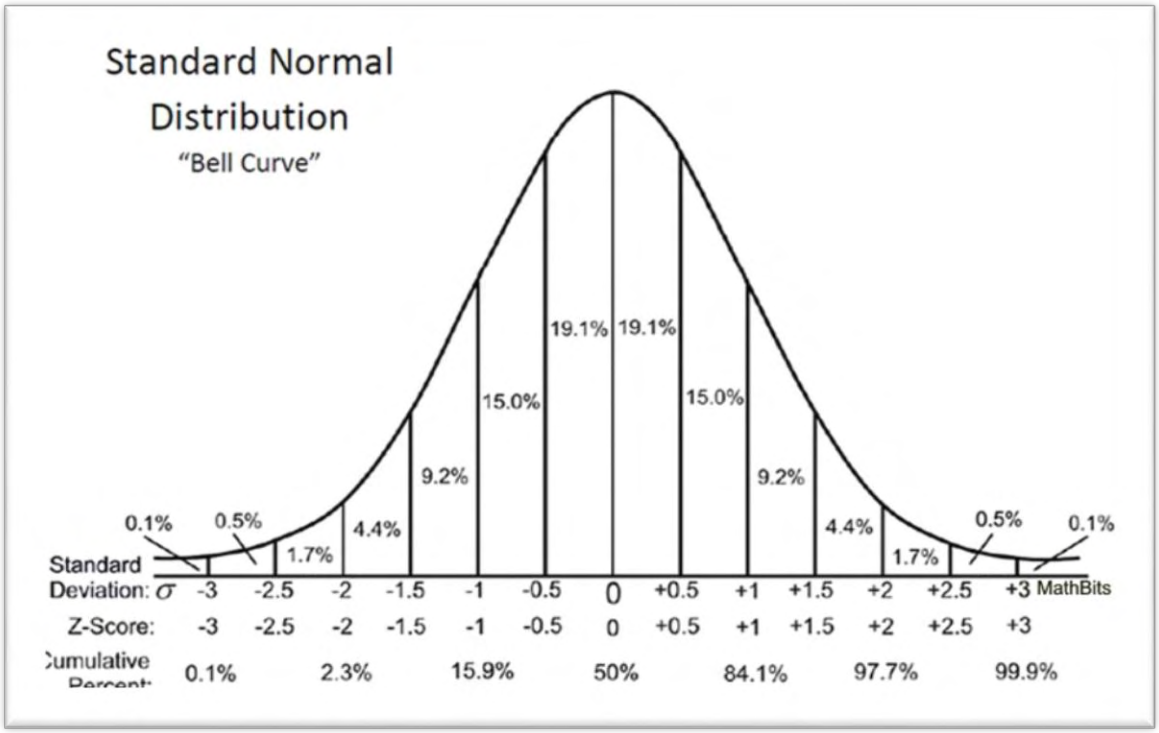
Για να βρεθεί ο μέγιστος αριθμός ενός πίνακα που έχει αποθηκευμένους integers, θεωρείται ως μέγιστη η πρώτη τιμή του πίνακα και ελέγχονται μία-μία οι υπόλοιπες τιμές του. Αν βρεθεί αριθμός μεγαλύτερος από αυτόν που θεωρήθηκε ως μέγιστος, γίνεται η αντικατάστασή του.

4.2.4 Κανονική κατανομή

Η κανονική κατανομή (ή Γκαουσιανή Συνάρτηση) [35] αναφέρεται σε συνεχείς μεταβλητές αποτελώντας μία συνεχή συνάρτηση πυκνότητας πιθανότητας. Χρησιμοποιείται ως μία πρώτη προσέγγιση για να περιγραφούν τυχαίες μεταβλητές πραγματικών τιμών, οι οποίες τείνουν να συγκεντρώνονται γύρω από μια μέση τιμή. Η κανονική κατανομή αποτελεί την πιο σημαντική κατανομή της στατιστικής μεθοδολογίας.

Με τη χρήση της μεθόδου **NormalDistribution()**, επιλέγεται μια τιμή κοντά στο μέσο όρο του εύρους τιμών, στο οποίο ανήκει ο πρώτος κόμβος/χρήστης. Η μέθοδος αυτή συμπεριφέρεται ακριβώς όπως η κανονική κατανομή (ή Γκαουσιανή συνάρτηση). Επιλέγει τυχαίες πραγματικές τιμές, οι οποίες τείνουν να συγκεντρώνονται γύρω από μια μέση τιμή (Εικόνα 9).

Η κανονική κατανομή χρησιμοποιείται στην κλάση **Menu** για την επιλογή ενός αριθμού κοντά στο μέσο όρο ενός εύρους τιμών. Απαραίτητη είναι η προσθήκη της βιβλιοθήκης org.apache.commons.math3.distribution.*.



Εικόνα 9. Διάγραμμα κανονικής κατανομής.

4.2.5 Βιβλιοθήκη bluecove

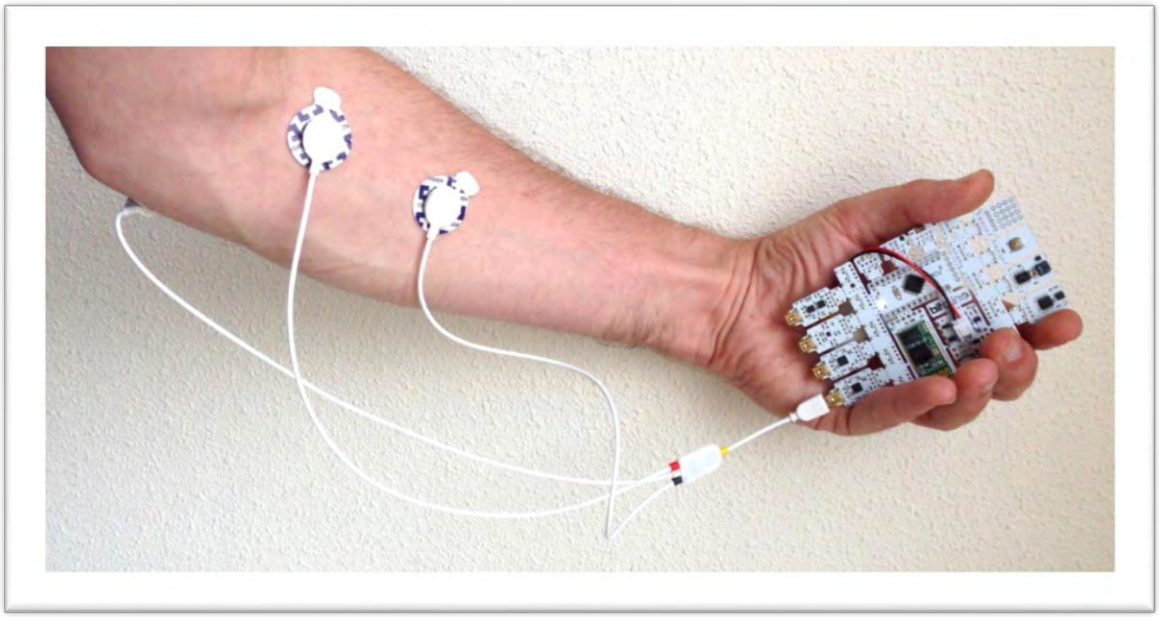
Η bluecove είναι μια βιβλιοθήκη της JAVA και σχετίζεται με τις λειτουργίες του Bluetooth. Είναι απαραίτητη για την ανάπτυξη του κώδικα, καθώς η συσκευή BITalino συνδέεται ασύρματα, μέσω Bluetooth, με τον υπολογιστή που τρέχει την εφαρμογή. Αναλυτικά, η εφαρμογή θα ψάξει τις συσκευές που είναι διαθέσιμες για σύνδεση μέσω Bluetooth, θα βρει το BITalino και θα κάνει τη ζεύξη. Με αυτόν τον τρόπο, η συσκευή θα μπορέσει να στείλει τα δείγματα στον υπολογιστή. Για όλα αυτά τα βήματα απαιτούνται εντολές που περιέχονται στη βιβλιοθήκη bluecove.

4.3 Hardware-BITalino

Το απαραίτητο στοιχείο, πάνω στο οποίο εξελίχθηκε η πτυχιακή εργασία, είναι το BITalino. Όπως αναφέρθηκε και προηγούμενα, πρόκειται για μια πλακέτα με αισθητήρες που έχουν την ικανότητα να διαβάζουν τα σήματα του ανθρώπινου σώματος. Η πλακέτα που χρησιμοποιήθηκε έχει έξι αναλογικά κανάλια αισθητήρων, με την εξής σειρά: αισθητήρα ηλεκτρομυογραφίας, αισθητήρα ηλεκτροδερμικής δραστηριότητας, αισθητήρα ηλεκτροκαρδιογραφίας (ο οποίος χρησιμοποιήθηκε για τη διεκπεραίωση της παρούσας πτυχιακής εργασίας), αξελερόμετρο, αισθητήρα φωτός και ένα ελεύθερο κανάλι για άλλα εξαρτήματα. Ωστόσο, σημαντικό είναι να σημειωθεί πως το BITalino δεν είναι ιατρική συσκευή ούτε προορίζεται για ιατρική διάγνωση.

Η γλώσσα που χρησιμοποιήθηκε για ολόκληρο τον κώδικα υλοποίησης είναι η JAVA. Επομένως, ψάξαμε στο διαδίκτυο για ελεύθερο «πακέτο» (kit) ανάπτυξης λογισμικού του BITalino σε JAVA.

Αρχικά, λοιπόν, ο χρήστης πρέπει να κολλήσει τα ηλεκτρόδια στις παλάμες του (Εικόνα 5) και έπειτα η πλακέτα να στείλει τα δεδομένα που θα συλλέξει στον υπολογιστή. Γι’ αυτό το λόγο γίνεται η σύνδεση του BITalino με τον υπολογιστή μέσω Bluetooth (η κάθε πλακέτα έχει τη δική της Bluetooth MAC διεύθυνση). Στη συνέχεια, ξεκινά η λήψη 3000 δειγμάτων από κάθε κανάλι. Επειδή, όμως, τα κανάλια είναι αναλογικά, πρέπει να γίνει μετατροπή των δειγμάτων (μόνο από τον αισθητήρα ηλεκτροκαρδιογραφίας, αφού μόνο αυτά θα χρειαστούμε) από αναλογική μορφή σε ψηφιακή, που είναι και αναγνώσιμη από τον άνθρωπο.



Εικόνα 5. Σύνδεση χρήστη με το BITalino.

Η ψηφιοποίηση των δειγμάτων επιτυγχάνεται με τις ακόλουθες μαθηματικές πράξεις:

$$\mathbf{ECG_V = (ECG_B * VCC / 2^n – VCC/2) / G_{ECG}}$$

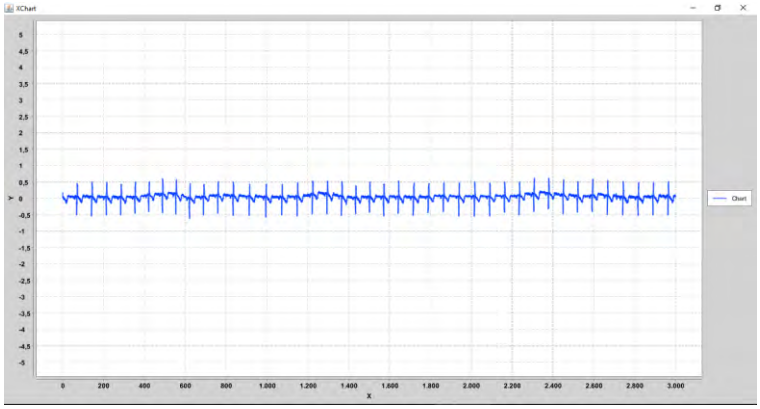
$$\mathbf{ECG_{mV} = ECG_V * 1000}$$

Όπου:

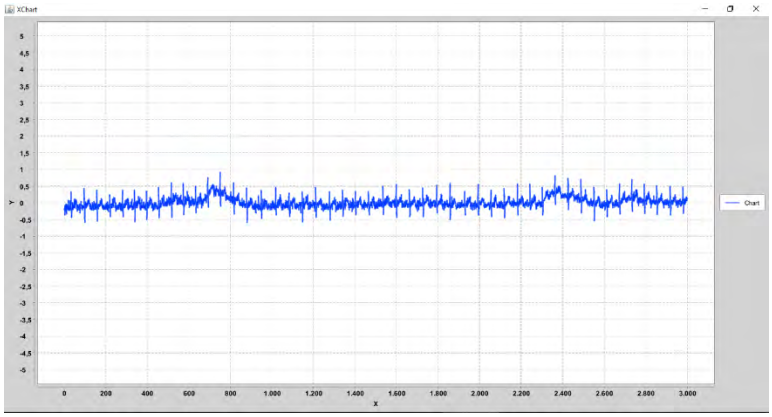
- ECG_V, η τιμή σε Volts
- ECG_B, τιμή που αποκτήθηκε από το BITalino
- VCC, η τιμή της τάσης λειτουργίας του BITalino (3.3V)
- n, αριθμός bits (10)
- G_{ECG}, χαρακτηριστική τιμή αισθητήρα ηλεκτροκαρδιογραφίας/ECG (1100)
- ECG_{mV}, η τιμή σε millivolts

Τα ψηφιακά, πλέον, αποτελέσματα, αποτυπώνονται σε ένα διάγραμμα, δημιουργώντας ένα καρδιογράφημα. Το πρόβλημα που δημιουργήθηκε σε αυτό το σημείο, αφορούσε την ανάπτυξη μιας μεθόδου καταμέτρησης των καρδιακών παλμών, διότι για κάθε άνθρωπο υπάρχουν διαφορετικές τιμές στα δείγματα, επομένως και διαφορετικά

καρδιογραφήματα (Εικόνες 6α και 6β). Με άλλα λόγια, η μέθοδος θα έπρεπε να προσαρμόζεται στα βιοσήματα κάθε ανθρώπου (που είναι εξαιρετικά δύσκολο) ή να πλησιάζει -όσο το δυνατόν περισσότερο- στο πραγματικό σύνολο των καρδιακών του παλμών.



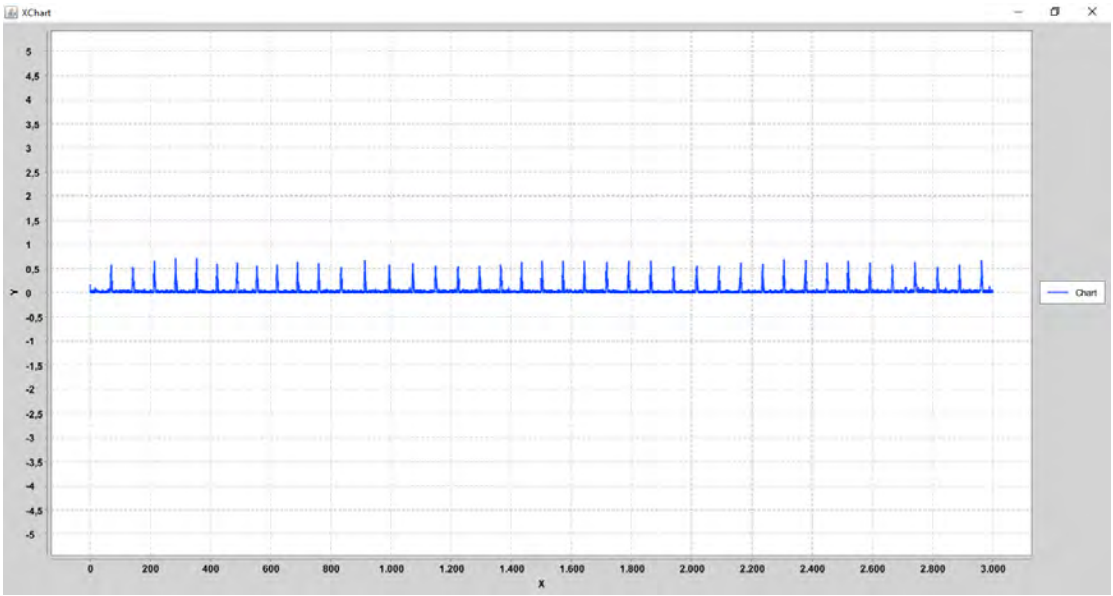
Εικόνα 6α. Παράδειγμα καρδιογραφήματος.



Εικόνα 6β. Παράδειγμα καρδιογραφήματος.

Το πρόβλημα αυτό αντιμετωπίστηκε ως εξής: υπολογίστηκαν οι αποστάσεις (κατ' απόλυτο τιμή) μεταξύ των δειγμάτων/σημείων και κατασκευάστηκε διάγραμμα με αυτές τις τιμές (Εικόνα 7). Σε κάθε απότομη αλλαγή, στο διάγραμμα αυτό,

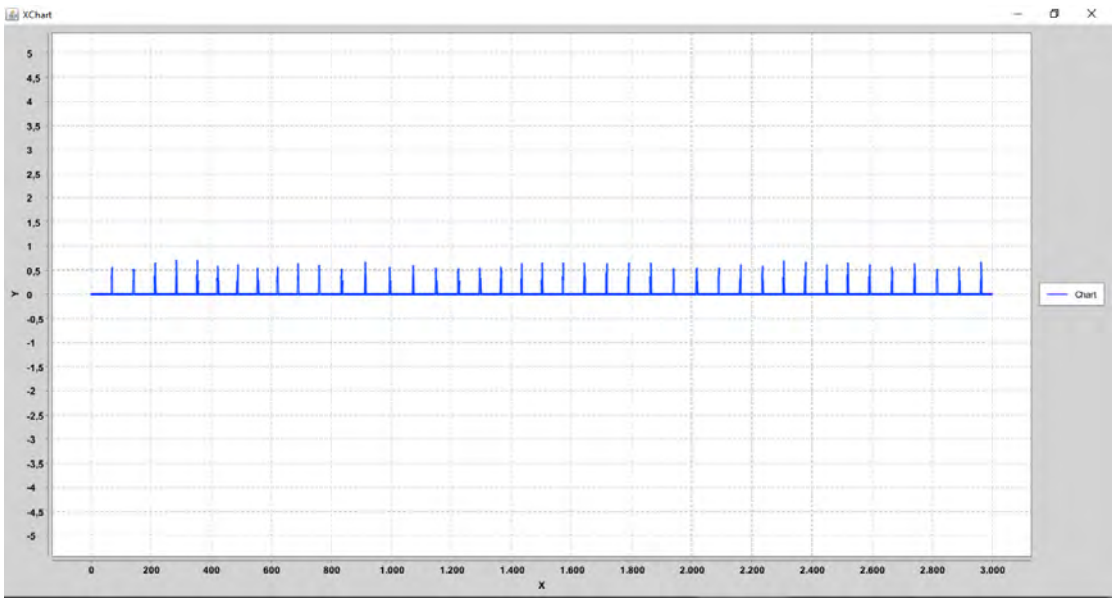
αναπαρίσταται και ένας παλμό. Μετά από πολλά δείγματα και πειράματα αποφασίστηκε μία τιμή (η τιμή 0.3), η οποία θα αντιπροσωπεύει το όριο πάνω από το οποίο σχεδιάζονται, κατά κόρον, οι κορυφές των παλμών στο καρδιογράφημα. Στόχος ήταν να μηδενιστούν όλες οι τιμές κάτω από το όριο αυτό και να απομείνουν οι κορυφές. Έτσι, υπολογίστηκε το μέγιστο των αποστάσεων και το πολλαπλασιάστηκε με την οριακή τιμή 0.3. Το αποτέλεσμα λειτούργησε ως οριακή τιμή στο διάγραμμα των αποστάσεων, δηλαδή μηδενίστηκαν όλες τις τιμές που ήταν μικρότερές της. Για την εξαγωγή ρεαλιστικών αποτελεσμάτων –όσο το δυνατόν πιο κοντά στα πραγματικά- και για να ελαχιστοποιηθεί η πιθανότητα καταμέτρησης παλμών που δεν υφίστανται, κρίθηκε απαραίτητη η επανάληψη της διαδικασίας.



Εικόνα 7. Διάγραμμα αποστάσεων.

Επομένως, θα οριστεί νέα οριακή τιμή για τις αποστάσεις μεταξύ των μη μηδενικών τιμών. Η τιμή θα οριστεί ως εξής: αφού πρώτα βρεθούν οι νέες αποστάσεις των μη μηδενικών τιμών που έχουν απομείνει, υπολογίζεται ο μέσος όρος τους. Αν υπάρχουν αποστάσεις μικρότερες του μέσου όρου αυξάνεται κάθε φορά η τιμή 0.3 κατά 0.1, ενώ αν υπάρχουν αποστάσεις μεγαλύτερες από 20 μονάδες από το μέσο όρο (η τιμή 20 είναι

εμπειρική) μειώνεται κάθε φορά κατά 0.1. Τέλος, η τιμή αυτή πολλαπλασιάζεται με το μέγιστο των αποστάσεων που υπολογίστηκε αρχικά. Στο επόμενο βήμα, μηδενίζουμε τις τιμές που είναι μικρότερες της νέας οριακής τιμής και δημιουργούμε νέο σχεδιάγραμμα (Εικόνα 8).



Εικόνα 8. Διάγραμμα νέων αποστάσεων.

Σε αυτό το σημείο, πραγματοποιείται η καταμέτρηση των παλμών του χρήστη που είναι συνδεδεμένος με το BITalino. Θεωρούμε ότι έχουμε παλμό αν και μόνο αν μία μη μηδενική τιμή προηγείται αλλά και έπεται από δύο εκάστοτε μηδενικές τιμές. Με αυτόν το γνώμονα υπολογίζεται το πλήθος των παλμών.

Οι κλάσεις που αφορούν το BITalino και προήλθαν από το «πακέτο» λογισμικού που βρέθηκε στο GitHub, είναι οι εξής:

1. Η κλάση **BITalinoErrorTypes**, που μας βοηθάει στην αναγνώριση σφαλμάτων όπως:

i. Η συσκευή δεν κατάφερε να συνδεθεί μέσω Bluetooth.
ii. Δεν ήταν δυνατή η προετοιμασία της θύρας επικοινωνίας. Δεν ήταν δυνατή η ρύθμιση των παρεχόμενων παραμέτρων.
iii. Ο ρυθμός δειγματοληψίας που επιλέξατε δεν μπορεί να οριστεί στο BITalino. Επιλέξτε 1000, 100, 10 ή 1.
iv. Ο υπολογιστής έχασε την επικοινωνία.
v. Ο αριθμός των διαθέσιμων αναλογικών καναλιών είναι μεταξύ 0 και 5.

και άλλα.

2. Η κλάση **BITalinoException**, που μας τυπώνει εξαιρέσεις που είναι πιθανό να συμβούν σε ένα «μπλοκ» εντολών.

3. Η κλάση **DeviceDescoverer**, που από το όνομά της γίνεται κατανοητό ότι βρίσκει συσκευές για σύνδεση μέσω Bluetooth. Κάνει σάρωση για να καταγράψει τα ονόματα των διαθέσιμων συσκευών και μας ενημερώνει αν η σάρωση ολοκληρώθηκε, τερματίστηκε ή είχε σφάλματα.

4. Η κλάση **SensorDataConverter**, η οποία μετατρέπει τις αναλογικές τιμές, που λαμβάνονται από τους αισθητήρες του BITalino, σε ψηφιακές. Για κάθε κανάλι/αισθητήρα υπάρχει μέθοδος με την κατάλληλη μαθηματική εξίσωση, που επιτυγχάνει την ψηφιοποίηση των δεδομένων που αποκτήθηκαν από το BITalino.

5. Η κλάση **Frame**, η οποία χρησιμοποιείται για την ανάλυση/αποκρυπτογράφηση του μηνύματος που λήφθηκε από το BITalino. Τα μηνύματα που στέλνει το BITalino είναι ακατέργαστες αλληλουχίες από bytes και μετουσιώνονται σε μία από τις τρεις παρακάτω πιθανές μορφές:
   i. Σε αλληλουχία αριθμών, που αυξάνεται κατά μία μονάδα σε κάθε διαδοχικό καρέ, και υπερχειλίζει στο 0 μετά το 15 (είναι ένας αριθμός 4-bit). Αυτός ο αριθμός μπορεί να χρησιμοποιηθεί για να ανιχνεύσει αν τα πλαίσια χάθηκαν κατά τη μετάδοση δεδομένων.

ii. Σε πίνακα τιμών (έξι θέσεων) αναλογικών εισόδων (0 ... 1023 στα πρώτα 4 κανάλια και 0 ... 63 στα υπόλοιπα κανάλια).

iii. Σε πίνακα (τεσσάρων θέσεων) που περιέχει την κατάσταση των θυρών (false για χαμηλό επίπεδο ή true για υψηλό επίπεδο).

6. Η κλάση **BITalino**, η οποία χρησιμοποιώντας σχεδόν όλες τις παραπάνω κλάσεις συνδέει τον υπολογιστή με το BITalino και συλλέγει τα δεδομένα. Η σύνδεση δημιουργείται με τη μέθοδο BITalino.open () και απελευθερώνεται με τη μέθοδο BITalino.close ().
7. Η κλάση **ChartMatrix**, δημιουργεί σύστημα αξόνων X, Y πλάτους 600 και ύψους 400 στο οποίο σχεδιάζονται τα καρδιογραφήματα και οι αποστάσεις μεταξύ των παλμών (Εικόνες 6α, 6β, 7, 8).

8. Και τέλος, η κλάση **Readfrombitalino**, χρησιμοποιεί όλες τις κλάσεις που αναφέρθηκαν, με σκοπό την εύρεση του πλήθους παλμών του χρήστη (όπως παρουσιάστηκε στην υποενότητα αυτή).

4.4 Software

Ο κώδικας έχει δύο λειτουργίες, καθώς ο πρώτος κόμβος διαφοροποιείται από τους υπόλοιπους, αφού πρέπει να παίξει το ρόλο τον εκκινητή της διαδικασίας. Τα δύο χαρακτηριστικά κάθε κόμβου είναι μια διεύθυνση IP και μια πόρτα.

Η διεύθυνση IP (Internet Protocol), είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών. Οι συσκευές αυτές, εκτός από ηλεκτρονικοί υπολογιστές, μπορεί να είναι δρομολογητές (routers), εκτυπωτές, μηχανές για fax μέσω Internet, και ορισμένα τηλέφωνα. Όλες αυτές πρέπει να έχουν τη δική τους μοναδική διεύθυνση. Για καλύτερη κατανόηση, μπορεί να υπάρξει ταύτιση μεταξύ μιας διεύθυνσης IP και μιας διεύθυνσης κατοικίας. Όπως κάθε διεύθυνση κατοικίας (με την οδό, τον αριθμό και τον

ταχυδρομικό κώδικα) αντιστοιχεί σε ένα κτήριο, έτσι και μια IP address χρησιμοποιείται για την αναγνώριση ενός υπολογιστή ή άλλης συσκευής που συνδέεται στο δίκτυο [36].

Σε ένα δίκτυο υπολογιστών, η πόρτα αποτελεί ένα τελικό σημείο επικοινωνίας σε ένα λειτουργικό σύστημα. Ενώ ο όρος χρησιμοποιείται και για φυσικές συσκευές, στο λογισμικό είναι ένα λογικό κατασκεύασμα που αναγνωρίζει μια συγκεκριμένη διαδικασία ή έναν τύπο υπηρεσίας δικτύου [37].

Με λίγα λόγια, η διεύθυνση IP και η πόρτα χρησιμοποιούνται για να γίνεται γνωστό, κάθε στιγμή, ποιος κόμβος στέλνει σε ποιον μήνυμα.

Αφού εξηγήθηκε τι είναι η διεύθυνση IP και η πόρτα, στη συνέχεια θα παρουσιαστεί η υπόλοιπη υλοποίηση.

4.4.1 Πρώτη λειτουργία

Αρχικά, δημιουργείται μια τυχαία τιμή, με τη χρήση της μεθόδου **Random()**, που θα χρειαστεί αργότερα. Στη συνέχεια, ζητούνται δύο πληροφορίες από το χρήστη, η ηλικία του και το φύλο του, οι οποίες εκχωρούνται από το πληκτρολόγιο και στέλνονται σαν όρισμα στη μέθοδο **menu**. Στη μέθοδο **menu**, έχουν χωριστεί σε περιπτώσεις οι ομάδες ηλικιών και σε υποπεριπτώσεις τα δύο φύλα. Με βάση τις πληροφορίες που έδωσε ο χρήστης, θα αντιστοιχηθεί σε μια υποπερίπτωση. Η κάθε υποπερίπτωση έχει ένα δικό της εύρος τιμών, που αντιστοιχούν στους αριθμούς καρδιακών παλμών ανά λεπτό, που αναμένεται να έχει ο χρήστης σύμφωνα πάντα με τα χαρακτηριστικά του (όπως παρουσιάζονται στον Πίνακα 1).

Όταν επιλεχθεί η κατάλληλη κατηγορία για το συγκεκριμένο χρήστη, επιλέγεται και η μέση τιμή από το εύρος τιμών στο οποίο έχει καταταχθεί. Η μέθοδος **menu** επιστρέφει μια συμβολοακολουθία (String) της μορφής:

hr + " " + average

Όπου:

- hr, η τιμή καρδιακών παλμών ανά λεπτό
- average, ο μέσος όρος ή μέση τιμή που αναφέρθηκε

Επομένως η συμβολοακολουθία αποτελείται από δύο δεκαδικούς αριθμούς χωρισμένους με κενά.

Χρησιμοποιούμε τη μέθοδο **split()** με όρισμα το κενό (" "), για να σπάσει τη συμβολοακολουθία στους δύο δεκαδικούς αριθμούς. Ο κάθε αριθμός εκχωρείται στο αντίστοιχο κελί ενός πίνακα (ο πρώτος αριθμός στο κελί 0 και ο δεύτερος στο κελί 1).

Δημιουργούνται δύο λίστες, οι οποίες θα χρησιμοποιηθούν ως όρισμα στην κλήση της συνάρτησης **rualive()**. Με την προϋπόθεση ότι όλοι οι κόμβοι χρησιμοποιούν την ίδια πόρτα, ο εκκινητής/πρώτος κόμβος ψάχνει τους υπόλοιπους διαθέσιμους με γνώμονα τη δική του IP διεύθυνση. Για παράδειγμα αν η IP του είναι η 192.168.22.5, θα ψάξει για χρήστες συνδεδεμένους στο ίδιο τοπικό δίκτυο με τις υπόλοιπες 254 διευθύνσεις (από την 192.168.22.0 μέχρι την 192.168.22.255, εκτός της δικής του). Η πρώτη λίστα, λοιπόν, θα έχει την κοινή πόρτα των κόμβων και η δεύτερη τις διευθύνσεις IP.

Η μέθοδος **rualive()** συγκεντρώνει σε μια λίστα τις πόρτες και τις διευθύνσεις των ενεργών κόμβων. Κάθε κελί της λίστας αυτής έχει μια συμβολοακολουθία της μορφής: **IP PORT**. Ένα String και έναν Integer (ακέραιο αριθμό) χωρισμένα με ένα κενό. Για να γίνει αντιληπτό αν ένας κόμβος είναι ενεργός ή όχι, γίνεται προσπάθεια αποστολής ενός μηνύματος στον πρώτο κόμβο από τις δύο λίστες που δόθηκαν σαν όρισμα στη μέθοδο. Στη συνέχεια, «ανοίγει» η πόρτα του πρώτου κόμβου και αναμένεται απάντηση. Αν δεν έρθει απάντηση ο κόμβος δεν είναι ενεργός και γίνεται μετάβαση στον επόμενο μέχρι το τέλος των δύο λιστών. Αν, όμως, έρθει μήνυμα εκχωρείται στη λίστα που, τελικά, θα επιστραφεί στον πρώτο κόμβο.

Χρησιμοποιείται και πάλι η μέθοδος **split()** για την κατασκευή δύο νέων λιστών, από τη λίστα που επέστρεψε η μέθοδος **rualive()**. Η πρώτη θα περιέχει τις διευθύνσεις IP και η δεύτερη τις πόρτες των ενεργών κόμβων.

Στη συνέχεια, μέσω της μεθόδου **rfb()** (που ανήκει στην κλάση Readfrombitalino), θα επιστραφεί ο αριθμός των καρδιακών παλμών του πρώτου χρήστη. Ο τρόπος που επιτυγχάνεται αυτό έχει παρουσιαστεί και αναλυθεί σε προηγούμενη ενότητα.

Ο αριθμός των καρδιακών παλμών αποθηκεύεται σε μια λίστα. Όταν η λίστα γεμίσει με δέκα τιμές, στην ενδέκατη θα διαγραφεί η πρώτη καταχώρηση και θα προστεθεί η νέα τιμή. Σκοπός είναι να υπάρχουν αποθηκευμένες έως δέκα τιμές, οι πιο πρόσφατες.

Για τον υπολογισμό της απόκλισης του πρώτου κόμβου θα συμμετέχουν δύο τιμές. Η μέση τιμή που έδωσε η μέθοδος **menu()** και η απόκλιση που θα υπολογιστεί από τις αποθηκευμένες τιμές της λίστας.

Αυτό επιτυγχάνεται με τον εξής τρόπο:

1. Θέτουμε ως $\mathbf{r_c}$ τη μετρούμενη τιμή και ως $\mathbf{r_t}$ την τυπική τιμή. Έστω ότι έχουμε **n** πρόσφατες μετρήσεις ($\mathbf{v_1},\ldots,\mathbf{v_2}$).

2. Εάν $\mathbf{n \geq 10}$ τότε $\mathbf{v_{normal}} = \frac{1}{2}\mathbf{r_t} + \frac{1}{2}\frac{\sum_{i=1}^{10} v_i}{10}$.

3. Εάν $\mathbf{n < 10}$ τότε $\mathbf{v_{normal}} = \frac{1}{2}\mathbf{r_t} + \frac{1}{2}\frac{10-n}{10}\mathbf{r_t} + \frac{1}{2}\frac{n}{10}\frac{\sum_{i=1}^{n} v_i}{n}$.

4. Οπότε μετά η απόκλιση είναι $\mathbf{dev} = \frac{r_c}{v_{normal}}$.

Το κλάσμα των δύο αυτών τιμών αποτελεί και την απόκλιση του πρώτου κόμβου/χρήστη, από την τιμή που αναμενόταν να έχει με βάση το φύλο και την ηλικία του.

Στην απόκλιση θα προστεθεί και ο τυχαίος αριθμός που υπολογίστηκε στην αρχή του κώδικα. Με αυτόν τον τρόπο, όταν ο τρέχων κόμβος στείλει την τελική τιμή στον επόμενο κόμβο, ο δεύτερος δε θα μπορέσει να μάθει την απόκλιση του πρώτου.

Η επιλογή του κόμβου στον οποίο θα στείλει ο πρώτος κόμβος γίνεται τυχαία, από τη λίστα που έστειλε η μέθοδος **rualive()** (η τυχαία επιλογή γίνεται με τη χρήση της μεθόδου **Math.random()**). Εάν, για κάποιο λόγο, ο κόμβος που επιλέχθηκε δεν είναι πλέον ενεργός και διαθέσιμος, θα διαγραφεί από τη λίστα των ενεργών, καθώς θα διαγραφούν η πόρτα του και η διεύθυνση IP του από τις αντίστοιχες λίστες (οι λίστες αυτές είχαν προκύψει -με τη βοήθεια της μεθόδου **split()**- από τη λίστα που επέστρεψε η μέθοδος **rualive()**). Η διαδικασία συνεχίζεται μέχρι να βρεθεί ενεργός κόμβος. Επειδή θα χρησιμοποιηθεί αυτός ο κόμβος, θα πρέπει να διαγραφεί από τις τρεις λίστες, έτσι όπως διαγράφτηκαν και οι μη ενεργοί.

Τότε θα του σταλεί το μήνυμα:

z + " " + PORT1 + " " + HOST + "-" + pList.get()

Όπου:

- z, το άθροισμα της απόκλισης με τον τυχαίο αριθμό.
- PORT1, η πόρτα του πρώτου κόμβου.
- HOST, η διεύθυνση IP του πρώτου κόμβου.
- pList.get(), οι πόρτες και οι διευθύνσεις των κόμβων που απέμειναν.

Τέλος, ο πρώτος κόμβος περιμένει να περάσει το μήνυμα από κόμβο σε κόμβο και ο τελευταίος να του στείλει το άθροισμα όλων των αποκλίσεων. Το μήνυμα λαμβάνεται ως συμβολοακολουθία, οπότε πρέπει να μετατραπεί σε δεκαδικό (double). Τώρα μπορεί να αφαιρεθεί ο τυχαίος αριθμός -που μόνο αυτός γνωρίζει- και να τυπωθεί το «καθαρό» άθροισμα των αποκλίσεων.

Ο κώδικας επαναλαμβάνεται από το σημείο που δημιουργούνται ο πίνακας με τις πόρτες των ενεργών κόμβων και ο πίνακας με τις διευθύνσεις IP τους. Σε κάθε επανάληψη μπορεί να παρατηρηθεί η μεταβολή στο άθροισμα των αποκλίσεων.

4.4.2 Δεύτερη λειτουργία

Στη συνέχεια θα αναλυθεί η δεύτερη λειτουργία του κώδικα, η οποία αφορά τους ενδιάμεσους χρήστες. Όπως και ο πρώτος κόμβος, έτσι και οι υπόλοιποι κόμβοι που θα ακολουθήσουν έχουν δύο χαρακτηριστικά, μια διεύθυνση IP και μία πόρτα.

Ξεκινώντας, όπως στον πρώτο χρήστη, έτσι και στους υπόλοιπους, ζητούνται δύο πληροφορίες, η ηλικία και το φύλο τους. Ακολουθεί ένα «μπλοκ» κώδικα **try-catch,** στο οποίο ο κόμβος «ανοίγει» την πόρτα του και περιμένει ένα μήνυμα. Το μήνυμα στέλνεται από τον πρώτο κόμβο και είναι ένα String με τη διεύθυνσή του και την πόρτα του χωρισμένα με ένα κενό. Με βάση αυτό το κενό η μέθοδος **split()** θα «σπάσει» το μήνυμα, του οποίου τα δύο μέρη θα αποθηκευτούν σε έναν πίνακα δύο θέσεων.

Στο επόμενο «μπλοκ» **try-catch**, ο κόμβος θα στείλει μια απάντηση στον αρχικό κόμβο που θα έχει τη μορφή:

HOST + "/" + PORT1

Όπου:

- HOST, η διεύθυνση IP του κόμβου (δηλαδή το String localhost).
- PORT1, η πόρτα του κόμβου.

Το μήνυμα αυτό προστίθεται στη λίστα με τους ενεργούς κόμβους που κατασκευάζεται στη λειτουργία του πρώτου χρήστη.

Στη συνέχεια ξεκινάει η επανάληψη όλων των εντολών που θα ακολουθήσουν. Έπονται δύο «μπλοκ» **try-catch**. Στο πρώτο, ο κόμβος «ανοίγει» την πόρτα του και περιμένει έναν άλλον κόμβο να συνδεθεί μαζί του. Στο δεύτερο, λαμβάνει ένα μήνυμα από τον κόμβο που μόλις συνδέθηκε.

Το μήνυμα αυτό κουβαλάει πολλές πληροφορίες. Είναι ένα String που αναπτύσσεται και διαμορφώνεται ως εξής:

απόκλιση + " " + PORT1 + " " + IP1 + " " + PORT2 + " " + PORT3+ "-" + IP4 + "/" + PORT4 + " " + IP5 + "/" + PORT5

Αναλυτικά, το πρώτο μέρος του μηνύματος περιέχει:

1. το τρέχον άθροισμα των αποκλίσεων
2. την πόρτα του πρώτου κόμβου/χρήστη
3. τη διεύθυνση IP του πρώτου κόμβου/χρήστη
4. τις πόρτες των κόμβων που χρησιμοποιήθηκαν

και το δεύτερο μέρος έχει τις διευθύνσεις IP και τις αντίστοιχες πόρτες των ενεργών κόμβων που δεν έχουν χρησιμοποιηθεί ως τώρα. Τα δύο μέρη είναι χωρισμένα μεταξύ τους με μία παύλα και τα επιμέρους στοιχεία τους ή με ένα κενό ή με μία πλάγια γραμμή (/).

Σε μία καινούρια μεταβλητή String αποθηκεύονται τα στοιχεία του πρώτου κόμβου και οι πόρτες των κόμβων που έχουν χρησιμοποιηθεί. Η μεταβλητή αυτή θα βοηθήσει στη σύνταξη του μηνύματος που θα στείλει ο τρέχων κόμβος στον επόμενο.

Σε μια λίστα εκχωρούνται τα στοιχεία των διαθέσιμων κόμβων (η διεύθυνση IP και η πόρτα ενός κόμβου καταλαμβάνει ένα κελί της λίστας). Δημιουργούνται άλλες δύο λίστες όπου η μία θα έχει μόνο τις διευθύνσεις και η άλλη μόνο τις πόρτες.

Για την επίτευξη των παραπάνω ενεργειών, χρησιμοποιείται η μέθοδος **split()** με το κατάλληλο όρισμα (κενό, παύλα ή πλάγια γραμμή).

Στη συνέχεια, επιλέγεται τυχαία, από τη λίστα με τις διευθύνσεις των ενεργών κόμβων, ο κόμβος στον οποίο θα στείλει ο τρέχων το μήνυμα. Γίνεται προσπάθεια σύνδεσης και αν η προσπάθεια αυτή –για κάποιο λόγο- αποτύχει, διαγράφονται τα στοιχεία του από τη λίστα ενεργών κόμβων, καθώς και από τις λίστες με τις διευθύνσεις και τις πόρτες.

Αν η προσπάθεια, όμως, είναι επιτυχής πρέπει να διαγραφούν τα στοιχεία του κόμβου με τον οποίο συνδέθηκε ο τρέχων κόμβος. Τα στοιχεία του βρίσκονται σε τρεις λίστες. Στη λίστα με τους ενεργούς κόμβους, στη λίστα με τις διευθύνσεις IP και στη λίστα με τις πόρτες.

Σε κάθε επανάληψη, έχουμε και νέο αριθμό παλμών από το BITalino (η διαδικασία που αφορά το BITalino και την αναγνώριση των παλμών, είναι η ίδια με αυτή που παρουσιάστηκε και αναλύθηκε στη λειτουργία του πρώτου χρήστη). Κάθε αριθμός παλμών, λοιπόν, που υπολογίζεται θα αποθηκεύεται σε μια λίστα δέκα θέσεων. Αν η λίστα γεμίσει, διαγράφεται η πρώτη καταχώριση και γίνεται προσθήκη της νέας τιμής.

Όπως και στον πρώτο κόμβο/χρήστη, ομοίως κι εδώ υπολογίζεται η απόκλιση του τρέχοντος κόμβου, συνυπολογίζοντας το μέσο όρο που στάλθηκε από τη μέθοδο **menu()** και την απόκλιση που έχουν οι αποθηκευμένοι αριθμοί παλμών. Για να βρεθεί η απόκλιση των αριθμών που έχουν αποθηκευτεί ακολουθούνται τα ίδια βήματα με αυτά της πρώτης λειτουργίας:

1. Θέτουμε ως $\mathbf{r_c}$ τη μετρούμενη τιμή και ως $\mathbf{r_t}$ την τυπική τιμή. Έστω ότι έχουμε **n** πρόσφατες μετρήσεις ($\mathbf{v_1}$,…,$\mathbf{v_2}$).

2. Εάν $\mathbf{n \geq 10}$ τότε $\mathbf{v_{normal} = \frac{1}{2} r_t + \frac{1}{2} \frac{\sum_{i=1}^{10} v_i}{10}}$.

3. Εάν $\mathbf{n < 10}$ τότε $\mathbf{v_{normal} = \frac{1}{2} r_t + \frac{1}{2} \frac{10-n}{10} r_t + \frac{1}{2} \frac{n}{10} \frac{\sum_{i=1}^{n} v_i}{n}}$.

4. Οπότε μετά η απόκλιση είναι $\mathbf{dev = \frac{r_c}{r_{normal}}}$.

Στις επόμενες εντολές του κώδικα, υπολογίζεται το ποσοστό στο οποίο επηρεάζεται η εύρεση της τελικής απόκλισης, από τις δύο τιμές. Παρακάτω δίνεται ένα πιο λεπτομερές παράδειγμα.

Έστω ότι υπάρχουν αποθηκευμένες οι τιμές 77, 76 και 77. Στην τελευταία επανάληψη, η μέθοδος **menu()** έστειλε τον αριθμό 78 και το μέσο όρο 76.

Ισχύει n<10.

Αθροίζονται όλες οι τιμές: 77+76+77+78=308.

Διαιρούνται με το 10: 308/10=30.8.

Το αποτέλεσμα πολλαπλασιάζεται με το $\frac{1}{2} : \frac{30.8}{2} = 15.4$.

Υπολογίζεται το $\mathbf{\frac{1}{2}\frac{10-n}{10}\,r_t} : \mathbf{\frac{1}{2}\frac{10-4}{10}}\,76 = 22.8$.

Υπολογίζεται το $\mathbf{\frac{1}{2}\,r_t} = 38$.

Η απόκλιση θα είναι το αποτέλεσμα της πρόσθεσης των τριών αποτελεσμάτων:

15.4 + 22.8 + 38 = 76.2.

Αφού υπολογίστηκε η απόκλιση του χρήστη, προστίθεται στο άθροισμα των αποκλίσεων που είχε λάβει από τον προηγούμενο χρήστη. Η σύνταξη των μηνυμάτων που στέλνονται και λαμβάνονται έχουν πάντα την ίδια μορφή. Η μορφή αυτή παρουσιάστηκε όταν αναλύθηκε το μήνυμα που έλαβε ο χρήστης.

Στις επόμενες γραμμές του κώδικα, ελέγχεται η περίπτωση να έχει αδειάσει η λίστα των ενεργών κόμβων (δηλαδή να υπήρχαν ένας ή περισσότεροι υποψήφιοι κόμβοι για να σταλεί μήνυμα, αλλά για κάποιο λόγο η σύνδεση μαζί τους δεν είναι εφικτή) ή να υπάρχει άδεια λίστα (δηλαδή στο δεύτερο μέρος του μηνύματος, εκεί που θα έπρεπε να υπάρχουν τα στοιχεία των ενεργών κόμβων (μετά την παύλα), δεν υπάρχουν πληροφορίες).

Αυτό σημαίνει ότι αποτελεί τον τελευταίο κόμβο, και για να κλείσει ο κύκλος, το μήνυμά του πρέπει να σταλεί στον πρώτο. Επομένως, συνδέεται με τον πρώτο κόμβο/χρήστη και ακολουθεί τα ίδια βήματα, όπως και οι προηγούμενοι κόμβοι. Δηλαδή, υπολογίζεται αριθμός παλμών μέσω της μεθόδου **menu()**, αποθηκεύεται στη λίστα και υπολογίζεται η τελική απόκλιση. Στον πρώτο κόμβο επιστρέφεται μόνο το άθροισμα των αποκλίσεων.

Με την αποστολή του αθροίσματος στον πρώτο κόμβο έχει κλείσει ο πρώτος κύκλος και τρέχουν επαναληπτικά τα τμήματα του κώδικα που περιβάλλονται από βρόγχους. Όσες περισσότερες επαναλήψεις οριστούν στον πρώτο κόμβο τόσα περισσότερα αποτελέσματα θα δοθούν για μελέτη.

4.5 Προβλήματα

4.5.1 Εύρεση οριακής τιμής

Για να βρεθεί ο αριθμός παλμών του χρήστη που είναι συνδεδεμένος με το BITalino, πραγματοποιήθηκαν κάποιες μαθηματικές πράξεις με τα δείγματα που δόθηκαν από τη συσκευή. Η εύρεση αυτής της μαθηματικής μεθόδου. για την επίλυση αυτού του προβλήματος, δεν ήταν εύκολη. Καθώς εύκολη δεν ήταν και η εύρεση της οριακής τιμής που χρησιμοποιήθηκε στις πράξεις αυτές. Πραγματοποιήθηκαν πολλές υλοποιήσεις του κώδικα με διαφορετικές τιμές. Παρατηρήθηκαν και αναλύθηκαν τα διαφορετικά αποτελέσματα που έδωσαν όλες οι τιμές, ώστε να βρεθεί η καταλληλότερη. Εκείνη, δηλαδή, που θα ερχόταν πιο κοντά στην εύρεση των πραγματικών παλμών διαφορετικών χρηστών.

4.5.2 Αποθήκευση δειγμάτων

Τα παραδείγματα που έπρεπε να υλοποιηθούν, όπως έγινε αναφορά στην προηγούμενη υποενότητα, δημιούργησαν ένα ακόμα πρόβλημα. Κάθε φορά που ελεγχόταν μία πιθανή τιμή, έπρεπε να δοκιμαστεί σε διαφορετικούς ανθρώπους για να παρατηρηθεί η προσαρμογή της σε διαφορετικά βιοσήματα. Επειδή, όμως, κάτι τέτοιο θα ήταν πολύ χρονοβόρο, κρίθηκε απαραίτητη η αποθήκευση δειγμάτων. Δηλαδή, συνδέθηκαν διαφορετικά άτομα με τους αισθητήρες του BITalino, έγινε η δειγματοληψία και οι τιμές κάθε ατόμου αποθηκεύτηκαν σε ένα ξεχωριστό αρχείο. Επομένως, αναπτύχθηκε ένας παράλληλος κώδικας με τον αρχικό, με τη διαφορά ότι αντί να διαβάζει τιμές από το BITalino, θα διαβάζει από το εκάστοτε αρχείο που θα του υποδειχθεί. Η κλάση που περιέχει το βοηθητικό κώδικα ονομάζεται **readfromfile** και η λειτουργία της είναι παρόμοια με αυτή της κλάσης **Readfrombitalino**.

4.5.3 Ενδιάμεσοι κόμβοι

Στην πράξη, η υλοποίηση είχε δύο σημαντικά προβλήματα. Το πρώτο –και ίσως το πιο βασικό- είναι ότι δεν υπήρχαν αρκετές διαθέσιμες συσκευές για την πραγματοποίηση του μοντέλου που παρουσιάστηκε. Για το λόγο αυτό, οι ενδιάμεσοι χρήστες/κόμβοι δεν είναι συνδεδεμένοι με το BITalino. Επομένως, ο πραγματικός καρδιακός παλμός, θα παραχθεί, όχι και τόσο τυχαία, αλλά με βάση ενός εύρους τιμών που αντιστοιχούν στα χαρακτηριστικά τους (ηλικία και φύλο). Ο μέσος όρος, αυτού του εύρους τιμών, αποτελεί και τον αντιπροσωπευτικό παλμό (Πίνακας 1). Τα χαρακτηριστικά αυτά (ηλικία και φύλο) αποτελούν και τους κυριότερους παράγοντες διαφοροποίησης του πλήθους καρδιακών παλμών ανάμεσα στους ανθρώπους. Η ισχυρότερη παράμετρος είναι η ηλικία, καθώς παρατηρείται μείωση στο πλήθος των καρδιακών παλμών ανά λεπτό, όταν αναφερόμαστε σε άτομα μεγαλύτερης ηλικίας.

Age (yr.) and Gender	Heart Rate ($^{beats}/_{min}$)
10 – 29	
F	83 ± 8
M	76 ± 10
30 – 49	
F	79 ± 7
M	76 ± 7
50 – 69	
F	74 ± 10
M	78 ± 11
70 – 99	
F	73 ± 8
M	72 ± 11

Πίνακας 1. Υπολογισμός καρδιακών παλμών.

Για τους ενδιάμεσους κόμβους, λοιπόν, η διαδικασία παραγωγής των καρδιακών παλμών εξαρτάται από τις επαναλήψεις του κώδικα. Αναλυτικά, υπάρχουν δύο περιπτώσεις:

1. Η πρώτη περίπτωση αφορά την πρώτη επανάληψη. Καλείται η μέθοδος **menu()** με ορίσματα την ηλικία και το φύλο του χρήστη. Η μέθοδος εντάσσει το χρήστη σε μια κατηγορία (εύρος τιμών), με βάση τα ορίσματα που της δόθηκαν και υπολογίζει τα εξής (όπως περιγράφηκαν στο κεφάλαιο 4):

   i. το μέσο όρο του εύρους τιμών

   ii. τον αριθμό καρδιακών παλμών

   iii. και την απόκλισή που έχουν μεταξύ τους οι δύο αριθμοί των βημάτων **i** και **ii**.

   Οι τρεις αυτοί αριθμοί χωρισμένοι μεταξύ τους με ένα κενό, αποτελούν τη μεταβλητή String που θα επιστραφεί από τη μέθοδο **menu()**.

2. Η δεύτερη περίπτωση ισχύει για τις επόμενες επαναλήψεις του κώδικα, αφού θα έχει υπολογιστεί τουλάχιστον μία τιμή για τον αριθμό καρδιακών παλμών. Πρέπει η επόμενη τιμή που θα υπολογιστεί από τη μέθοδο **menu()**, να μην απέχει περισσότερο από 2 βαθμούς (είτε προς τα πάνω είτε προς τα κάτω) από την τιμή που υπολογίστηκε στην προηγούμενη επανάληψη. Για το λόγο αυτό, καλείται συνεχώς η μέθοδος αυτή μέχρι να ικανοποιηθεί η προηγούμενη συνθήκη. Με τον τρόπο αυτό προσπαθούμε να έχουμε πιο ρεαλιστικά αποτελέσματα. Διότι ο συνολικός αριθμός παλμών ανά λεπτό, που έχει ένας άνθρωπος, δε μεταβάλλεται σημαντικά σε μετρήσεις που διαφέρουν μεταξύ τους λίγα λεπτά.

4.5.4 Διεύθυνση IP

Το δεύτερο πρόβλημα που μας ανάγκασε να αλλάξουμε τον κώδικα, ως προς την υλοποίησή του, είναι ότι η εφαρμογή τρέχει από έναν υπολογιστή. Επομένως, αφού όλοι οι κόμβοι/χρήστες είναι συνδεδεμένοι στην ίδια πλατφόρμα (δηλαδή στον ίδιο υπολογιστή) θα έχουν την ίδια διεύθυνση IP, που μπορεί να αντικατασταθεί και με ένα όνομα. Το κοινό όνομα που χρησιμοποιήθηκε σε όλους τους κόμβους/χρήστες είναι το **localhost.**

Το χαρακτηριστικό, λοιπόν, που παίζει το ρόλο του διαχωριστή και βοηθάει στην αναγνώριση του ποιος χρήστης επικοινωνεί με ποιον, είναι η πόρτα. Κάθε κόμβος/χρήστης αντιστοιχίζεται με έναν μοναδικό αριθμό που αποτελεί την πόρτα του. Έτσι ο πρώτος κόμβος έχει την πόρτα 8201, ο δεύτερος έχει την πόρτα 8202, ο τρίτος την πόρτα 8203 και ούτω καθ’ εξής.

5.ΣΥΜΠΕΡΑΣΜΑΤΑ

Η χρήση του BITalino για την καταμέτρηση των καρδιακών παλμών του χρήστη, έπαιξε σημαντικό ρόλο στην επίτευξη του στόχου της παρούσας πτυχιακής εργασίας. Παράλληλα, με τη βοήθεια του Secure Multi-party Computation ικανοποιήθηκε και η διατήρηση της ιδιωτικότητας. Η εφαρμογή που αναπτύχθηκε στα πλαίσια της εργασίας αυτής, είναι ένα δείγμα των όσων μπορούν να επιτευχθούν χρησιμοποιώντας wearable συσκευές.

Μπορεί το BITalino να μην αποτελεί μια διακριτική και ευέλικτη συσκευή, προορισμένη για καθημερινή χρήση. Ωστόσο, οι μετρήσεις είναι έγκυρες και οι δυνατότητες που παρέχει, είναι πολλές.

Η ανταλλαγή των μετρήσεων μεταξύ των χρηστών έχει ως στόχο τη σύγκριση των αποτελεσμάτων και την πρόβλεψη πιθανής ασθένειας. Παρ' όλα αυτά μπορεί να χρησιμοποιηθεί και για διαφορετικές εφαρμογές. Παραδείγματος χάριν, για την αξιολόγηση της συναισθηματικής κατάστασης στην οποία βρίσκεται μια ομάδα ανθρώπων κατά την αξιολόγηση γνώσεων, ή σε άλλες καταστάσεις στρες.

Όλα αυτά πραγματοποιούνται μέσω του Secure Multi-party Computation. Με τον τρόπο αυτό εξασφαλίζεται η ιδιωτικότητα των προσωπικών δεδομένων των χρηστών, κατά τη μετάδοση των μετρήσεών τους. Συγκεκριμένα, οι μόνες πληροφορίες που γνωρίζουν οι χρήστες είναι οι δικές τους μετρήσεις. Το μοναδικό νέο δεδομένο που αποκαλύπτεται (χωρίς να έχει κάποιος την υπολογιστική ισχύ να παράγει από αυτό επιπλέον πληροφορίες) είναι το άθροισμα όλων των μετρήσεων.

Ο περιορισμός σε wearable συσκευές, μπορεί να οδήγησε στη δημιουργία τεχνητών κόμβων και ενός μόνο πραγματικού, όμως η υλοποίηση δεν παρέκκλινε σημαντικά από αυτό που αρχικά είχε σχεδιαστεί.

Επίσης, η χρήση ενός μόνο φορητού υπολογιστή για την εκπόνηση της πτυχιακής εργασίας, περιόρισε αρκετά το κομμάτι των διευθύνσεων IP. Για το λόγο αυτό χρησιμοποιήθηκε η κοινή ονομασία «localhost» σε όλους τους κόμβους.

5.1 Μελλοντική Έρευνα

Στο πλαίσιο της μελλοντικής έρευνας, είναι πολλά τα σημεία στα οποία μπορεί να εξελιχθεί και να αναπτυχθεί η παρούσα εφαρμογή.

Μια πρόταση βελτίωσης είναι η υλοποίηση της εφαρμογής από παράλληλο δίκτυο υπολογιστών. Με τον τρόπο αυτό θα λυθεί ο περιορισμός που αναφέρθηκε παραπάνω και αφορά τις διευθύνσεις IP.

Επίσης, σημαντική κρίνεται η υλοποίηση της εφαρμογής με wearable συσκευές, όπως smartwatch, ούτως ώστε ο κάθε χρήστης να φοράει τη δική του συσκευή και να εξάγονται πραγματικές μετρήσεις.

Μια τελευταία πρόταση είναι η εισαγωγή κι άλλων παραμέτρων στο ήδη υπάρχων μοντέλο. Δηλαδή, η μέτρηση της πίεσης του αίματος (ή άλλων ζωτικών στοιχείων του χρήστη) και ο συνυπολογισμός της με τους καρδιακούς παλμούς, με σκοπό μια πολύπλευρη μελέτη και την πιθανή διεξαγωγή πιο έμπιστων αποτελεσμάτων όσο αφορά τη πιθανότητα ασθένειας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] André G. Pinto, Gil Dias and Virginie Felizardo. Electrocardiography, electromyography, and accelerometry signals collected with BITalino while swimming: Device assembly and preliminary results. ICCP, 2016 IEEE 12th International Conference on 8-10 Sept. 2016.

[2] Diana Batista, Hugo Silva and Ana Fred. Experimental characterization and analysis of the BITalino platforms against a reference device. EMBC, 2017 39th Annual International Conference of the IEEE, 11-15 July 2017.

[3] Andrew Meola. Wearable technology and IoT wearable devices, Dec. 19, 2016.

[4] Internet of Things (IoT), Τι είναι και γιατί είναι σημαντικό. https://www.sas.com/el_gr/insights/big-data/internet-of-things.html

[5] Wearable Devices and the Internet of Things. MOUSER ELECTRONICS

[6] Scott Christian. The Wearable Revolution that has arrived… Sort of, Sept.19 2017.

[7] Margaret Rouse. Biometric Authentication, December 2014.

[8] Ιπποκράτης Αποστολίδης, Άννα Παρασκευά, Κωνσταντίνα Καραγκιόζη, Θρασύβουλος Τσιάτσος και Μαγδαληνή Τσολάκη. Αξιολόγηση ευχρηστίας και χρησιμότητας πρωτότυπης συσκευής βιο-ανάδρασης στην διαχείριση του άγχους φοιτητών, 28-30 Σεπτεμβρίου 2012.

[9] Τσίτογλου Κυριάκος. Εξέταση της εγκυρότητας του Polar RS800CX για την αξιολόγηση της μεταβλητότητας του καρδιακού παλμού σε ηρεμία άσκηση και αποκατάσταση. 11/04/2014.

[10] Sreedhar Vineel R. Kaipu, Joyline G. D'sa and Divyesh Sachan. Fabrication of flexible sensors for electrodermal activity measurement. Microelectronics (ICM), 10-13 Dec. 2017 29th International Conference.

[11] Benny P.L. Lo, Surapa Thiemjarus, Rachel King and Guang-Zhong Yang. Body Sensor Network – A Wireless Sensor Platform For Pervasive Healthcare Monotoring.

[12] Y. M. Huang, M. Y. Hsieh and H. C. Chao. Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. IEEE Journal on Selected Areas in Communications (Volume: 27, Issue: 4, May 2009).

[13] Ashraf Darwish and Aboul Ella Hassanien. Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring, 26 May 2011.

[14] Wan-Young Chung, Young-Dong Lee and Sang-Joong Jung. A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO2, EMBS 20-25 Aug. 2008. 30th Annual International Conference of the IEEE.

[15] Changzhi Li, Victor M. Lubecke and Olga Boric-Lubecke. A Review on Recent Advances in Doppler Radar Sensors for Noncontact Healthcare Monitoring, IEEE Transactions on Microwave Theory and Techniques (Volume: 61, Issue: 5, May 2013)

[16] R. Snelick, U. Uludag and A. Mink. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems, IEEE Transactions on Pattern Analysis and Machine Intelligence (Volume: 27, Issue: 3, March 2005).

[17] Pim Tuyls, Anton H. M. Akkermans, Tom A. M. Kevenaar, Geert-Jan Schrijen, Asker M. Bazen and Raimond N. J. Veldhuis. Practical Biometric Authentication with Template Protection.

[18] Dario Maio, Davide Maltoni, Raffaele Cappelli, Jim L. Wayman and Anil K. Jain. FVC2004: Third Fingerprint Verification Competition.

[19] Paul M. Burger. Biometric authentication system, 09/07/1998.

[20] Noel D. Matchett, Brian D. Kehoe. Continuous biometric authentication matrix, 20/06/1991.

[21] Adams Wai-Kin Kong and David Zhang. Feature-Level Fusion for Effective Palmprint Authentication.

[22] Pim Tuyls and Jasper Goseling. Capacity and Examples of Template-Protecting Biometric Authentication Systems.

[23] Yuan-Pin Yu, Stephen Wong and Mark B. Hoffberg. Web-based biometric authentication system and method, 09/06/1997.

[24] Artemiy Oleinikov, Berdakh Abibullaev and Almas Shintermirov. Feature extraction and real-time recognition of hand motion intentions from EMGs via artificial neural networks, Brain-Computer Interface (BCI), 2018 6th International Conference on 15-17 Jan..

[25] Jan Meyer, Paul Lukowicz and Gerhard Troster. Textile Pressure Sensor for Muscle Activity and Motion Detection, Wearable Computers, 2006 10th IEEE International Symposium on 11-14 Oct. 2006.

[26] Jaeyong Sung, Colin Ponce and Bart Selman. Unstructured human activity detection from RGBD images, Robotics and Automation (ICRA), 2012 IEEE International Conference on 14-18 May 2012.

[27] Daphney-Stavroula Zois, Marco Levorato and Urbashi Mitra. Energy-Efficient, Heterogeneous Sensor Selection for Physical Activity Detection in Wireless Body Area Networks, IEEE Transactions on Signal Processing (Volume: 61, Issue: 7, April1, 2013).

[28] N. Noury. A smart sensor for the remote follow up of activity and fall detection of the elderly, Microtechnologies in Medicine & Biology 2nd Annual International IEEE-EMB Special Topic Conference on 2-4 May 2002.

[29] Mark W. Kroll, Chris Sorensen and Gene A. Bornzin. Detection of patient's position and activity status using 3D accelerometer-based position sensor, 2001-08-24.

[30] Kaustubh Kalgaonkar, Rongquiang Hu and Bhiksha Raj. Ultrasonic Doppler Sensor for Voice Activity Detection, IEEE Signal Processing Letters (Volume: 14, Issue: 10, Oct. 2007).

[31] Seon-Woo Lee and K. Mase. Activity and location recognition using wearable sensors, IEEE Pervasive Computing (Volume: 1, Issue: 3, July-Sept. 2002).

[32] Ronald Cramer, Ivan Bjerre Damgård and Jesper Buus Nielsen. Secure Multiparty Computation and Secret Sharing.

[33] Charles P. Pfleeger and Shari Lawrence Pfleeger. Security in Computing 3rd, Prentice Hall Professional Technical Reference ©2002.

[34] Paulo Pires and Svein Petter Gjøby. Bitalino Java SDK. https://github.com/BITalinoWorld/java-sdk, 2016.

[35] https://el.wikipedia.org/wiki/Κανονική_κατανομή

[36] https://el.wikipedia.org/wiki/Διεύθυνση_IP

[37] https://en.wikipedia.org/wiki/Port_(computer_networking)