ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Απομακρυσμένη υπηρεσία αυθεντικοποίησης μέσω βιομετρικών δεδομένων

Γεώργιος Λ. Κυρίτσης

ΛΑΜΙΑ

ΣΕΠΤΕΜΒΡΙΟΣ 2019

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Απομακρυσμένη υπηρεσία αυθεντικοποίησης μέσω βιομετρικών δεδομένων

Γεώργιος Λ. Κυρίτσης

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

Γεώργιος Σπαθούλας
Μέλος ΕΔΙΠ
Πανεπιστήμιο Θεσσαλίας

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

Γεώργιος Σπαθούλας
Μέλος ΕΔΙΠ
Πανεπιστήμιο Θεσσαλίας

Ιωάννης Αναγνωστόπουλος
Αναπληρωτής Καθηγητής
Πανεπιστήμιο Θεσσαλίας

Αθανάσιος Κακαρούντας
Επίκουρος Καθηγητής
Πανεπιστήμιο Θεσσαλίας

Ημερομηνία Εξέτασης: 25 Σεπτεμβρίου 2019

ΠΕΡΙΛΗΨΗ

Η Ασφάλεια των Πληροφοριακών Συστημάτων είναι από τις βασικότερες προτεραιότητες στον χώρο της Πληροφορικής. Ένα μέρος αυτών των συστημάτων έχουν αποθηκευμένα προσωπικά δεδομένα που τις περισσότερες φορές είναι πολύ σημαντικά για τους ιδιοκτήτες αυτών των συστημάτων. Η διαδικασία identification - authentication - authorization (αναγνώρισης - ταυτοποίησης - χορήγησης πρόσβασης), απαιτείται και στην περίπτωση του δικτύου υπολογιστών, όσο και στην πραγματική ζωή. Όπως και στους υπολογιστές, έτσι και σε πραγματικές συνθήκες είναι αρκετά διαδεδομένο στις μέρες μας να συναντάται η περίπτωση υποκλοπής προσωπικών δεδομένων ενός ατόμου, όπως για παράδειγμα ο κωδικός πρόσβασής του ή ακόμα και η αστυνομική του ταυτότητα. Σε μια προσπάθεια αποφυγής τέτοιων κρουσμάτων, εδώ και αρκετό καιρό έχουν δημιουργηθεί συστήματα τα οποία θεωρούν ότι είναι ασφαλέστερα από τα ήδη χρησιμοποιούμενα. Υλοποιήθηκε μια πλατφόρμα η οποία αποθηκεύει και διαμοιράζει τα δεδομένα αυτά στους κόμβους που είναι εξουσιοδοτημένοι για την χρήση αυτών των πληροφοριών. Εδώ αλληλεπιδρούν χρήστης – πλατφόρμα – ιστοσελίδα, οι οποίοι ανταλλάζουν δεδομένα μεταξύ τους, πάντα με ενδιάμεσο κόμβο την πλατφόρμα. Όλη η κίνηση των δεδομένων γίνεται κρυπτογραφώντας όλες αυτές τις πληροφορίες με την χρήση ομομορφικής κρυπτογράφησης.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Βιομετρία, Κρυπτογραφία και ιδιωτικότητα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Βιομετρική αυθεντικοποίηση, ομομορφική κρυπτογράφηση

ABSTRACT

Information Systems Security is one of the top priorities in the IT field. Some of these systems have personal data stored which is often very important to the owners of these systems. The identification - authentication - authorization process is required both in the computer network and in real life. As with computers, in real life, it is quite common nowadays to encounter a person's theft of personal information, such as their password or even their police ID. To avoid such incidents, systems have been developed for some time that they consider to be safer than those already in use. A platform has been implemented that stores and distributes this data to the nodes that are authorized to use this information. Here, users - platform - website interact, exchanging data with each other, always interfacing the platform. All data traffic is encrypted with all this information using homomorphic encryption.

SUBJECT AREA: Biometrics, Cryptography and privacy

KEYWORDS: Biometric authentication, Homomorphic encryption

Στους αγαπημένους μου.

ΕΥΧΑΡΙΣΤΙΕΣ

Πριν προχωρήσω παρακάτω, θέλω πραγματικά να ευχαριστήσω ορισμένους από τους ανθρώπους που γνώρισα και συνεργάστηκα μαζί τους για την πραγματοποίηση της πτυχιακής μου εργασίας αλλά και τους αφανείς ήρωες που είχα στο πλευρό μου κατά την διάρκεια των φοιτητικών μου χρόνων.

Πρώτα από όλους θέλω να ευχαριστήσω τον επιβλέποντα της πτυχιακής μου εργασίας, διδάσκοντα Γεώργιο Σπαθούλα για την πίστη που έδειξε στο πρόσωπο μου και την συνεχή καθοδήγηση που μου παρείχε σε όλη την διάρκεια της έρευνας και εκπόνησης της εργασίας.

Δεν θα μπορούσα να παραλείψω να ευχαριστήσω τους καθηγητές της σχολής που με υπομονή τόσα χρόνια συνέβαλαν στην απόκτηση των απαραίτητων γνώσεων για την επιτυχή φοίτησή μου και την εκπόνηση της πτυχιακής μου εργασίας, αλλά κυρίως που ενίσχυσαν την αγάπη μου για την επιστήμη και την έρευνα, που τώρα πια έχει γίνει αναπόσπαστο κομμάτι της καθημερινότητας μου.

Τέλος, θέλω να ευχαριστήσω την οικογένεια μου και ιδιαίτερα τους γονείς μου, για την βοήθεια τους όλα αυτά τα χρόνια. Σας ευχαριστώ για την ψυχολογική αλλά και οικονομική υποστήριξη που μου προσφέρατε.

Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο **Απομακρυσμένη υπηρεσία αυθεντικοποίησης μέσω βιομετρικών δεδομένων** αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Γεώργιος Κυρίτσης

25/09/2019

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

1. ΕΙΣΑΓΩΓΗ

Η Ασφάλεια των Πληροφοριακών Συστημάτων είναι από τις βασικότερες προτεραιότητες στον χώρο της Πληροφορικής. Ένα μέρος αυτών των συστημάτων έχουν αποθηκευμένα προσωπικά δεδομένα που τις περισσότερες φορές είναι πολύ σημαντικά για τους ιδιοκτήτες αυτών των συστημάτων.

Η προστασία λοιπόν των προσωπικών δεδομένων, αποτελούσε ανέκαθεν ένα ιδιαίτερο πρόβλημα για τους υπεύθυνους προστασίας του ιδιωτικού απορρήτου. Τόσο στην περίπτωση προφύλαξης προσωπικών δεδομένων στο Internet και σε τοπικά δίκτυα εταιρειών, όσο και στη διατήρηση ελέγχου πρόσβασης σε κτιριακές εγκαταστάσεις και γενικότερους χώρους περιορισμένης πρόσβασης. Το ζήτημα της ασφάλειας των πληροφοριακών συστημάτων αποκτά ιδιαίτερη σημασία σε μια εποχή όπου η τεχνολογία, ο ανταγωνισμός και οι αυξημένες απαιτήσεις των επιχειρήσεων απαιτούν τη λήψη αυστηρότερων πολιτικών ασφαλείας

Η διαδικασία identification - authentication - authorization (αναγνώρισης - ταυτοποίησης - χορήγησης πρόσβασης), απαιτείται και στην περίπτωση του δικτύου υπολογιστών, όσο και στην πραγματική ζωή. Όπως και στους υπολογιστές, έτσι και σε πραγματικές συνθήκες είναι αρκετά διαδεδομένο στις μέρες μας να συναντάται η περίπτωση υποκλοπής προσωπικών δεδομένων ενός ατόμου, όπως για παράδειγμα ο κωδικός πρόσβασής του ή ακόμα και η αστυνομική του ταυτότητα. Σε μια προσπάθεια αποφυγής τέτοιων κρουσμάτων, εδώ και αρκετό καιρό έχουν δημιουργηθεί συστήματα τα οποία θεωρούν ότι είναι ασφαλέστερα από τα ήδη χρησιμοποιούμενα. Αυτά τα συστήματα τα ονομάζουν βιομετρικά και αναφέρονται στα φυσιολογικά χαρακτηριστικά και χαρακτηριστικά συμπεριφοράς για την ταυτοποίηση του κάθε ατόμου. Σε αντίθεση με συμβατικές μεθόδους ασφαλείας όπως οι κωδικοί πρόσβασης και τα κλειδιά ασφαλείας, που μπορούν εύκολα να χαθούν, κλαπούν ή ξεχαστούν, οι βιομετρικές τεχνολογίες προσφέρουν αξιόπιστες λύσεις στο πρόβλημα της διαχείρισης της ταυτότητας των χρηστών και της ασφαλούς πρόσβασης σε υπηρεσίες πληροφοριακών συστημάτων.

Υλοποιήθηκε μια πλατφόρμα η οποία αποθηκεύει και διαμοιράζει τα δεδομένα αυτά στους κόμβους που είναι εξουσιοδοτημένοι για την χρήση αυτών των πληροφοριών. Εδώ αλληλεπιδρούν χρήστης – πλατφόρμα – ιστοσελίδα, οι οποίοι ανταλλάζουν δεδομένα μεταξύ τους, πάντα με ενδιάμεσο κόμβο την πλατφόρμα. Όλη η κίνηση των δεδομένων γίνεται κρυπτογραφώντας όλες αυτές τις πληροφορίες.

Η πλατφόρμα αυτή υλοποιήθηκε με την σκέψη πως θα εφαρμόζεται σε ιστοσελίδες και θα είναι υπεύθυνη για την είσοδο του χρήστη σε αυτήν, από τον απλό συμβατικό τρόπο εισόδου(κωδικός πρόσβασης) σε αναγνώριση βιομετρικών χαρακτηριστικών του προσώπου(αναγνώριση προσώπου). Η ευρύτερη ιδέα είναι πως σε όλη την διαδικασία τα προσωπικά δεδομένα είναι εμφανή μόνο στην πλευρά του χρήστη και κανείς άλλος δεν μπορεί να αναγνωρίσει ή να ανακτήσει κάποια πληροφορία καθώς αποσταλλούν από την συσκευή αυτού.

Χρησιμοποιήθηκαν τεχνικές ομομορφικής κρυπτογράφησης(Paillier cryptosystem) για τα προσωπικά δεδομένα των χρηστών, ώστε να είναι δυνατή η επεξεργασία τους από μια έμπιστη τρίτη οντότητα(Server), χωρίς να απαιτείται η αποκρυπτογράφηση τους.

2. ΒΙΟΜΕΤΡΙΑ

Η βιομετρία είναι ο τεχνικός όρος για τις μετρήσεις και τους υπολογισμούς του σώματος.Αναφέρεται σε μετρήσεις που σχετίζονται με τα ανθρώπινα χαρακτηριστικά. Ο έλεγχος ταυτότητας με βιομετρικά στοιχεία [2] (ή ρεαλιστικός έλεγχος ταυτότητας) χρησιμοποιείται στην επιστήμη των υπολογιστών ως μορφή αναγνώρισης και ελέγχου πρόσβασης. Χρησιμοποιείται επίσης για τον εντοπισμό ατόμων σε ομάδες που βρίσκονται υπό επιτήρηση.

Τα βιομετρικά δεδομένα είναι τα διακριτικά, μετρήσιμα χαρακτηριστικά που χρησιμοποιούνται για την επισήμανση και την περιγραφή των ατόμων. Τα βιομετρικά αναγνωριστικά στοιχεία συχνά ταξινομούνται ως φυσιολογικά και συμπεριφορικά χαρακτηριστικά.

- Τα φυσιολογικά χαρακτηριστικά σχετίζονται με το σχήμα του σώματος. Κάποια παραδείγματα είναι:
  - δακτυλικά αποτυπώματα,
  - παλμός της καρδιάς,
  - αναγνώριση προσώπου,
  - DNA,
  - εκτύπωση παλάμης,
  - γεωμετρία χεριών,
  - αναγνώριση ίριδας,
  - αμφιβληστροειδή,
  - οσμή / άρωμα.
- Τα συμπεριφορικά χαρακτηριστικά σχετίζονται με το πρότυπο συμπεριφοράς ενός ατόμου, συμπεριλαμβανομένων:
  - του ρυθμού δακτυλογράφησης,
  - του βαδίσματος,
  - της φωνής.

Ορισμένοι ερευνητές έχουν εξειδίκευση τον όρο **behaviometrics** για να περιγράψουν την τελευταία κατηγορία βιομετρικών στοιχείων.

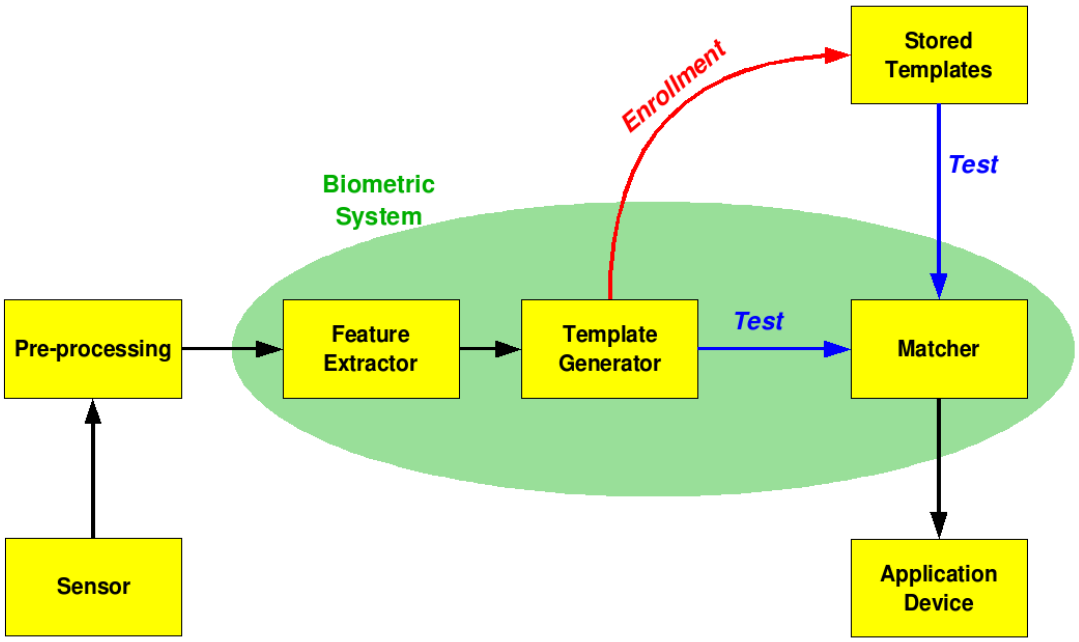
Τα πιο παραδοσιακά μέσα ελέγχου πρόσβασης περιλαμβάνουν αναγνωριστικά συστήματα που βασίζονται σε διακριτικά σήματα, όπως άδεια οδήγησης ή διαβατήριο, και συστήματα αναγνώρισης με βάση τη γνώση, όπως κωδικό πρόσβασης ή προσωπικό αναγνωριστικό αριθμό. Δεδομένου ότι τα βιομετρικά δεδομένα είναι μοναδικά για το άτομο, είναι πιο αξιόπιστα όσον αφορά την επαλήθευση της ταυτότητας παρά με τις συμβολικές μεθόδους και τις μεθόδους που βασίζονται στη γνώση. Ωστόσο, η συλλογή βιομετρικών αναγνωριστικών δημιουργεί ανησυχίες για την προστασία της ιδιωτικής ζωής όσον αφορά την τελική χρήση αυτών των πληροφοριών.

Πολλές διαφορετικές πτυχές της ανθρώπινης φυσιολογίας, της χημείας ή της συμπεριφοράς μπορούν να χρησιμοποιηθούν για τη βιομετρική πιστοποίηση. Η επιλογή ενός συγκεκριμένου βιομετρικού στοιχείου για χρήση σε μια συγκεκριμένη εφαρμογή συνεπάγεται τη στάθμιση πολλών παραγόντων. Προσδιορίστηκαν επτά τέτοιοι παράγοντες που πρέπει να χρησιμοποιηθούν κατά την αξιολόγηση της καταλληλότητας οποιουδήποτε χαρακτηριστικού για χρήση στη βιομετρική πιστοποίηση, τα οποία είναι:

- Η καθολικότητα, σημαίνει ότι κάθε άτομο που χρησιμοποιεί ένα σύστημα πρέπει να έχει το χαρακτηριστικό.
- Η μοναδικότητα σημαίνει ότι το χαρακτηριστικό πρέπει να είναι αρκετά διαφορετικό για τα άτομα του σχετικού πληθυσμού, ώστε να μπορούν να διακριθούν μεταξύ τους.
- Η διαχρονικότητα σχετίζεται με τον τρόπο με τον οποίο ένα χαρακτηριστικό ποικίλλει με την πάροδο του χρόνου. Πιο συγκεκριμένα, ένα χαρακτηριστικό με «καλή» μονιμότητα θα είναι λογικά αμετάβλητο με την πάροδο του χρόνου σε σχέση με τον συγκεκριμένο αλγόριθμο αντιστοίχισης.
- Η μετρησιμότητα (συλλογή) σχετίζεται με την ευκολία απόκτησης ή μέτρησης του χαρακτηριστικού. Επιπλέον, τα δεδομένα που αποκτήθηκαν πρέπει να είναι σε μορφή που να επιτρέπει την περαιτέρω επεξεργασία και εξαγωγή των σχετικών συνόλων των χαρακτηριστικών.
- Η απόδοση σχετίζεται με την ακρίβεια, την ταχύτητα και την ευρωστία της χρησιμοποιούμενης τεχνολογίας.
- Η αποδοχή σχετίζεται με το πόσο καλά τα άτομα του οικείου πληθυσμού αποδέχονται την τεχνολογία έτσι ώστε να είναι διατεθειμένα να καταγράψουν και να αξιολογήσουν το βιομετρικό τους χαρακτηριστικό.

- Η παράκαμψη σχετίζεται με την ευκολία με την οποία ένα χαρακτηριστικό θα μπορούσε να μιμηθεί χρησιμοποιώντας ένα τεχνούργημα ή ένα υποκατάστατο.

Η σωστή βιομετρική χρήση εξαρτάται από την εφαρμογή. Ορισμένα βιομετρικά στοιχεία θα είναι καλύτερα από άλλα με βάση τα απαιτούμενα επίπεδα άνεσης και ασφάλειας. Καμία μοναδική βιομετρική πληροφορία δεν θα καλύψει όλες τις απαιτήσεις κάθε πιθανής εφαρμογής.



Σχήμα 2.1: Δομικό διάγραμμα βιομετρικού συστήματος

Πρώτον, κατά τη λειτουργία επαλήθευσης (ή ελέγχου ταυτότητας) το σύστημα εκτελεί μια σύγκριση one-to-one μιας βιομετρίας που έχει συλληφθεί με ένα συγκεκριμένο πρότυπο που είναι αποθηκευμένο σε μια βιομετρική βάση δεδομένων προκειμένου να επαληθευτεί ότι το άτομο είναι το πρόσωπο που ισχυρίζεται ότι είναι. Υπάρχουν τρία βήματα για την επαλήθευση ενός ατόμου:

- Στο πρώτο βήμα, παράγονται και αποθηκεύονται μοντέλα αναφοράς για όλους τους χρήστες στη βάση δεδομένων.

- Στο δεύτερο βήμα, μερικά δείγματα αντιστοιχίζονται με μοντέλα αναφοράς για να δημιουργήσουν τις γνησιότητές τους και να υπολογίσουν το κατώτατο όριο.

- Το τρίτο βήμα είναι το βήμα της δοκιμής. Αυτή η διαδικασία μπορεί να χρησιμοποιεί έξυπνη κάρτα, όνομα χρήστη ή αναγνωριστικό (π.χ. PIN) για να υποδείξει ποιο πρότυπο θα χρησιμοποιηθεί για σύγκριση. Η «θετική αναγνώριση» είναι μια κοινή χρήση του τρόπου επαλήθευσης, όπου ο στόχος είναι να αποτρέψει τη χρήση πολλών ατόμων στο να χρησιμοποιήσουν την ίδια ταυτότητα.

Δεύτερον, στον τρόπο αναγνώρισης το σύστημα εκτελεί μια σύγκριση ενός προς πολλούς με μια βιομετρική βάση δεδομένων σε μια προσπάθεια να διαπιστωθεί η ταυτότητα ενός άγνωστου ατόμου. Το σύστημα θα επιτύχει στην αναγνώριση του ατόμου εάν η σύγκριση του βιομετρικού δείγματος με ένα πρότυπο στη βάση δεδομένων εμπίπτει σε ένα προκαθορισμένο όριο. Ο τρόπος αναγνώρισης μπορεί να χρησιμοποιηθεί είτε για «θετική αναγνώριση» (έτσι ώστε ο χρήστης δεν χρειάζεται να παράσχει καμία πληροφορία σχετικά με το πρότυπο που πρόκειται να χρησιμοποιηθεί) είτε για «αρνητική αναγνώριση» του προσώπου στο οποίο το σύστημα διαπιστώνει εάν το πρόσωπο είναι αυτό που αρνείται να είναι. Η τελευταία λειτουργία μπορεί να επιτευχθεί μόνο μέσω βιομετρικών στοιχείων, καθώς άλλες μέθοδοι προσωπικής αναγνώρισης, όπως οι κωδικοί πρόσβασης, τα PIN ή τα κλειδιά, είναι αναποτελεσματικά.

Η πρώτη φορά που ένα άτομο χρησιμοποιεί ένα βιομετρικό σύστημα ονομάζεται εγγραφή. Κατά τη διάρκεια της εγγραφής, οι βιομετρικές πληροφορίες από ένα άτομο συλλαμβάνονται και αποθηκεύονται [3]. Σε μεταγενέστερες χρήσεις, ανιχνεύονται βιομετρικές πληροφορίες και συγκρίνονται με τις πληροφορίες που αποθηκεύονται κατά την εγγραφή. Σημειώστε ότι είναι ζωτικής σημασίας η αποθήκευση και η ανάκτηση τέτοιων συστημάτων να είναι ασφαλή. Το πρώτο μπλοκ (αισθητήρας) είναι η διεπαφή μεταξύ του πραγματικού κόσμου και του συστήματος,όπου πρέπει να αποκτήσει όλα τα απαραίτητα δεδομένα. Τις περισσότερες φορές είναι ένα σύστημα λήψης εικόνων, αλλά μπορεί να αλλάξει ανάλογα με τα επιθυμητά χαρακτηριστικά. Το δεύτερο μπλοκ εκτελεί όλη την απαραίτητη προεπεξεργασία: πρέπει να αφαιρέσει αντικείμενα από τον αισθητήρα, να βελτιώσει την είσοδο (π.χ. αφαίρεση θορύβου υποβάθρου), να χρησιμοποιήσει κάποιο είδος ομαλοποίησης κλπ. Στο τρίτο μπλοκ, εξάγονται τα απαραίτητα χαρακτηριστικά. Αυτό το βήμα είναι ένα σημαντικό βήμα καθώς τα σωστά χαρακτηριστικά πρέπει να εξαχθούν με έναν βέλτιστο τρόπο. Χρησιμοποιείται ένας φορέας αριθμών ή μια εικόνα με συγκεκριμένες ιδιότητες για τη δημιουργία ενός προτύπου. Ένα πρότυπο είναι μια σύνθεση των σχετικών χαρακτηριστικών που εξάγονται από την πηγή.

Κατά τη διάρκεια της φάσης εγγραφής, το πρότυπο αποθηκεύεται απλά κάπου (σε μια κάρτα ή μέσα σε μια βάση δεδομένων ή και στα δύο). Κατά τη διάρκεια της φάσης αντι-

στοίχισης, το λαμβανόμενο πρότυπο μεταβιβάζεται σε ένα εργαλείο αντιστοιχίας που το συγκρίνει με άλλα υπάρχοντα πρότυπα, εκτιμώντας την απόσταση μεταξύ τους χρησιμοποιώντας οποιοδήποτε αλγόριθμο. Το πρόγραμμα αντιστοίχισης θα αναλύσει το πρότυπο με την είσοδο. Τούτο αποδίδεται στη συνέχεια για οποιαδήποτε συγκεκριμένη χρήση ή σκοπό (π.χ. είσοδος σε μια περιορισμένη περιοχή). Γίνεται επιλογή βιομετρικών στοιχείων σε κάθε πρακτική εφαρμογή ανάλογα με τις χαρακτηριστικές μετρήσεις και τις απαιτήσεις των χρηστών. Κατά την φάση της βιομετρίας, οι παράγοντες που πρέπει να εξεταστούν περιλαμβάνουν την απόδοση, την κοινωνική αποδοχή, την ευκολία καταστρατήγησης και πλαστογράφησης, την ευρωστία, την κάλυψη του πληθυσμού, το μέγεθος του αναγκαίου εξοπλισμού και την αποτροπή της κλοπής ταυτότητας. Η επιλογή ενός βιομετρικού βασισμένου στις απαιτήσεις του χρήστη προϋποθέτει τη διαθεσιμότητα αισθητήρων και συσκευών, τον υπολογιστικό χρόνο και την αξιοπιστία, το κόστος, το μέγεθος του αισθητήρα και την κατανάλωση ενέργειας.

Τα πολυτροπικά βιομετρικά συστήματα [18] χρησιμοποιούν πολλαπλούς αισθητήρες ή βιομετρικά στοιχεία για να ξεπεράσουν τους περιορισμούς των μονόδρομων βιομετρικών συστημάτων. Για παράδειγμα, τα συστήματα αναγνώρισης ίριδας μπορούν να διακυβευτούν από τη γήρανση των ίριδων και η ηλεκτρονική αναγνώριση των δακτυλικών αποτυπωμάτων μπορεί να επιδεινωθεί από τα φθαρμένα ή κομμένα δακτυλικά αποτυπώματα. Τα πολυτροπικά βιομετρικά συστήματα μπορούν να αποκτήσουν ομάδες πληροφοριών από τον ίδιο δείκτη (δηλ. Πολλαπλές εικόνες μιας ίριδας ή σαρώσεις του ίδιου δακτύλου) ή πληροφορίες από διαφορετικά βιομετρικά στοιχεία (που απαιτούν σαρώσεις δακτυλικών αποτυπωμάτων και, χρησιμοποιώντας φωνητική αναγνώριση, έναν προφορικό κωδικό πρόσβασης).

Τα πολυτροπικά βιομετρικά συστήματα μπορούν να συγχωνεύσουν αυτά τα μονοτροπικά συστήματα διαδοχικά, έναν συνδυασμό αυτών ή σε σειρά, τα οποία αναφέρονται σε διαδοχικούς, παράλληλους, ιεραρχικούς και σειριακούς τρόπους ολοκλήρωσης. Η συγχώνευση των πληροφοριών βιομετρικών στοιχείων μπορεί να συμβεί σε διαφορετικά στάδια ενός συστήματος αναγνώρισης. Σε περίπτωση σύντηξης των χαρακτηριστικών, τα ίδια τα δεδομένα ή τα χαρακτηριστικά που εξάγονται από πολλαπλά βιομετρικά στοιχεία είναι συντηγμένα. Η συγχώνευση επιπέδου αντιστοιχίας-βαθμού ενοποιεί τις βαθμολογίες που παράγονται από πολλαπλούς ταξινομητές που σχετίζονται με διαφορετικούς τρόπους. Τέλος, σε περίπτωση σύντηξης σε επίπεδο απόφασης τα τελικά αποτελέσματα πολλαπλών ταξινομητών συνδυάζονται μέσω τεχνικών όπως η ψηφοφορία με πλειοψηφία. Η σύντηξη επιπέδου λειτουργίας πιστεύεται ότι είναι πιο αποτελεσματική από τα άλλα επί-

πεδα συγχώνευσης επειδή το σετ χαρακτηριστικών περιέχει πλουσιότερες πληροφορίες για τα βιομετρικά δεδομένα εισαγωγής από το αντίστοιχο σκορ ή την απόφαση εξόδου ενός ταξινομητή. Συνεπώς, η σύντηξη σε επίπεδο χαρακτηριστικών αναμένεται να προσφέρει καλύτερα αποτελέσματα αναγνώρισης.

Οι επιθέσεις συνίστανται στην υποβολή πλαστών βιομετρικών χαρακτηριστικών σε βιομετρικά συστήματα και αποτελούν μείζονα απειλή που μπορεί να περιορίσει την ασφάλειά τους. Τα πολυτροπικά βιομετρικά συστήματα πιστεύεται ότι είναι εγγενώς πιο αξιόπιστα για τέτοιου είδους επιθέσεις, αλλά πρόσφατες μελέτες έχουν δείξει ότι μπορούν να αποφευχθούν ακόμη και με ένα μοναδικό βιομετρικό χαρακτηριστικό.

Τα παρακάτω χρησιμοποιούνται ως μετρήσεις απόδοσης για τα βιομετρικά συστήματα:

- Ψευδές ποσοστό αντιστοίχισης (FMR, ονομαζόμενη επίσης FAR = False Accept Rate): η πιθανότητα το σύστημα να μην ταιριάζει σωστά με το πρότυπο εισαγωγής σε ένα μη προσαρμοσμένο πρότυπο στη βάση δεδομένων. Μετρά το ποσοστό των μη έγκυρων εισροών που είναι εσφαλμένα αποδεκτές. Σε περίπτωση ομοιότητας, αν το άτομο είναι απατεώνας στην πραγματικότητα, αλλά το σκορ αντιστοιχίας είναι υψηλότερο από το όριο, τότε αντιμετωπίζεται ως γνήσιο. Αυτό αυξάνει το FMR, το οποίο επίσης εξαρτάται από την τιμή κατωφλίου.

- Ψευδής ποσοστό μη αντιστοίχισης (FNMR, επίσης αποκαλούμενο FRR = False Rate Reject): η πιθανότητα το σύστημα να μην εντοπίσει μια αντιστοιχία μεταξύ του προτύπου εισόδου και ενός προτύπου που ταιριάζει στη βάση δεδομένων. Μετρά το ποσοστό των έγκυρων εισόδων που απορρίπτονται εσφαλμένα.

- Χαρακτηριστικό ή σχετικό χαρακτηριστικό λειτουργίας του δέκτη (ROC): Το γράφημα ROC είναι ένας οπτικός χαρακτηρισμός της σχέσης μεταξύ του FMR και του FNMR. Σε γενικές γραμμές, ο αλγόριθμος αντιστοίχισης εκτελεί μια απόφαση βασισμένη σε ένα κατώφλι που καθορίζει πόσο κοντά σε ένα πρότυπο πρέπει να είναι η είσοδος για να θεωρηθεί ότι ταιριάζει. Εάν μειωθεί το κατώτατο όριο, θα υπάρξουν λιγότερες ψευδείς μη αντιστοιχίες, αλλά περισσότερες εσφαλμένες απολαβές. Αντίθετα, ένα υψηλότερο όριο θα μειώσει το FMR αλλά θα αυξήσει το FNMR. Μια κοινή παραλλαγή είναι η αντιστοίχιση σφάλματος ανίχνευσης (DET), η οποία λαμβάνεται με κλίμακες κανονικής απόκλισης και στους δύο άξονες. Αυτό το πιο γραμμικό γράφημα φωτίζει τις διαφορές για υψηλότερες επιδόσεις (σπανιότερα σφάλματα).

- Ποσοστό ίσου σφάλματος ή ποσοστό σφάλματος διασταύρωσης (EER ή CER): ο ρυθμός με τον οποίο τα σφάλματα αποδοχής και απόρριψης είναι ίσα. Η τιμή του EER μπορεί εύκολα να ληφθεί από την καμπύλη ROC. Το EER είναι ένας γρήγορος τρόπος σύγκρισης της ακρίβειας των συσκευών με διαφορετικές καμπύλες ROC. Σε γενικές γραμμές, η συσκευή με το χαμηλότερο EER είναι η πιο ακριβής.

- Αποτυχία εγγραφής (FTE ή FER): ο ρυθμός με τον οποίο επιχειρείται η δημιουργία ενός προτύπου από μια είσοδο και δεν είναι επιτυχής. Αυτό προκαλείται συνήθως από εισόδους χαμηλής ποιότητας.

- Αποτυχία λήψης ρυθμού (FTC): Σε αυτόματα συστήματα, η πιθανότητα το σύστημα να μην ανιχνεύσει μια βιομετρική είσοδο όταν παρουσιάζεται σωστά.

- Ικανότητα προτύπου: ο μέγιστος αριθμός συνόλων δεδομένων που μπορούν να αποθηκευτούν στο σύστημα.

Τα προσαρμοστικά βιομετρικά συστήματα αποσκοπούν στην αυτόματη ενημέρωση των προτύπων ή μοντέλων στην ενδοκλαδική παραλλαγή των λειτουργικών δεδομένων. Τα διπλά πλεονεκτήματα αυτών των συστημάτων είναι η επίλυση του προβλήματος των περιορισμένων δεδομένων εκπαίδευσης και η παρακολούθηση των χρονικών διακυμάνσεων των δεδομένων εισόδου μέσω της προσαρμογής. Πρόσφατα, η προσαρμοστική βιομετρική έχει λάβει σημαντική προσοχή από την ερευνητική κοινότητα. Αυτή η κατεύθυνση της έρευνας αναμένεται να κερδίσει δυναμική λόγω των βασικών πλεονεκτημάτων που έχουν αναλάβει. Πρώτον, με ένα προσαρμοστικό βιομετρικό σύστημα, δεν χρειάζεται πλέον να συλλέγει μεγάλο αριθμό βιομετρικών δειγμάτων κατά τη διάρκεια της διαδικασίας εγγραφής. Δεύτερον, δεν είναι πλέον απαραίτητο να εγγραφείτε ξανά ή να επαναπροσδιορίσετε το σύστημα από το μηδέν για να αντιμετωπίσετε το μεταβαλλόμενο περιβάλλον. Αυτή η ευκολία μπορεί να μειώσει σημαντικά το κόστος διατήρησης ενός βιομετρικού συστήματος. Παρά τα πλεονεκτήματα αυτά, υπάρχουν πολλά ανοικτά ζητήματα που σχετίζονται με αυτά τα συστήματα. Ωστόσο, οι συνεχείς προσπάθειες έρευνας στοχεύουν στην επίλυση των ανοιχτών θεμάτων που σχετίζονται με τον τομέα της προσαρμοστικής βιομετρίας [17].

Τον τελευταίο καιρό έχουν προκύψει βιομετρικά στοιχεία που βασίζονται σε σήματα εγκεφάλου (ηλεκτροεγκεφαλογράφημα) και καρδιά (ηλεκτροκαρδιογράφημα). Η ερευνητική ομάδα του Πανεπιστημίου του Κεντ, με επικεφαλή τον Ramaswamy Palaniappan, έχει δείξει ότι οι άνθρωποι έχουν συγκεκριμένα διακριτά μοτίβα εγκεφάλου και καρδιάς τα

οποία είναι μοναδικά για κάθε άτομο. Ένα άλλο παράδειγμα είναι η αναγνώριση των φλεβών των δακτύλων, χρησιμοποιώντας τεχνικές αναγνώρισης προτύπων, βασισμένες σε εικόνες ανθρώπινων αγγειακών μοτίβων. Το πλεονέκτημα μιας τέτοιας τεχνολογίας είναι ότι είναι πιο ανθεκτικό στην απάτη σε σύγκριση με τα συμβατικά βιομετρικά στοιχεία όπως τα δακτυλικά αποτυπώματα. Ωστόσο, αυτή η τεχνολογία είναι γενικά πιο περίπλοκη και εξακολουθεί να έχει ζητήματα όπως η χαμηλότερη ακρίβεια και η κακή αναπαραγωγικότητα με την πάροδο του χρόνου. Αυτή η νέα γενιά βιομετρικών συστημάτων ονομάζεται βιομετρία προθέσεως και αποσκοπεί στην ανίχνευση της πρόθεσης. Η τεχνολογία θα αναλύει τα φυσιολογικά χαρακτηριστικά όπως η κίνηση των ματιών, η θερμοκρασία του σώματος, η αναπνοή κ.λπ. και θα προβλέπουν επικίνδυνη συμπεριφορά ή εχθρική πρόθεση προτού συμβεί.

Όσον αφορά την πλευρά της φορητότητας των βιομετρικών προϊόντων, μικροσκοπικά συστήματα βιομετρικής πιστοποίησης (BAS), οδηγούν σε εξοικονόμηση κόστους, ειδικά για μεγάλης κλίμακας υλοποιήσεις.

2.1 Θέματα και ανησυχίες

2.1.1 Ανθρώπινη αξιοπρέπεια

Τα βιομετρικά στοιχεία θεωρήθηκαν επίσης χρήσιμα για την ανάπτυξη της κρατικής εξουσίας. Μετατρέποντας το ανθρώπινο άτομο σε συλλογή βιομετρικών δεδομένων, η βιομετρία θα αποθάρρυνε τον άνθρωπο να παραβιάζει την σωματική ακεραιότητα του και, τελικά, να προσβάλλει την ανθρώπινη αξιοπρέπεια.

Σε μια γνωστή περίπτωση, ο ιταλός φιλόσοφος Giorgio Agamben αρνήθηκε να εισέλθει στις Ηνωμένες Πολιτείες σε ένδειξη διαμαρτυρίας για την απαίτηση του προγράμματος Visitor and Immigrant Status Indicator (US-VISIT) του Ηνωμένου Βασιλείου να αποτυπώνονται και να φωτογραφίζονται οι επισκέπτες. Ο Agamben υποστήριξε ότι η συλλογή βιομετρικών δεδομένων είναι μια μορφή βιοπολιτικού τατουάζ, παρόμοια με το τατουάζ των Εβραίων κατά τη διάρκεια του Ολοκαυτώματος. Σύμφωνα με τον Agamben, τα βιομετρικά στοιχεία μετατρέπουν το ανθρώπινο πρόσωπο σε γυμνό σώμα. Ο Agamben αναφέρεται στις δύο λέξεις που χρησιμοποίησαν οι αρχαίοι Έλληνες για την ένδειξη ”ζωή”, η οποία είναι η κοινή ζωή των ζώων και των ανθρώπων, απλή ζωή. και το βιολογική ζωή, που είναι η ζωή στο ανθρώπινο πλαίσιο, με έννοιες και σκοπούς. Ο Agamben προβλέπει τη μείωση σε γυμνά σώματα για ολόκληρη την ανθρωπότητα. Για αυτόν, μια νέα βιοπολι-

τική σχέση μεταξύ πολιτών και κράτους μετατρέπει τους πολίτες σε καθαρή βιολογική ζωή που τους στερεί από την ανθρωπότητα τους και τα βιομετρικά στοιχεία θα δημιουργήσουν αυτόν τον νέο κόσμο.

Ο μελετητής επιτήρησης Simone Browne διατυπώνει παρόμοια κριτική με τον Agamben, επικαλούμενος μια πρόσφατη μελέτη σχετικά με την έρευνα και ανάπτυξη βιομετρικών στοιχείων που διαπίστωσε ότι το σύστημα ταξινόμησης των φύλων που έχει ερευνηθεί ”τείνει να ταξινομήσει τους Αφρικανούς ως αρσενικά Mongoloids ». Συνεπώς, ο Browne υποστηρίζει ότι η σύλληψη μιας αντικειμενικής βιομετρικής τεχνολογίας είναι δύσκολη αν τέτοια συστήματα έχουν σχεδιασθεί υποκειμενικά και είναι ευάλωτα να προκαλέσουν σφάλματα όπως περιγράφονται στην παραπάνω μελέτη. Η έντονη επέκταση των βιομετρικών τεχνολογιών τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα μεγεθύνει αυτή την ανησυχία. Η αυξανόμενη εμπορευματοποίηση των βιομετρικών στοιχείων από τον ιδιωτικό τομέα προσθέτει σε αυτόν τον κίνδυνο απώλειας ανθρώπινης αξίας. Πράγματι, οι εταιρείες εκτιμούν τα βιομετρικά χαρακτηριστικά περισσότερο από ό, τι τα εκτιμούν τα άτομα. Ο Browne υποστηρίζει ότι η σύγχρονη κοινωνία θα πρέπει να ενσωματώσει μια ”βιομετρική συνείδηση” που να συνεπάγεται ενημερωμένο δημόσιο διάλογο γύρω από αυτές τις τεχνολογίες και την εφαρμογή τους, καθώς και τη λογοδοσία του κράτους και του ιδιωτικού τομέα, όπου η ιδιοκτησία και η πρόσβαση στα δεδομένα του σώματος ή άλλη πνευματική ιδιοκτησία που παράγεται από τα δεδομένα του σώματος του ατόμου πρέπει να νοείται ως δικαίωμα. ”

Άλλοι μελετητές υπογράμμισαν ωστόσο ότι ο παγκοσμιοποιημένος κόσμος βρίσκεται αντιμέτωπος με μια τεράστια μάζα ανθρώπων με αδύναμες ή απούσες πολιτικές ταυτότητες. Οι περισσότερες αναπτυσσόμενες χώρες έχουν αδύναμα και αναξιόπιστα έγγραφα και οι φτωχότεροι σε αυτές τις χώρες δεν έχουν ούτε αυτά τα αναξιόπιστα έγγραφα . Χωρίς πιστοποιημένες προσωπικές ταυτότητες, δεν υπάρχει καμία βεβαιότητα δικαιώματος, καμία πολιτική ελευθερία. Μπορεί κανείς να διεκδικήσει τα δικαιώματά του, συμπεριλαμβανομένου του δικαιώματος να αρνηθεί την ταυτοποίησή του, μόνο εάν είναι αναγνωρίσιμο θέμα, αν έχει δημόσια ταυτότητα. Με αυτή την έννοια, τα βιομετρικά στοιχεία θα μπορούσαν να διαδραματίσουν κεντρικό ρόλο στην υποστήριξη και προαγωγή του σεβασμού της ανθρώπινης αξιοπρέπειας και των θεμελιωδών δικαιωμάτων.

Η βιομετρία της πρόθεσης ενέχει περαιτέρω κινδύνους. Στην επιστολή του στο Harvard International Review, ο καθηγητής Nayef Al-Rodhan προειδοποιεί για τους υψηλούς κινδύνους εσφαλμένων υποτιμήσεων, καταχρηστικών κατηγοριών και παραβιάσεων των πολιτικών ελευθεριών. Οι επικριτές στις ΗΠΑ σηματοδότησαν επίσης μια σύγκρουση με την 4η τροποποίηση.

2.1.2 Απόρρητο και διακρίσεις

Είναι πιθανό τα δεδομένα που λαμβάνονται κατά τη διάρκεια της βιομετρικής εγγραφής να μπορούν να χρησιμοποιηθούν με τρόπους για τους οποίους το εγγεγραμμένο άτομο δεν έχει συναινέσει. Για παράδειγμα, τα περισσότερα βιομετρικά χαρακτηριστικά θα μπορούσαν να αποκαλύψουν φυσιολογικές και παθολογικές ιατρικές παθήσεις (π.χ. ορισμένα σχέδια δακτυλικών αποτυπωμάτων σχετίζονται με χρωμοσωμικές ασθένειες, τα πρότυπα ίριδας θα μπορούσαν να αποκαλύψουν γενετικό φύλο, τα μοτίβα των φλεβών θα μπορούσαν να αποκαλύψουν αγγειακές παθήσεις, οι περισσότερες βιομετρικές συμπεριφορές θα μπορούσαν να αποκαλύψουν νευρολογικές ασθένειες, κ.λπ.). Επιπλέον, η βιομετρία δεύτερης γενιάς, και ιδίως η συμπεριφορική και η ηλεκτρο-φυσιολογική βιομετρία (π.χ. με βάση την ηλεκτροκαρδιογραφία, την ηλεκτροεγκεφαλογραφία, την ηλεκτρομυογραφία), θα μπορούσαν επίσης να χρησιμοποιηθούν για ανίχνευση συναισθημάτων.

Υπάρχουν τρεις κατηγορίες ανησυχιών για την προστασία της ιδιωτικής ζωής:

- Αθέλητο λειτουργικό πεδίο: Ο έλεγχος ταυτότητας υπερβαίνει τον έλεγχο ταυτότητας, όπως η εύρεση όγκου.

- Αθέλητο πεδίο εφαρμογής: Η διαδικασία επαλήθευσης αναγνωρίζει σωστά το άτομο όταν το άτομο δεν επιθυμεί να αναγνωριστεί.

- Ταυτοποιημένη ταυτότητα: Το άτομο εντοπίζεται χωρίς να αναζητηθεί ταυτοποίηση ή ταυτότητα, δηλαδή το πρόσωπο ενός ατόμου εντοπίζεται σε ένα πλήθος.

2.1.3 Κίνδυνος για τους ιδιοκτήτες ασφαλισμένων αντικειμένων

Όταν οι κλέφτες δεν μπορούν να αποκτήσουν πρόσβαση σε ασφαλείς ιδιότητες, υπάρχει πιθανότητα οι κλέφτες να καταδιώξουν και να επιτεθούν στον ιδιοκτήτη της περιουσίας για να αποκτήσουν πρόσβαση. Εάν το στοιχείο είναι ασφαλισμένο με μια βιομετρική συσκευή, η ζημιά στον ιδιοκτήτη μπορεί να είναι μη αναστρέψιμη και ενδεχομένως να κοστίζει περισσότερο από την εγγεγραμμένη ιδιοκτησία. Για παράδειγμα, το 2005, οι κλοπές αυτοκινήτων της Μαλαισίας έκοψαν το δάκτυλο ενός ιδιοκτήτη της Mercedes-Benz S-Class όταν προσπάθησαν να κλέψουν το αυτοκίνητο.

2.1.4 Διεθνής ανταλλαγή βιομετρικών δεδομένων

Πολλές χώρες, συμπεριλαμβανομένων των Ηνωμένων Πολιτειών, σκοπεύουν να μοιραστούν βιομετρικά δεδομένα με άλλα έθνη.

Σε μαρτυρία ενώπιον της επιτροπής των ΗΠΑ για τις πιστώσεις του Κοινοβουλίου, η Υποεπιτροπή Εσωτερικής Ασφάλειας για την «βιομετρική ταυτοποίηση» το 2009, οι Kathleen Kraninger και Robert A Mocny σχολίασαν τη διεθνή συνεργασία σε σχέση με τα βιομετρικά δεδομένα, ως εξής:

”Για να διασφαλίσουμε ότι μπορούμε να κλείσουμε τα τρομοκρατικά δίκτυα πριν φτάσουν ποτέ στις Ηνωμένες Πολιτείες, πρέπει επίσης να αναλάβουμε ηγετικό ρόλο στην προώθηση διεθνών βιομετρικών προτύπων. Με την ανάπτυξη συμβατών συστημάτων, θα είμαστε σε θέση να μοιραζόμαστε με ασφάλεια τα στοιχεία της τρομοκρατίας σε διεθνές επίπεδο για να ενισχύσουμε τις άμυνές μας. Ακριβώς όπως βελτιώνουμε τον τρόπο με τον οπο+ίο συνεργαζόμαστε εντός της κυβέρνησης των ΗΠΑ για τον εντοπισμό και την εξάλειψη τρομοκρατών και άλλων επικίνδυνων ανθρώπων, έχουμε την ίδια υποχρέωση να συνεργαστούμε με τους εταίρους μας στο εξωτερικό για να εμποδίσουμε τους τρομοκράτες να μην εντοπίσουν οποιαδήποτε κίνηση. Η βιομετρία παρέχει έναν νέο τρόπο να φέρει στο φως την αληθινή ταυτότητα των τρομοκρατών, αποφορτίζοντάς τους από το μεγαλύτερο πλεονέκτημά τους-που παραμένει άγνωστο. ”

Σύμφωνα με άρθρο που δημοσίευσε το 2009 ο S. Magnuson στο περιοδικό National Defense με τίτλο ”Τμήμα Άμυνας υπό πίεση για την από κοινού χρήση βιομετρικών δεδομένων”, οι Ηνωμένες Πολιτείες έχουν διμερείς συμφωνίες με άλλα έθνη με στόχο την ανταλλαγή βιομετρικών δεδομένων . Για να αναφέρετε αυτό το άρθρο:

”Ο Μίλερ [σύμβουλος της Υπηρεσίας Ατομικής Προστασίας και Αμερικανικών Υποθέσεων Ασφάλειας δήλωσε ότι οι Ηνωμένες Πολιτείες έχουν διμερείς συμφωνίες για την κοινή χρήση βιομετρικών δεδομένων με περίπου 25 χώρες. Κάθε φορά που ένας ξένος ηγέτης έχει επισκεφθεί την Ουάσινγκτον τα τελευταία χρόνια, το Υπουργείο Εξωτερικών έχει βεβαιωθεί ότι υπογράφουν μια τέτοια συμφωνία. ”

2.2 Χώρες που εφαρμόζουν βιομετρικά στοιχεία

Οι χώρες που χρησιμοποιούν βιομετρικά στοιχεία περιλαμβάνουν την Αυστραλία, τη Βραζιλία, τον Καναδά, την Κύπρο, την Ελλάδα, την Κίνα, τη Γκάμπια, τη Γερμανία,

την Ινδία, το Ιράκ, το Ισραήλ, την Ιταλία, τη Μαλαισία, την Ολλανδία, τη Νέα Ζηλανδία, τη Νιγηρία, Ουκρανία, Ηνωμένα Αραβικά Εμιράτα, Ηνωμένο Βασίλειο, Ηνωμένες Πολιτείες και Βενεζουέλα.

Μεταξύ των χωρών με χαμηλό και μεσαίο εισόδημα, περίπου 1,2 δισεκατομμύρια άνθρωποι έχουν ήδη λάβει αναγνώριση μέσω ενός βιομετρικού προγράμματος αναγνώρισης .

Υπάρχουν επίσης πολλές χώρες που εφαρμόζουν βιομετρική αναγνώριση για την εγγραφή ψηφοφόρων και παρόμοιους εκλογικούς σκοπούς. Σύμφωνα με τις Διεθνείς Βάσεις Δεδομένων για τις ΤΠΕ στην εκλογική βάση , μερικές από τις χώρες που χρησιμοποιούν τη Βιομετρική Εγγραφή Βουλευτών (BVR) (2017) είναι η Αρμενία, η Αγκόλα, το Μπαγκλαντές, το Μπουτάν, η Βολιβία, η Βραζιλία, η Μπουρκίνα Φάσο, η Καμπότζη, , Κομόρες, Κονγκό, Ακτή Ελεφαντοστού, Δομινικανή Δημοκρατία, Φίτζι, Γκάμπια, Γκάνα, Γουατεμάλα, Ινδία, Ιράκ, Κένυα, Λεσόθο, Λιβερία, Μαλάουι, Μάλι, Μαυριτανία, Μεξικό, Μαρόκο, Μοζαμβίκη, Ναμίμπια , Το Νεπάλ, τη Νικαράγουα, τη Νιγηρία, τον Παναμά, το Περού, τις Φιλιππίνες, τη Σενεγάλη, τη Σιέρα Λεόνε, τις Νήσους Σολομώντος, τη Σομαλιλάνδη, τη Σουαζιλάνδη, την Τανζανία, την Ουγκάντα, την Ουρουγουάη, τη Βενεζουέλα, την Υεμένη, τη Ζάμπια και τη Ζιμπάμπουε.

2.3 Μια ιστορική αναδρομή

Μια πρώιμη καταγραφή των δακτυλικών αποτυπωμάτων χρονολογείται από το 1891 όταν ο Juan Vucetich ξεκίνησε μια συλλογή δακτυλικών αποτυπωμάτων εγκληματιών στην Αργεντινή. Οι Josh Ellenbogen και Nitzan Lebovic υποστήριξαν ότι η βιομετρία προέρχεται από τα συστήματα αναγνώρισης της εγκληματικής δραστηριότητας που αναπτύχθηκε από τον Alphonse Bertillon (1853-1914) και από τη θεωρία των δακτυλικών αποτυπωμάτων και φυσιογνωμίας του Francis Galton Σύμφωνα με τον Lebovic, το έργο του Galton οδήγησε στην εφαρμογή μαθηματικών μοντέλων σε δακτυλικά αποτυπώματα, φρενολογία και χαρακτηριστικά του προσώπου", ως μέρος της "απόλυτης αναγνώρισης" και "κλειδί για την ένταξη και τον αποκλεισμό" των πληθυσμών. Κατά συνέπεια, «το βιομετρικό σύστημα είναι το απόλυτο πολιτικό όπλο της εποχής μας» και μια μορφή «μαλακού ελέγχου». Ο θεωρητικός David Lyon έδειξε ότι κατά τη διάρκεια των τελευταίων δύο δεκαετιών τα βιομετρικά συστήματα έχουν διεισδύσει στην πολιτική αγορά και έχουν θολώσει

τις γραμμές μεταξύ κυβερνητικών μορφών ελέγχου και ιδιωτικού εταιρικού ελέγχου. Η Κέλι Α. Γκέιτς αναγνώρισε την 11η Σεπτεμβρίου ως την κρίσιμη καμπή της πολιτιστικής γλώσσας του παρόντος: «Στη γλώσσα των πολιτιστικών σπουδών, οι συνέπειες της 9/11 ήταν μια στιγμή της άρθρωσης, όπου αντικείμενα ή γεγονότα που δεν έχουν καμία αναγκαία σχέση έρχονται μαζί και δημιουργείται ένας νέος σχηματισμός λόγου: αυτοματοποιημένη αναγνώριση προσώπου ως τεχνολογία εθνικής ασφάλειας ». Kelly A. Gates, Το βιομετρικό μέλλον μας: Τεχνολογία αναγνώρισης προσώπου και η κουλτούρα επιτήρησης (New York, 2011).

3. ΟΜΟΜΟΡΦΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η ομομορφική κρυπτογράφηση είναι μια μορφή κρυπτογράφησης που επιτρέπει τους υπολογισμούς σε κρυπτοκείμενα, δημιουργώντας ένα κρυπτογραφημένο αποτέλεσμα το οποίο όταν αποκρυπτογραφείται, ταιριάζει με το αποτέλεσμα των πράξεων σαν να είχαν εκτελεστεί στο απλό κείμενο.

Η ομομορφική κρυπτογράφηση μπορεί να χρησιμοποιηθεί για την αποθήκευση και τον υπολογισμό δεδομένων με βάση την προστασία της ιδιωτικής ζωής. Αυτό επιτρέπει την κρυπτογράφηση των δεδομένων και την εξαγωγή τους σε περιβάλλοντα συννέφων για επεξεργασία, ενώ όλα αυτά είναι κρυπτογραφημένα. Σε βιομηχανίες με υψηλό ρυθμό ανάγνωσης και επεξεργασίας δεδομένων, όπως η υγειονομική περίθαλψη, μπορεί να χρησιμοποιηθεί ομομορφική κρυπτογράφηση για να ενεργοποιηθούν οι νέες υπηρεσίες, αφαιρώντας τα εμπόδια απορρήτου που εμποδίζουν την ανταλλαγή δεδομένων. Για παράδειγμα, οι προγνωστικές αναλύσεις στην υγειονομική περίθαλψη μπορεί να είναι δύσκολο να εφαρμοστούν λόγω ανησυχιών για την προστασία της ιδιωτικής ζωής των ιατρικών δεδομένων, αλλά εάν ο παροχέας υπηρεσιών πρόβλεψης αναλυτικών δεδομένων μπορεί να λειτουργήσει με κρυπτογραφημένα δεδομένα, αυτά τα προβλήματα προστασίας της ιδιωτικής ζωής μειώνονται.

Η ομομορφική κρυπτογράφηση είναι μια μορφή κρυπτογράφησης με πρόσθετη δυνατότητα αξιολόγησης για υπολογιστικά κρυπτογραφημένα δεδομένα χωρίς πρόσβαση στο μυστικό κλειδί. Το αποτέλεσμα ενός τέτοιου υπολογισμού παραμένει κρυπτογραφημένο. Η ομομορφική κρυπτογράφηση μπορεί να θεωρηθεί ως επέκταση κρυπτογράφησης είτε με συμμετρικό κλειδί είτε με δημόσιο κλειδί. Η ομομορφική κρυπτογράφηση αναφέρεται στην άλγεβρα ως ομομορφισμός: οι λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης μπορούν να θεωρηθούν ως ομομορφισμοί μεταξύ διαστημάτων απλού κειμένου και κρυπτοκειμένου.

Η ομομορφική κρυπτογράφηση περιλαμβάνει πολλούς τύπους σχημάτων κρυπτογράφησης που μπορούν να εκτελέσουν διαφορετικές κατηγορίες υπολογισμών σε κρυπτογραφημένα δεδομένα. Κάποιοι συνηθισμένοι τύποι ομομορφικής κρυπτογράφησης είναι:

- μερικώς ομομορφικοί,
- κάπως ομομορφικοί,
- επίπεδοι πλήρως ομομορφικοί,

- πλήρως ομομορφικοί.

Οι υπολογισμοί αντιπροσωπεύονται είτε ως Boolean είτε ως αριθμητικά κυκλώματα.

- Η εν μέρει ομομορφική κρυπτογράφηση περιλαμβάνει σχέδια που υποστηρίζουν την αξιολόγηση κυκλωμάτων που αποτελούνται από έναν μόνο τύπο πύλης, π.χ. προσθήκη ή πολλαπλασιασμό.

- Τα κάπως ομομορφική συστήματα κρυπτογράφησης μπορούν να αξιολογήσουν δύο τύπους πυλών, αλλά μόνο για ένα υποσύνολο κυκλωμάτων.

- Η επίπεδη πλήρως ομομορφορική κρυπτογράφηση υποστηρίζει την αξιολόγηση αυθαίρετων κυκλωμάτων οριοθετημένου (προκαθορισμένου) βάθους.

- Η πλήρως ομομορφορική κρυπτογράφηση (FHE) επιτρέπει την αξιολόγηση αυθαίρετων κυκλωμάτων χωρίς βάθος και είναι η ισχυρότερη έννοια της ομομορφικής κρυπτογράφησης.

Για την πλειονότητα των ομομορφικών σχημάτων κρυπτογράφησης, το πολλαπλασιαστικό βάθος των κυκλωμάτων είναι ο κύριος πρακτικός περιορισμός των υπολογισμών σε κρυπτογραφημένα δεδομένα.

Τα ομόμορφα σχήματα κρυπτογράφησης είναι εγγενώς ευέλικτα. Όσον αφορά την ευελιξία, τα ομομορφοποιημένα συστήματα κρυπτογράφησης έχουν ασθενέστερη ασφάλεια από τα μη ομομορφικά σχήματα.

3.1 Πλήρως ομομορφική κρυπτογράφηση

Ένα κρυπτοσύστημα που υποστηρίζει αυθαίρετους υπολογισμούς σε κρυπτοκείμενα είναι γνωστό ως πλήρως ομομορφική κρυπτογράφηση (FHE)[11]. Ένα τέτοιο σχήμα επιτρέπει την κατασκευή προγραμμάτων για οποιαδήποτε επιθυμητή λειτουργία, η οποία μπορεί να εκτελεστεί σε κρυπτογραφημένες εισόδους για την κρυπτογράφηση του αποτελέσματος. Δεδομένου ότι ένα τέτοιο πρόγραμμα δεν χρειάζεται ποτέ να αποκρυπτογραφήσει τις εισόδους του, μπορεί να γίνει από ένα μη αξιόπιστο άτομο χωρίς να αποκαλύψει τις εισόδους του και την εσωτερική του κατάσταση. Τα πλήρως ομομορφικά κρυπτοσυστήματα έχουν μεγάλες πρακτικές συνέπειες στην εξωτερική ανάθεση ιδιωτικών υπολογι-

σμών, για παράδειγμα, στο πλαίσιο του cloud computing.

3.1.1 Υλοποιήσεις

Δεν υπάρχουν ενεργά αναπτυγμένες υλοποιήσεις συστημάτων πρώτης γενιάς. Υπάρχουν πολλές εφαρμογές ανοιχτού κώδικα των πλήρως ομομορφικών συστημάτων κρυπτογράφησης δεύτερης και τρίτης γενιάς. Οι εφαρμογές FHE δεύτερης γενιάς συνήθως λειτουργούν σε επίπεδο ισοτιμίας FHE (αν και το bootstrapping εξακολουθεί να είναι διαθέσιμο σε ορισμένες βιβλιοθήκες) και υποστηρίζει αποτελεσματική συσκευασία δεδομένων τύπου SIMD. Χρησιμοποιούνται συνήθως για τον υπολογισμό κρυπτογραφημένων ακεραίων ή πραγματικών / πολύπλοκων αριθμών. Οι εφαρμογές FHE τρίτης γενιάς εκτελούν συχνά εκκίνηση μετά από κάθε λογική πράξη αλλά έχουν περιορισμένη υποστήριξη για τη συσκευασία και αποδοτικούς αριθμητικούς υπολογισμούς. Χρησιμοποιούνται συνήθως για τον υπολογισμό κυκλωμάτων Boolean πάνω σε κρυπτογραφημένα bit. Η επιλογή της χρήσης μιας δεύτερης γενιάς έναντι τρίτης γενεάς εξαρτάται από τους τύπους δεδομένων εισόδου και τον επιθυμητό υπολογισμό.

3.1.2 Εφαρμογές FHE δεύτερης γενιάς

- Η Helib από την IBM εφαρμόζει το σύστημα BGV με τις βελτιστοποιήσεις του GHS και το σύστημα CKKS.
- Το Microsoft SEAL εφαρμόζει τα προγράμματα κρυπτογράφησης BFV και CKKS.
- PALISADE από μια κοινοπραξία αμυντικών εργολάβων και ακαδημαϊκών, συμπεριλαμβανομένου του Ινστιτούτου Τεχνολογίας του Νιου Τζέρσεϋ, της διπλής τεχνολογίας, της Raytheon BBN Technologies, του MIT, του Πανεπιστημίου της Καλιφόρνια, του Σαν Ντιέγκο και άλλων. Το PALISADE είναι βιβλιοθήκη κρυπτογραφίας πλέγματος γενικής χρήσης που εφαρμόζει τα συστήματα BFV, BGV και άλλα.
- Το HEAAN από το Εθνικό Πανεπιστήμιο της Σεούλ εφαρμόζει το σύστημα CKKS μαζί με το bootstrapping.

3.1.3 Εφαρμογές FHE τρίτης γενιάς

- Το FHEW από τους Leo Ducas και Daniele Micciancio εφαρμόζει το σύστημα FHEW.

- Η TFHE της Ilaria Chillotti, του Nicolas Gama, της Mariya Georgieva και της Malika Izabachene εφαρμόζουν το σύστημα TFHE [5].

3.1.4 Τυποποίηση

Ένα κοινοτικό πρότυπο για την ομομορφορική κρυπτογράφηση διατηρείται από τον όμιλο HomomorphicEncryption.org, μια ανοιχτή κοινοπραξία βιομηχανίας/κυβέρνησης/ακαδημαϊκής κοινότητας που ιδρύθηκε το 2017. Το τρέχον πρότυπο έγγραφο περιλαμβάνει προδιαγραφές ασφαλών παραμέτρων για το RLWE.

Ένας ενημερωμένος κατάλογος ομομορφικών εφαρμογών κρυπτογράφησης διατηρείται επίσης από την κοινοπραξία.

3.2 Μερικώς ομομορφικά κρυπτοσυστήματα

3.2.1 Paillier

Στο κρυπτοσύστημα Paillier,το οποιό εφαρμόζουμε και στην εργασία μας, εάν το δημόσιο κλειδί είναι το μέτρο m και η βάση g, τότε η κρυπτογράφηση ενός μηνύματος x είναι E(x) = gx *rm mod m2 για τυχαία r ε 0,……,m – 1. Η ομομορφική ιδιότητα είναι τότε:

$$E(x_1) * E(x_2) = (g^{x_1} * r_1^m) * (g^{x_2} * r_2^m) mod m^2 = g^{x_1+x_2}(r_1 r_2)^m mod m^2 = E(x_1 + x_2)$$

3.2.2 Άλλα μερικώς ομομορφικά κρυπτοσυστήματα

- Κρυπτοσύστημα Okamoto-Uchiyama,
- Κρυπτοσύστημα Naccache-Stern,
- Κρυπτοσύστημα Damgard-Jurik,
- Σύστημα κρυπτογράφησης Sander-Young-Yung,
- Κρυπτοσύστημα Boneh-Goh-Nissim,
- Κρυπτοσύστημα Ishai-Paskin,
- Κρυπτοσύστημα Castagnos-Laguillaumie.

3.3 Μια ιστορική αναδρομή

Τα ομομορφικά συστήματα κρυπτογράφησης έχουν αναπτυχθεί χρησιμοποιώντας διαφορετικές προσεγγίσεις. Συγκεκριμένα, τα πλήρως ομοιομορφικά συστήματα κρυπτογράφησης συχνά ομαδοποιούνται σε γενιές που αντιστοιχούν στην υποκείμενη προσέγγιση.

3.3.1 Pre-FHE

Το πρόβλημα της κατασκευής ενός πλήρως ομομορφικού συστήματος κρυπτογράφησης προτάθηκε για πρώτη φορά το 1978, εντός ενός έτους από τη δημοσίευση του σχεδίου RSA. Για περισσότερα από 30 χρόνια, δεν ήταν σαφές εάν υπήρχε λύση. Κατά την περίοδο αυτή, τα μερικά αποτελέσματα περιλάμβαναν τα ακόλουθα συστήματα:

- Κρυπτοσύστημα RSA (απεριόριστος αριθμός δομοστοιχειωτών πολλαπλασιασμών)
- Κρυπτοσύστημα ElGamal (απεριόριστος αριθμός αρθρωτών πολλαπλασιασμών)
- Κρυπτοσύστημα Goldwasser-Micali (περιορισμένος αριθμός πράξεων)
- Benaloh κρυπτοσύστημα (απεριόριστος αριθμός αρθρωτών προσθέσεων)
- Κρυπτοσύστημα Paillier (απεριόριστος αριθμός αρθρωτών προσθέσεων)
- Σύστημα Sander-Young-Yung (μετά από περισσότερα από 20 χρόνια λύθηκε το πρόβλημα για λογαριθμικά κυκλώματα βάθους)
- Κρυπτοσύστημα Boneh-Goh-Nissim (απεριόριστος αριθμός λειτουργιών πρόσθεσης, αλλά το πολύ ένας πολλαπλασιασμός)
- Κρυπτοσύστημα Ishai-Paskin (προγράμματα διακλάδωσης πολυωνυμικού μεγέθους)

3.3.2 First-Generation FHE

Ο Craig Gentry, χρησιμοποιώντας κρυπτογράφηση βασισμένη σε πλέγματα, περιέγραψε την πρώτη εύλογη κατασκευή για ένα πλήρως ομομορφικό σχήμα κρυπτογράφησης. Το σχέδιο Gentry υποστηρίζει τόσο λειτουργίες πρόσθεσης όσο και πολλαπλασιασμού σε κρυπτοκείμενα, από τα οποία είναι δυνατή η κατασκευή κυκλωμάτων για την εκτέλεση αυθαίρετων υπολογισμών. Η κατασκευή ξεκινά από ένα κάπως ομομορφικό σχήμα κρυπτογράφησης, το οποίο περιορίζεται στην αξιολόγηση πολυωνύμων χαμηλού βαθμού

έναντι κρυπτογραφημένων δεδομένων. Είναι περιορισμένη επειδή κάθε κρυπτογράφημα είναι θορυβώδες με κάποια έννοια και αυτός ο θόρυβος αυξάνεται καθώς κάποιος προσθέτει και πολλαπλασιάζει τα κρυπτογραφημένα κείμενα, μέχρι που τελικά ο θόρυβος καθιστά το κρυπτοκείμενο να μην μπορεί να διακριθεί. Ο Gentry δείχνει πώς να τροποποιήσει ελαφρώς αυτό το σχέδιο για να το κάνει bootstrappable, δηλ. Ικανό να αξιολογήσει το δικό του κύκλωμα αποκρυπτογράφησης και έπειτα τουλάχιστον μία ακόμη λειτουργία. Τελικά, δείχνει ότι κάθε εκκίνηση που μπορεί να μετατραπεί σε ομομορφορική κρυπτογράφηση μπορεί να μετατραπεί σε μια πλήρως ομομορφική κρυπτογράφηση μέσω μιας αναδρομικής αυτο-ενσωμάτωσης. Για το ”θορυβώδες” σχήμα του Gentry, η διαδικασία bootstrapping [12] ανανεώνει αποτελεσματικά το κρυπτογράφημα, εφαρμόζοντας ομομορφικά τη διαδικασία αποκρυπτογράφησης, αποκτώντας έτσι ένα νέο κρυπτογράφημα που κρυπτογραφεί την ίδια τιμή όπως πριν αλλά έχει μικρότερο θόρυβο. Με την ”ανανέωση” του κρυπτογράφου περιοδικά κάθε φορά που ο θόρυβος μεγαλώνει πολύ, είναι δυνατόν να υπολογιστεί ένας αυθαίρετος αριθμός προσθηκών και πολλαπλασιασμών χωρίς να αυξηθεί υπερβολικά ο θόρυβος. Ο Gentry βασίζει την ασφάλεια του σχεδίου του στην υποτιθέμενη σκληρότητα του προβλήματος αραιών (ή χαμηλού βάρους) υποσυνόλων. Η διατριβή του Gentry παρέχει πρόσθετες λεπτομέρειες. Η εφαρμογή Gentry-Halevi του αρχικού κρυπτοσυστήματος του Gentry ανέφερε χρονοδιάγραμμα περίπου 30 λεπτών ανά λειτουργία βασικού δυαδικού ψηφίου. Οι εκτεταμένες εργασίες σχεδίασης και υλοποίησης τα επόμενα χρόνια έχουν βελτιωθεί σε αυτές τις πρώιμες υλοποιήσεις με πολλές επιδόσεις εκτέλεσης κατά σειρά μεγεθών.

Το 2010, ο Marten van Dijk, ο Craig Gentry, ο Shai Halevi και ο Vinod Vaikuntanathan [21] παρουσίασαν ένα δεύτερο πλήρως ομομορφικό σύστημα κρυπτογράφησης, το οποίο χρησιμοποιεί πολλά από τα εργαλεία της κατασκευής του Gentry, αλλά δεν απαιτεί ιδανικά πλέγματα. Αντίθετα, δείχνουν ότι η κάπως ομομορφική συνιστώσα του ιδανικού σχεδίου που βασίζεται στο πλέγμα Gentry μπορεί να αντικατασταθεί με ένα πολύ απλό κάπως ομομορφικό σχήμα που χρησιμοποιεί ακέραιους αριθμούς. Επομένως, το σχέδιο είναι απλούστερο από το ιδανικό σύστημα πλέγματος του Gentry, αλλά έχει παρόμοιες ιδιότητες όσον αφορά τις ομομορφικές λειτουργίες και την αποδοτικότητα. Η κάπως ομομορφική συνιστώσα στο έργο των van Dijk et al. είναι παρόμοια με ένα σύστημα κρυπτογράφησης που προτάθηκε από τον Levieil και τον Naccache το 2008, αλλά και σε ένα που προτάθηκε από τον Bram Cohen το 1998. Ωστόσο, η μέθοδος του Cohen δεν είναι καθόλου ομομορφική. Το σχήμα Levieil-Naccache υποστηρίζει μόνο προσθήκες, αλλά μπορεί να τροποποιηθεί για να υποστηρίξει επίσης ένα μικρό αριθμό πολλαπλασιασμών. Πολλές βελτιώσεις και

βελτιστοποιήσεις του σχεδίου των van Dijk et al. προτάθηκαν σε μια σειρά έργων του Jean-Sébastien Coron, του Tancrède Lepoint, του Avradip Mandal, του David Naccache και του Mehdi Tibouchi. Ορισμένα από αυτά τα έργα περιελάμβαναν και υλοποιήσεις των σχεδίων που προέκυψαν.

3.3.3 Second-Generation FHE

Τα ομομορφικά κρυπτοσυστήματα στην τρέχουσα χρήση προέρχονται από τεχνικές που αναπτύχθηκαν από το 2011-2012 από τους Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan και άλλους. Αυτές οι καινοτομίες οδήγησαν στην ανάπτυξη πολύ πιο αποτελεσματικών κάπως και πλήρως ομομορφικών κρυπτοσυστημάτων. Αυτά περιλαμβάνουν:

- Το πρόγραμμα Brakerski-Gentry-Vaikuntanathan (BGV, 2011), με βάση τις τεχνικές του Brakerski-Vaikuntanathan [16]
- Το σύστημα βασισμένο σε NTRU από τους Lopez-Alt, Tromer και Vaikuntanathan (LTV, 2012)
- Το σύστημα Brakerski / Fan-Vercauteren (BFV, 2012), το οποίο βασίζεται στο σύστημα κρυπτοσυστήματος της αμετάβλητης κλίμακας Brakerski
- Το πρόγραμμα βασισμένο σε NTRU από τους Bos, Lauter, Loftus και Naehrig [1] (BLLN, 2013), βασισμένο στο LTV και στο αμετάβλητο κρυπτοσύστημα Brakerski's
- Το σχέδιο Cheon-Kim-Kim-Song (CKKS, 2016) [19]

Η ασφάλεια των περισσότερων από αυτά τα συστήματα βασίζεται στην σκληρότητα του προβλήματος (RLWE), εκτός από τα προγράμματα LTV και BLLN που βασίζονται σε μια υπερβολικά τεταμένη παραλλαγή του υπολογιστικού προβλήματος NTRU. Αυτή η παραλλαγή NTRU παρουσιάστηκε στη συνέχεια ευάλωτη σε επιθέσεις πλέγματος υποπεδίων, γι 'αυτό και αυτά τα δύο συστήματα δεν χρησιμοποιούνται πλέον στην πράξη.

Όλα τα κρυπτοσυστήματα δεύτερης γενιάς εξακολουθούν να ακολουθούν το βασικό σχέδιο της αρχικής κατασκευής του Gentry, δηλαδή να κατασκευάσουν πρώτα ένα κάπως ομομορφικό κρυπτοσύστημα και μετά να το μετατρέψουν σε ένα πλήρως ομομορφικό κρυπτοσύστημα χρησιμοποιώντας bootstrapping.

Ένα χαρακτηριστικό των κρυπτοσυστημάτων δεύτερης γενιάς είναι ότι όλα αυτά χαρακτηρίζονται από πολύ βραδύτερη αύξηση του θορύβου κατά τη διάρκεια των ομομορφικών υπολογισμών. Οι επιπρόσθετες βελτιστοποιήσεις από τους Craig Gentry, Shai Halevi και Nigel Smart είχαν σαν αποτέλεσμα κρυπτοσυστήματα με σχεδόν βέλτιστη ασυμπτωτική πολυπλοκότητα: Η εκτέλεση λειτουργιών T σε δεδομένα κρυπτογραφημένα με την παράμετρο ασφαλείας k έχει πολυπλοκότητα μόνο T * polylog(k). Αυτές οι βελτιστοποιήσεις βασίζονται στις τεχνικές Smart-Vercauteren [6] που επιτρέπουν τη συλλογή πολλών τιμών κειμένου σε ένα απλό κρυπτογράφημα και λειτουργούν σε όλες αυτές τις τιμές κειμένου σε μορφή SIMD. Πολλές από τις προόδους αυτών των κρυπτοσυστημάτων δεύτερης γενιάς μεταφέρθηκαν επίσης στο κρυπτοσύστημα πάνω από τους ακέραιους αριθμούς.

3.3.4 Third-Generation FHE

Το 2013, οι Craig Gentry, Amit Sahai και Brent Waters (GSW) πρότειναν μια νέα τεχνική για την κατασκευή συστημάτων FHE [13] που αποφεύγουν ένα βήμα ”επανεγγραφής” στον ομομορφικό πολλαπλασιασμό. Οι Zvika Brakerski και Vinod Vaikuntanathan παρατήρησαν ότι για ορισμένα είδη κυκλωμάτων το κρυπτοσύστημα GSW χαρακτηρίζεται από ακόμη πιο αργό ρυθμό ανάπτυξης θορύβου και επομένως καλύτερη απόδοση και ισχυρότερη ασφάλεια. Ο Jacob Alperin-Sheriff και ο Chris Peikert περιέγραψαν στη συνέχεια μια πολύ αποτελεσματική τεχνική εκκίνησης βασισμένη σε αυτή την παρατήρηση.

Αυτές οι τεχνικές βελτιώθηκαν περαιτέρω για να αναπτύξουν αποτελεσματικές παραλλαγές δακτυλίου του κρυπτοσυστήματος GSW: FHEW (2014) και TFHE (2016). Το πρόγραμμα FHEW ήταν το πρώτο που έδειξε ότι με την ανανέωση των κρυπτογραφημάτων μετά από κάθε λειτουργία, είναι δυνατό να μειωθεί ο χρόνος εκκίνησης σε ένα κλάσμα του δευτερολέπτου. Το FHEW [8] εισήγαγε μια νέα μέθοδο για τον υπολογισμό των θυρών Boolean σε κρυπτογραφημένα δεδομένα που απλουστεύουν σημαντικά την εκκίνηση και υλοποίησαν μια παραλλαγή της διαδικασίας bootstrapping. Η αποτελεσματικότητα του FHEW βελτιώθηκε περαιτέρω από το σχήμα TFHE, το οποίο υλοποιεί μια παραλλαγή δακτυλίου της διαδικασίας εκκίνησης με χρήση μιας μεθόδου παρόμοιας με αυτή της FHEW.

4. ΚΡΥΠΤΟΣΥΣΤΗΜΑ PAILLIER

Το κρυπτοσύστημα Paillier, το οποίο εφευρέθηκε και ονομάστηκε από τον Pascal Paillier το 1999, είναι ένας πιθανοτικός ασύμμετρος αλγόριθμος για την κρυπτογραφία με δημόσιο κλειδί [20]. Το πρόβλημα της υπολογιστικής n-th κλάσεων θεωρείται ότι είναι υπολογιστικά δύσκολο. Η υπόθεση λήψης σύνθετης απόλυτης απόκλισης είναι η υπόθεση ακεραιότητας στην οποία βασίζεται αυτό το κρυπτοσύστημα.

Το σχήμα είναι ένα πρόσθετο ομομορφικό κρυπτοσύστημα. αυτό σημαίνει ότι, με δεδομένο μόνο το δημόσιο κλειδί και την κρυπτογράφηση m1 και m2, μπορεί να υπολογιστεί η κρυπτογράφηση του $m1 + m2$.

Ιδιαίτερη αναφορά πρέπει να γίνει στον υλοποιημένο κώδικα κρυπτογράφησης Paillier που χρησιμοποιήθηκε, από τον Mike Ivanov [15] και παρέχεται ελεύθερα στο GitHub.

4.1 Αλγόριθμος

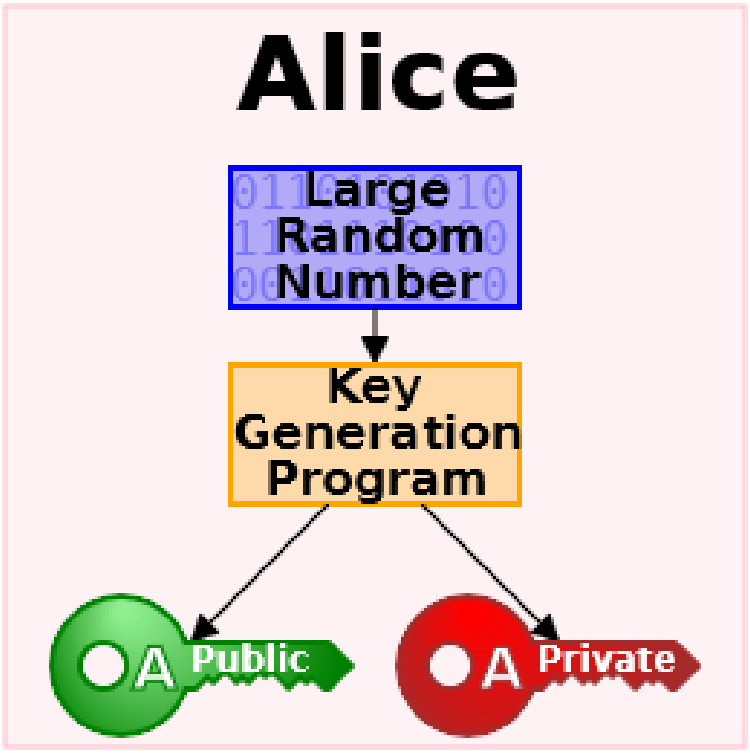
4.1.1 Δημιουργία κλειδιών

- Επιλέξτε δύο μεγάλους πρώτους αριθμούς p και q τυχαία και ανεξάρτητα ο ένας από τον άλλο έτσι ώστε $gcd(pq, (p-1)(q-1)) = 1$. Αυτή η ιδιότητα είναι εξασφαλισμένη εάν και οι δύο πρώτοι αριθμοί έχουν το ίδιο μήκος.
- Υπολογισμός $n = pq$ και $\lambda = lcm(p–1, q–1)$. Το lcm σημαίνει Μικρότερο Κοινό Πολλαπλάσιο.
- Επιλογή τυχαίου ακέραιου g όπου $g \epsilon {Z_{n^2}}^*$
- Βεβαιωθείτε ότι το n διαιρεί τη σειρά g ελέγχοντας την ύπαρξη του παρακάτω αρθρωτού πολλαπλασιαστικού αντιστρόφου: $m = (L(g^\lambda mod n^2))^{-1} mod n$,όπου η συνάρτηση L ορίζεται ως $L(x) = (x–1)/n$.

Σημειώστε ότι ο συμβολισμός a/b δεν υποδηλώνει τον μορφοποιημένο πολλαπλασιασμό a φορές το αρθρωτό πολλαπλασιαστικό αντίστροφο του b αλλά μάλλον το πηλίκο a διαιρούμενο με b, δηλαδή, η μεγαλύτερη ακέραια τιμή k≥0 για να ικανοποιήσει τη σχέση a≥kb.

- Το δημόσιο κλειδί (κρυπτογράφηση) είναι (n, g)

- Το ιδιωτικό κλειδί (αποκρυπτογράφηση) είναι (λ, ρ)



Σχήμα 4.1: Δημιουργία ζεύγους κλειδιών από την Alice

Αν χρησιμοποιούμε p, q ισοδύναμου μήκους, μια απλούστερη παραλλαγή των παραπάνω βημάτων γενιάς κλειδιών θα ήταν να ορίσουμε $g = n + 1$, $\lambda = k(n)$, και $= k(n) - 1 mod n$, όπου $k(n) = (p–1)(q–1)$.

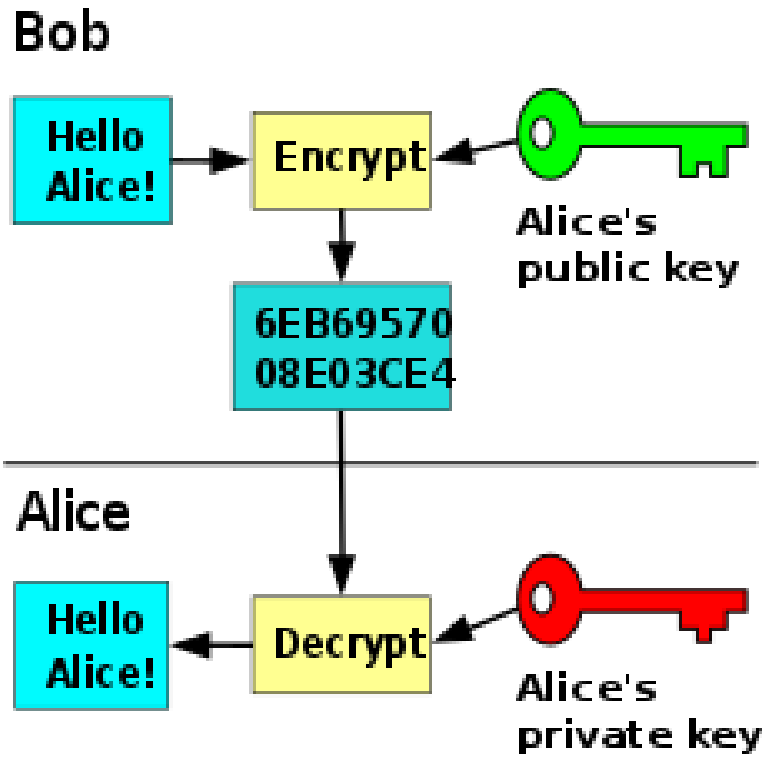
4.1.2 Κρυπτογράφηση

- Έστω m ένα μήνυμα προς κρυπτογράφηση όπου $0 \leq m < n$
- Επιλέξτε τυχαία r όπου $0 < r < n$ και $r \epsilon {Z_{n^2}}^*$(δηλαδή, βεβαιωθείτε ότι $gcd(r, n) = 1$)
- Υπολογίστε το κρυπτογραφικό κείμενο ως εξής: $c = g^m * r^n mod n^2$

4.1.3 Αποκρυπτογράφηση

- Έστω c το κρυπτογράφημα για να αποκρυπτογραφήσει, όπου $c \epsilon {Z_{n^2}}^*$

- Υπολογίστε το μήνυμα του απλού κειμένου ως: $m = L(c^{\lambda} mod n^2) * k mod n$



Σχήμα 4.2: Επικοινωνία του Bob και της Alice κρυπτογραφόντας και αποκρυπτογραφόντας το μήνυμα

4.1.4 Ομομορφικές ιδιότητες

Ένα αξιοσημείωτο χαρακτηριστικό του κρυπτοσυστήματος Paillier είναι οι ομομορφικές του ιδιότητες [10] καθώς και η μη-ντετερμινιστική κρυπτογράφηση του [14]. Καθώς η λειτουργία κρυπτογράφησης είναι προσθετικά ομομορφική, μπορούν να περιγραφούν οι ακόλουθες ταυτότητες:

- **Ομομορφική πρόσθεση απλού κειμένου:**

  Το προϊόν δύο κρυπτοκειμένων θα αποκρυπτογραφηθεί στο άθροισμα των αντίστοιχων απλών κειμένων τους

$$D(E(m_1, r_1) * E(m_2, r_2) mod n^2) = m_1 + m_2 mod n$$

Το προϊόν ενός κρυπτοκειμένου με απλό κείμενο υψωμένο στην g θα αποκρυπτογραφηθεί στο άθροισμα των αντίστοιχων απλών κειμένων

$$D(E(m_1, r_1) * g^{m_2} mod n^2) = m_1 + m_2 mod n$$

- **Ομομορφικός πολλαπλασιασμός απλού κειμένου:**

  Ένα κρυπτογραφημένο απλό κείμενο υψωμένο στην δύναμη ενός άλλου απλού κειμένου θα αποκρυπτογραφηθεί σαν αποτέλεσμα των δύο απλών κειμένων.

$$D(E(m_1, r_1)^{m_2} mod n^2) = m_1 m_2 mod n,$$
$$D(E(m_2, r_2)^{m_1} mod n^2) = m_1 m_2 mod n.$$

  Γενικότερα, ένα κρυπτογραφημένο κείμενο που υψώνεται σε μια σταθερά k, θα αποκρυπτογραφηθεί σαν αποτέλεσμα του απλού κειμένου και της σταθεράς,

$$D(E(m_2, r_2)^k mod n^2) = k m_1 mod n.$$

  Ωστόσο, δεδομένου των κρυπτογραφήσεων Paillier δύο μηνυμάτων δεν υπάρχει γνωστός τρόπος για τον υπολογισμό μιας κρυπτογράφησης του προϊόντος αυτών των μηνυμάτων χωρίς να γνωρίζουμε το ιδιωτικό κλειδί.

4.2 Ιστορικό

Το κρυπτοσύστημα Paillier εκμεταλλεύεται το γεγονός ότι ορισμένοι διακριτοί λογάριθμοι μπορούν να υπολογιστούν εύκολα.

Για παράδειγμα, με διωνυμικό θεώρημα,

$$(1+n)^x = \sum^x{}_{k=0} \binom{x}{k} n^k = 1 + nx + \binom{x}{2} n^2 + \text{higher powers of } n$$

Αυτό δείχνει ότι:

$$(1+n)^x = 1 + nx (mod n^2)$$

Επομένως, αν:

$$y = (1+n)^x mod n^2$$

έπειτα

$$x = (y–1)/n(modn)$$

Ετσι:

$$L((1+n)^x mod n^2) = x(modn),$$

όπου η συνάρτηση L ορίζεται ως $L(u) = (u-1)/n$ και $x \epsilon Z_n$

4.2.1 Σημασιολογική ασφάλεια

Το αρχικό κρυπτοσύστημα, όπως φαίνεται παραπάνω, παρέχει σημασιολογική ασφάλεια ενάντια σε επιλεγμένες επιθέσεις χωρίς εντολές (IND-CPA). Η ικανότητα να διακρίνει κανείς επιτυχώς το πρότυπο κρυπτοκείμενο ουσιαστικά ισοδυναμεί με την ικανότητα να αποφασίζει σύνθετη υπολειμματικότητα. Η αποκαλούμενη υπόθεση λήψης σύνθετων υπολειμματικών αποφάσεων (DCRA) θεωρείται ότι είναι ανυπόστατη.

Λόγω όμως των προαναφερθέντων ομομορφικών ιδιοτήτων, το σύστημα είναι εύπλαστο και επομένως δεν βρίσκεται στο υψηλότερο κλιμάκιο της σημασιολογικής ασφάλειας που προστατεύει τις προσαρμοστικές επιθέσεις επιλεγμένων κρυπτοπινάκων (IND-CCA2). Συνήθως στην κρυπτογραφία η έννοια της ελαχιστοποίησης δεν θεωρείται ως «πλεονέκτημα», αλλά υπό ορισμένες συνθήκες, όπως η ασφαλής ηλεκτρονική ψηφοφορία και τα κρυπτοσυστήματα κατωφλίου, η ιδιότητα αυτή μπορεί πράγματι να είναι απαραίτητη.

Ωστόσο, οι Paillier και Pointcheval συνέχισαν να προτείνουν ένα βελτιωμένο κρυπτοσύστημα τα οποία ενσωματώνουν το συνδυασμένο hashing του μηνύματος m με τυχαίο r. Παρόμοια με την πρόθεση του κρυπτοσυστήματος Cramer-Shoup [9], ο κατακερματισμός εμποδίζει έναν εισβολέα, δεδομένου μόνο του c, να είναι σε θέση να αλλάξει m με έναν ουσιαστικό τρόπο. Μέσω αυτής της προσαρμογής, το βελτιωμένο σχήμα μπορεί να αποδειχθεί ότι είναι IND-CCA2 [7] ασφαλές στο τυχαίο μοντέλο.

4.2.2 Εφαρμογές

4.2.2.1 Ηλεκτρονική ψηφοφορία

Η σημασιολογική ασφάλεια δεν είναι η μοναδική σκέψη. Υπάρχουν καταστάσεις κάτω από τις οποίες μπορεί να είναι επιθυμητή η ευκολία. Οι παραπάνω ομομορφικές ιδιότητες μπορούν να χρησιμοποιηθούν με ασφαλή ηλεκτρονικά συστήματα ψηφοφορίας. Εξετάστε μια απλή δυαδική (”υπερ” ή ”κατά”) ψήφο. Αφήστε τους ψηφοφόρους να ψηφίσουν είτε 1 (υπερ) είτε 0 (κατά). Κάθε ψηφοφόρος κρυπτογραφεί την επιλογή του πριν από την ψήφο του. Ο εκλογικός υπάλληλος παίρνει το προϊόν των m κρυπτογραφημένων ψήφων και στη συνέχεια αποκρυπτογραφεί το αποτέλεσμα και αποκτά την τιμή n, που είναι το άθροισμα όλων των ψήφων. Ο εκλογικός αξιωματούχος τότε γνωρίζει ότι n άνθρωποι ψήφισαν “υπερ” και m-n άνθρωποι ψήφισαν “κατά”. Ο ρόλος του τυχαίου r εξασφαλίζει ότι δύο ισοδύναμες ψήφους θα κρυπτογραφηθούν στην ίδια τιμή με αμελητέα πιθανότητα να ταιριάζουν, εξασφαλίζοντας έτσι την προστασία της ιδιωτικότητας των ψηφοφόρων.

4.2.2.2 Ηλεκτρονικά μετρητά

Ένα άλλο χαρακτηριστικό είναι η έννοια του αυτόαμφισβήτησης. Αυτή είναι η δυνατότητα αλλαγής ενός κρυπτοκειμένου σε άλλο χωρίς να αλλάζει το περιεχόμενο της αποκρυπτογράφησης του. Αυτό έχει εφαρμογή στην εξέλιξη του ecash, μια προσπάθεια που πρωτοανέφεραι ο David Chaum [4]. Φανταστείτε να πληρώνετε για ένα προιόν στο διαδίκτυο χωρίς ο πωλητής να χρειάζεται να γνωρίζει τον αριθμό της πιστωτικής σας κάρτας και, συνεπώς, την ταυτότητά σας. Ο στόχος τόσο στο ηλεκτρονικό χρήμα όσο και στην ηλεκτρονική ψηφοφορία είναι να εξασφαλιστεί ότι το ηλεκτρονικό χρήμα (όπως επίσης και η ηλεκτρονική ψηφοφορία) είναι έγκυρο, χωρίς ταυτόχρονα να αποκαλύπτεται η ταυτότητα του ατόμου με τον οποίο συνεργάζεται αυτή τη στιγμή.

5. ΑΝΑΛΥΣΗ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ

5.1 Αρχιτεκτονική

Η προτεινόμενη πλατφόρμα δίνει την δυνατότητα αυθεντικοποίησης ενός ατόμου με βάση τα βιομετρικά του χαρακτηριστικά και στην προκειμένη περίπτωση με βάση το πρόσωπο του. Συγκεκριμένα ο κάθε χρήστης μπορεί να συνδεθεί σε όποια ηλεκτρονική ιστοσελίδα επιθυμεί, εφόσον χρησιμοποιεί την πλατφόρμα, με ένα απλό όνομα χρήστη και βγάζοντας μια φωτογραφία το πρόσωπο του. Εν συνεχεία, γίνονται όλες οι διαδικασίες που χρειάζονται, ανάλυση των βιομετρικών στοιχείων του προσώπου, πάντα στην συσκευή του χρήστη και ακολουθεί μια κίνηση των δεδομένων μεταξύ αυτής της τριπλέτας(χρήστης, ιστοσελίδα και πλατφόρμα), προϋποθέτοντας πως όλα τα δεδομένα όταν εξέλθουν από τον χρήστη κωδικοποιούνται.

Καθένα από τα κομμάτια όλης της υλοποίησης(χρήστης, ιστοσελίδα, πλατφόρμα) ακολουθεί μια συγκεκριμένη διαδικασία, αναλύει, συγκρίνει, στέλνει και κρυπτογραφεί-αποκρυπτογραφεί δεδομένα. Όλα τα κομμάτια της υλοποίησης επικοινωνούν μεταξύ τους στέλνοντας διάφορες πληροφορίες κάθε φορά, ανάλογα με την διεργασία που χρειάζεται να εκτελέσουν. Ο ενδιάμεσος και βασικότερος σταθμός της υλοποίησης είναι η πλατφόρμα, με αυτήν επικοινωνούν όλοι, από εκεί αντλούν όλα τα δεδομένα και τις πληροφορίες που χρειάζονται, καθώς εκεί βρίσκονται και όλα τα βιομετρικά δεδομένα των χρηστών ,κωδικοποιημένα χωρίς η πλατφόρμα να γνωρίζει κανένα στοιχείο από τα βιομετρικά δεδομένα του χρήστη.

Η κρυπτογράφηση των δεδομένων είναι το βασικότερο κομμάτι αυτού του project. Όλη η διανομή των ευαίσθητων και προσωπικών δεδομένων που γίνεται κατά την διάρκεια της διαδικασίας είναι ασφαλή με τα δεδομένα να είναι κρυπτογραφημένα και χωρίς κανέναν από τους ενδιάμεσους κόμβους, πέραν από τον ίδιο τον χρήστη, να γνωρίζει την παραμικρή πληροφορία για τα βιομετρικά δεδομένα. Και εφόσον η διαδικασία ολοκληρωθεί, η μόνη αποκρυπτογράφηση που μπορεί να γίνει σε όλη την υλοποίηση είναι από την μεριά της ιστοσελίδας με το ιδιωτικό κλειδί που μόνο αυτή κατέχει. Εκεί γίνεται η αποκρυπτογράφηση ενός κεμένου και όχι των βιομετρικών δεδομένων, που με αυτό το κείμενο η ιστοσελίδα αποφασίζει εάν ταιριάζουν τα δεδομένα που συγκρίνονται.

Η υλοποίηση χωρίς σε δύο μέρη, η εγγραφή του χρήστη και η αυθεντικοποίηση αυτού, όπου τα δύο αυτά μέρη ακολουθούν μια διαφορετική διαδικασία.

5.2 Διαδικασία κατά την εγγραφή

5.2.1 Χρήστης

- Μπαίνει στην ιστοσελίδα για να κάνει εγγραφή πληκτρολογώντας το όνομα χρήστη του. Κατόπιν πατάει το κουμπί εγγραφή που υπάρχει κάτω από την φόρμα συμπλήρωσης του ονόματος χρήστη.

- Αναζητεί συνεχώς στην βάση δεδομένων, και συγκεκριμένα στον πίνακα που καταγράφονται όλες οι ενεργές αιτήσεις των χρηστών, εάν υπάρχει εγγραφή γι αυτόν τον χρήστη, δίνοντας το όνομα χρήστη του. Εφόσον υπάρξει εγγραφή που να ταιριάζει με τα στοιχεία του,τότε η πλατφόρμα στέλνει πίσω το δημόσιο κλειδί, το id της ιστοσελίδας που έχει αιτηθεί να εγγραφεί ο χρήστης και το είδος της διαδικασίας που θέλει να ακολουθήσει(εγγραφή ή αυθεντικοποίηση) ώστε να γνωρίζει ο χρήστης για να κάνει τις ανάλογες πράξεις αργότερα.

- Φωτογραφίζει του προσώπου του χρήστη, αναλύει την φωτογραφία, υπολογίζοντας ένα διάνυσμα. Στην συνέχεια κρυπτογραφεί τα δεδομένα αυτά.

- Στέλνει τα δεδομένα αυτά στην βάση δεδομένων σε συνδυασμό με το όνομα χρήστη του και το id της ιστοσελίδας.

5.2.2 Ιστοσελίδα

Η ιστοσελίδα στην φάση της εγγραφής ακολουθεί μια διαδικασία:

- Όταν ο χρήστης εκτελέσει την πρώτη **(1)** διαδικασία, όπως βλέπουμε παραπάνω, η ιστοσελίδα επικοινωνεί με την πλατφόρμα στέλνοντας το όνομα χρήστη, το id της και το είδος της διαδικασίας που θέλει να ακολουθήσει ο χρήστης. Κατόπιν αυτά τα δεδομένα καταχωρούνται στην βάση δεδομένων σε έναν πίνακα που καταγράφει όλες τις αιτήσεις που είναι ενεργές για τους χρήστες.

5.2.3 Πλατφόρμα – Βάση δεδομένων

Η πλατφόρμα δέχεται όλες τις αιτήσεις από την ιστοσελίδα και από τον χρήστη, είναι πάντα ο ενδιάμεσος σταθμός σε όλη την υλοποίηση. Δεν υπάρχει αμφίδρομη επικοινωνία μεταξύ χρήστη και ιστοσελίδας. Άρα σε κάθε ερώτηση που γίνεται στην πλατφόρμα, η ίδια στέλνει πίσω μια απάντηση, είτε είναι δεδομένα είτε είναι κάποιο μήνυμα που χρειάζεται να αποστείλουμε στον απέναντι κόμβο. Έτσι στην συγκεκριμένη περίπτωση η πλατφόρμα ακολουθεί τις τρεις διαδικασίες:

- Όταν η ιστοσελίδα εκτελέσει την πρώτη **(1)** διαδικασία της, όπως βλέπουμε παραπάνω, η ιστοσελίδα απαντάει με ένα μήνυμα πως όλα έγιναν σωστά και η καταγραφή ολοκληρώθηκε.

- Όταν ο χρήστης εκτελέσει την δεύτερη**(2)** διαδικασία του, εφόσον βρεθεί εγγραφή που να ταιριάζει με τις πληροφορίες του χρήστη, τότε απαντάει με το δημόσιο κλειδί, το id της εκάστοτε ιστοσελίδας και το είδος της διαδικασίας που ακολουθείτε.

- Όταν ο χρήστης εκτελέσει την τέταρτη**(4)** διαδικασία του τότε η πλατφόρμα θα απαντήσει με ένα μήνυμα ότι όλα εκτελέστηκαν σωστά και η αποθήκευση των κρυπτογραφημένων βιομετρικών δεδομένων του χρήστη έγινε με επιτυχία.

5.2.4 Εκτέλεση όλου του κύκλου της υλοποίησης στην φάση της εγγραφής

Βήμα-βήμα όλη η διαδικασία που ακολουθείτε από την αρχή μέχρι το τέλος και όλα τα βήματα της υλοποίησης που εκτελούνται.

- Ο χρήστης εισέρχεται στην ιστοσελίδα που θέλει να συνδεθεί και πληκτρολογεί το όνομα χρήστη του, στην συνέχεια πατάει το κουμπί που λέει εγγραφή.

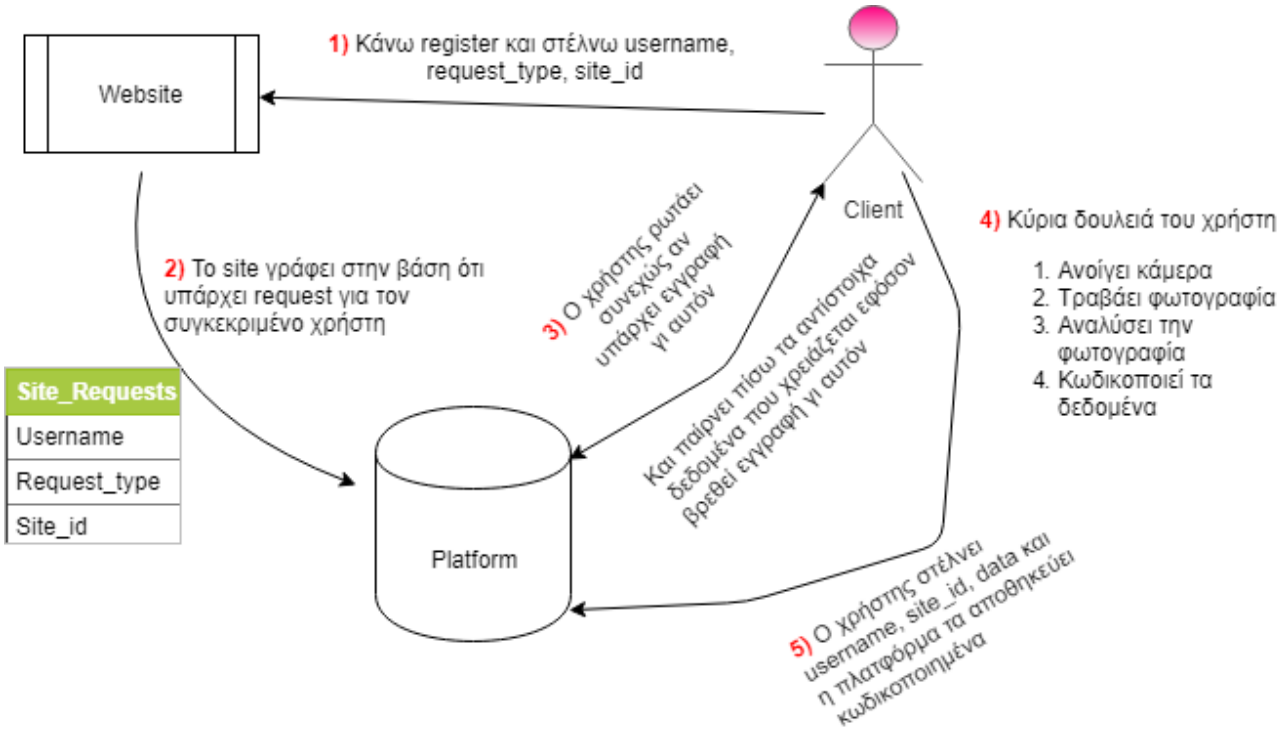
- Σε αυτό το σημείο η ιστοσελίδα δημιουργεί στην βάση δεδομένων, και στο πίνακα που είναι υπεύθυνος για την καταγραφή των αιτήσεων της κάθε ιστοσελίδας, μια εγγραφή που έχει τρεις μεταβλητές, όνομα χρήστη, id της εκάστοτε ιστοσελίδας και το είδος της ενέργειας που εκτελείται(εγγραφή ή αυθεντικοποίηση).

- Από την στιγμή που ο χρήστης εισέλθει στην ιστοσελίδα και εκτελεστούν τα παραπάνω βήματα, ρωτάει συνεχώς εάν υπάρχει εγγραφή γι αυτόν, ψάχνοντας στον πίνακα που έχει καταγεγραμμένες τις αιτήσεις κάθε χρήστη. Εφόσον βρεθεί εγγραφή

που να ταιριάζει με τις πληροφορίες που δίνει ο χρήστης, δηλαδή το συνδυασμό ονόματος χρήστης και id της ιστοσελίδας, τότε η πλατφόρμα επιστρέφει πίσω τα δεδομένα που χρειάζεται ο χρήστης για να συνεχίσει την διαδικασία, δηλαδή δημόσιο κλειδί, id ιστοσελίδας και είδος της ενέργειας που εκτελείται.

- Στην συνέχεια από την πλευρά του χρήστη ανοίγει η κάμερα, τραβάει φωτογραφία του προσώπου του, αναλύει την φωτογραφία βγάζοντας το διάνυσμα και κρυπτογραφεί τα δεδομένα που χρειάζεται να στείλει πίσω στην βάση δεδομένων για να αποθηκευτούν.

- Η τελευταία διαδικασία που ακολουθεί είναι όταν ο χρήστης στέλνει τα κρυπτογραφημένα δεδομένα στην βάση δεδομένων και εκεί αποθηκεύονται στέλνοντας πίσω ένα μήνυμα πως όλα εκτελέστηκαν σωστά και η εγγραφή ολοκληρώθηκε με επιτυχία.



Σχήμα 5.1: Σχεδιάγραμμα της υλοποίησης κατά την εγγραφή

5.3 Διαδικασία κατά την αυθεντικοποίηση

5.3.1 Χρήστης

Ο χρήστης κατά της αυθεντικοποίηση:

- Μπαίνει στην ιστοσελίδα για να κάνει εγγραφή πληκτρολογώντας το όνομα χρήστη του. Κατόπιν πατάει το κουμπί αυθεντικοποίηση που υπάρχει κάτω από την φόρμα συμπλήρωσης του ονόματος χρήστη.

- Ρωτάει συνεχώς την βάση δεδομένων, και συγκεκριμένα τον πίνακα που καταγράφονται όλες οι ενεργές αιτήσεις των χρηστών μας, εάν υπάρχει εγγραφή γι αυτόν τον χρήστη, δίνοντας το όνομα χρήστη του. Εφόσον υπάρχει εγγραφή για τον χρήστη στον πίνακα με τις αιτήσεις, η πλατφόρμα επιστρέφει πίσω το όνομα χρήστη, το δημόσιο κλειδί, το είδος της ενέργειας που εφαρμόστηκε(εγγραφή ή αυθεντικοποίηση), το άθροισμα των τετραγώνων αθροισμένο με την τυχαία τιμή r και το τελικό διάνυσμα με τις 13 μεταβλητές.

- Παίρνει την φωτογραφία του προσώπου του χρήστη και κάνει την ανάλυση αυτής, έπειτα προχωράει στην σύγκριση των δύο φωτογραφιών βγάζοντας τελικά την τελική απόσταση των δύο διανυσμάτων των φωτογραφιών με την τυχαία τιμή r μέσα σε αυτό.

- Ο χρήστης στέλνει στην βάση δεδομένων, και γράφει στον πίνακα FinalRes το όνομα χρήστη, το id της εκάστοτε σελίδας, την ώρα που έγινε αυτή η ενέργεια και την τελική απόσταση, έχοντας όμως αφαιρέσει η πλατφόρμα τον τυχαίο αριθμό r από αυτή.

5.3.2 Ιστοσελίδα

Η ιστοσελίδα στην φάση της εγγραφής ακολουθεί τρεις διαδικασία:

- Όταν ο χρήστης εκτελέσει την πρώτη**(1)** διαδικασία του, όπως βλέπουμε παραπάνω, η ιστοσελίδα επικοινωνεί με την πλατφόρμα στέλνοντας το όνομα χρήστη, το id της και το είδος της διαδικασίας που θέλει να ακολουθήσει ο χρήστης. Κατόπιν αυτά τα δεδομένα καταχωρούνται στην βάση δεδομένων σε έναν πίνακα που καταγράφει όλες τις αιτήσεις που είναι ενεργές για τους χρήστες.

- Η ιστοσελίδα ρωτάει συνεχώς την πλατφόρμα εάν υπάρχει εγγραφή στέλνοντας το συνδυασμό ονόματος χρήστη και το id της σελίδας, εφόσον βρεθεί εγγραφή με τα αντίστοιχα δεδομένα στον πίνακα FinalRes τότε η πλατφόρμα θα στείλει πίσω το όνομα χρήστη, το id της ιστοσελίδας, την χρονική στιγμή που καταχωρήθηκε και την τελική απόσταση κρυπτογραφημένη.

- Η ιστοσελίδα μόλις λάβει τα δεδομένα, αποκρυπτογραφεί την τελική απόσταση, κάνει τον έλεγχο της απόστασης με το όριο που έχει υπολογιστεί ως το κατάλληλο για την αυθεντικοποίηση και αποδέχεται ή όχι τον χρήστη που προσπαθεί να αυθεντικοποιηθεί.

5.3.3 Πλατφόρμα – Βάση δεδομένων

Η πλατφόρμα δέχεται όλες τις αιτήσεις από την ιστοσελίδα και από τον χρήστη και σε αυτή την περίπτωση, είναι πάντα ο ενδιάμεσος σταθμός σε όλη την υλοποίηση. Δεν υπάρχει αμφίδρομη επικοινωνία μεταξύ χρήστη και ιστοσελίδας ούτε στην λειτουργία της αυθεντικοποίησης. Άρα σε κάθε ερώτηση που γίνεται σε αυτή, η ίδια στέλνει πίσω μια απάντηση, είτε είναι δεδομένα είτε είναι κάποιο μήνυμα που θέλει να περάσει στον απέναντι κόμβο. Έτσι στην συγκεκριμένη περίπτωση η πλατφόρμα ακολουθεί τις τέσσερις διαδικασίες:

- Όταν η ιστοσελίδα εκτελέσει την πρώτη**(1)** διαδικασία της, όπως βλέπουμε παραπάνω, η ιστοσελίδα απαντάει με ένα μήνυμα πως όλα έγιναν σωστά και η καταγραφή ολοκληρώθηκε.

- Όταν ο χρήστης εκτελέσει την δεύτερη**(2)** διαδικασία του, εφόσον βρεθεί εγγραφή που να ταιριάζει με τις πληροφορίες του χρήστη, τότε απαντάει με το όνομα χρήστη, το δημόσιο κλειδί, το είδος της διαδικασίας που ακολουθεί, το άθροισμα των τετραγώνων του διανύσματος της εικόνας του χρήστη που είναι αποθηκευμένη, αθροισμένη με την τυχαία τιμή r και το διάνυσμα της εικόνας με τις δεκατρείς μεταβλητές.

- Όταν ο χρήστης εκτελέσει την τέταρτη**(4)** διαδικασία του, τότε η πλατφόρμα θα απαντήσει με ένα μήνυμα ότι όλα εκτελέστηκαν σωστά και η καταχώρηση της τελικής απόστασης των δύο φωτογραφιών(αποθηκευμένης και τρέχουσας φωτογραφίας) έγινε με επιτυχία.

- Όταν η ιστοσελίδα εκτελέσει την δεύτερη**(2)** διαδικασία της,εφόσον βρεθεί εγγραφή που να ταιριάζει με τον συνδυασμό των πληροφοριών του χρήστη και της ιστοσελίδας στον πίνακα FinalRes, τότε απαντάει στέλνοντας το όνομα χρήστη, το id της σελίδας, την χρονική στιγμή που έγινε η καταγραφή και την τελική απόσταση των δύο φωτογραφιών χωρίς την τυχαία τιμή r που την έχει αφαιρέσει η ίδια η πλατφόρμα.

5.3.4 Εκτέλεση όλου του κύκλου της υλοποίησης μας στην φάση της αυθεντικοποίησης

Βήμα-βήμα όλη η διαδικασία που ακολουθείτε από την αρχή μέχρι το τέλος και η εκτέλεση όλων των βημάτων της υλοποίησης.

- Ο χρήστης εισέρχεται στην ιστοσελίδα και πληκτρολογεί το όνομα χρήστη του και στην συνέχεια πατάει το κουμπί που λέει αυθεντικοποίηση.

- Σε αυτό το σημείο η ιστοσελίδα δημιουργεί στην βάση δεδομένων, και στο πίνακα που είναι υπεύθυνος για την καταγραφή των αιτήσεων της κάθε ιστοσελίδας, μια εγγραφή που έχει τρεις μεταβλητές, όνομα χρήστη, id της εκάστοτε ιστοσελίδας και το είδος της ενέργειας που εκτελείται(εγγραφή ή αυθεντικοποίηση).

- Από την στιγμή που ο χρήστης εισέλθει στην ιστοσελίδα και εκτελεστούν τα παραπάνω βήματα, ρωτάει συνεχώς εάν υπάρχει εγγραφή γι αυτόν, ψάχνοντας στον πίνακα που έχει καταγεγραμμένες τις αιτήσεις κάθε χρήστη. Εφόσον βρεθεί εγγραφή που να ταιριάζει με τις πληροφορίες που δίνει ο χρήστης, δηλαδή το συνδυασμό ονόματος χρήστης και id της ιστοσελίδας, τότε η πλατφόρμα επιστρέφει πίσω τα δεδομένα που χρειάζεται ο χρήστης για να συνεχίσει την διαδικασία, που είναι αυτή την φορά το όνομα χρήστη, το δημόσιο κλειδί, το είδος της ενέργειας που ακολουθείτε, το άθροισμα των τετραγώνων του διανύσματος της εικόνας του χρήστη που είναι αποθηκευμένη αθροισμένη με την τυχαία τιμή r και το διάνυσμα της εικόνας με τις δεκατρείς μεταβλητές.

- Στην συνέχεια η εφαρμογή από την μεριά του χρήστη ανοίγει την κάμερα, τραβάει την φωτογραφία του προσώπου του, αναλύει την φωτογραφία βγάζοντας το διάνυσμα, κάνει την σύγκριση των δύο διανυσμάτων(του αποθηκευμένου που παίρνει από την βάση δεδομένων και αυτού που αναλύει εκείνη την στιγμή) και από αυτό βγάζει την τελική απόσταση των φωτογραφιών αθροισμένη με την τυχαία τιμή r.

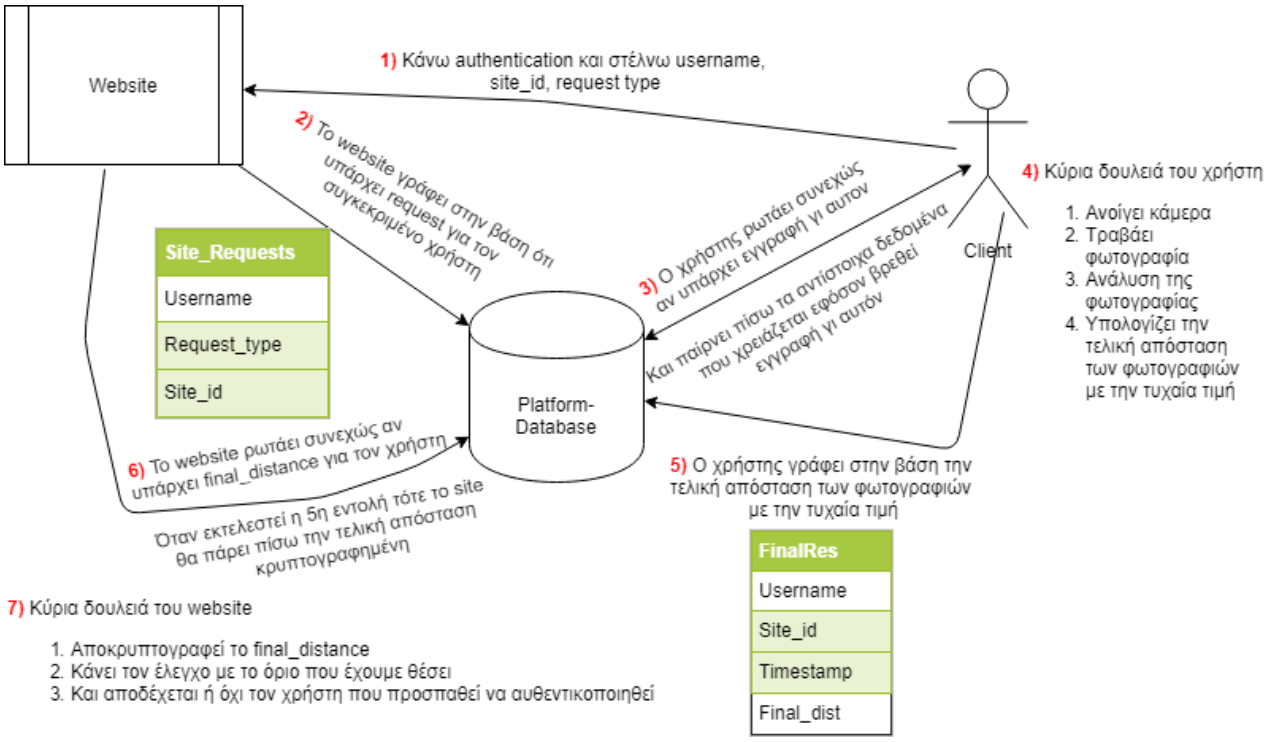
- Ο χρήστης στέλνει την τελική απόσταση αθροισμένη με τη τυχαία τιμή r κωδικοποιημένη, καταγράφοντας την τελική αυτή απόσταση στον πίνακα FinalDist το όνομα χρήστη, το id της εκάστοτε ιστοσελίδας, την χρονική στιγμή που γίνεται η εγγραφή καθώς και την τελική απόσταση.
- Όταν ξεκινήσει όλη η διαδικασία, η ιστοσελίδα κατ' επανάληψη ρωτάει συνεχώς την πλατφόρμα εάν υπάρχει εγγραφή στον πίνακα FinalDist με τον συνδυασμό των στοιχείων, όνομα χρήστη και id της εκάστοτε σελίδας. Εφόσον εκτελεστεί η τελευταία διαδικασία παραπάνω, αυτό σημαίνει πως η ερώτηση αυτή που κάνει η ιστοσελίδα θα πάρει απάντηση πως υπάρχει εγγραφή για τον χρήστη που ρωτάει και έτσι θα της επιστρέψει πίσω τα δεδομένα αυτά που χρειάζεται, όνομα χρήστη, το id της εκάστοτε σελίδας, την χρονική στιγμή που καταγράφηκε η εγγραφή και την τελική απόσταση χωρίς την τυχαία τιμή r αυτή την φορά επειδή η πλατφόρμα το έχει αφαιρέσει.
- Στην τελική φάση η ιστοσελίδα αφού έχει πάρει τα δεδομένα που χρειάζεται, αποκρυπτογραφεί την τελική απόσταση με το ιδιωτικό κλειδί, συγκρίνει την απόσταση με το όριο που έχει υπολογιστεί και αποφασίζει εάν ταιριάζουν οι δύο φωτογραφίες ή όχι για να γίνει η αυθεντικοποίηση του χρήστη και κατ' επέκταση η σύνδεση του στην ιστοσελίδα.

5.4 Τεχνικά χαρακτηριστικά

Η πλατφόρμα που υλοποιήθηκε είναι ένα **RESTful API** που επικοινωνεί με τους άλλους κόμβους μέσω της **Flask** βιβλιοθήκης, είναι πάντα ο ενδιάμεσος σταθμός σε όλες τις διαδικασίες, αποθηκεύει τα δεδομένα, επεξεργάζεται τα δεδομένα και τα αποστέλει σε όποιον από τους κόμβους τα χρειάζεται και έχει την δικαιοδοσία να διαβάσει τα δεδομένα αυτά. Για την αναγνώρησει του προσώπου έχει χρησιμοποιηθεί η βιβλιοθήκη **OpenCV** και για την κρυπτογράφηση των δεδομένων έχει χρησιμοποιηθεί κρυπτοσύστημα **Paillier** με ομομορφική κρυπτογράφηση όπως αναφέρθηκε παραπάνω. Αυτά είναι τα τέσσερα βασικά χαρακτηριστικά της πλατφόρμας.

5.4.1 RESTful API

RESTful API είναι μια εφαρμογή που χρησιμοποιεί τα αιτήματα HTTP για την διαχείρηση δεδομένων. Αναφέρεται ως web υπηρεσία, είναι ένα αρχιτεκτονικό στυλ που έχει



Σχήμα 5.2: Σχεδιάγραμμα της υλοποίησης κατά την αυθεντικοποίηση

προσέγγισει στις επικοινωνίες κυρίως στην ανάπτυξη web υπηρεσιών.

5.4.2 Flask

Το Flask είναι ένα micro περιβάλλον για την ανάπτυξη διαδικτυακών εφαρμογών με βάση τη γλώσσα Python. Micro σημαίνει ότι περιλαμβάνει τις βασικές λειτουργικότητες και αφήνει πιο σύνθετες λειτουργίες όπως η αυθεντικοποίηση σε πρόσθετα (extensions), σε αντίθεση με πιο σύνθετα περιβάλλοντα όπως το Django που διαθέτουν ένα ολοκληρωμένο σύνολο λειτουργιών χωρίς να απαιτούνται πρόσθετα.

5.4.3 OpenCV

Η OpenCV είναι μία ελεύθερη διαθέσιμη, ανοικτού κώδικα βιβλιοθήκη, που αφορά την επεξεργασία εικόνας και την μηχανική εκμάθηση.

Ακόμα χρησιμοποιήθηκε η βιβλιοθήκη **dlib** που είναι υπεύθυνη για την μηχανική μάθηση, μέσω της αναγνώρισεις του προσώπου σε αυτή την υλοποίηση.

5.5 Υπολογισμοί και μαθηματικές σχέσεις

Για την σύγκριση των δύο φωτογραφιών χρησιμοποιήθηκε **Ευκλείδια Απόσταση**.

- **Κατά την αυθεντικοποίηση:**

  Έστω $E(y_1^2+y_2^2+r), E(y_1), E(y_2)$ τα δεδομένα που παίρνει από την βάση δεδομένων ο χρήστης και $x = [x_1, x_2]$ το διάνυσμα που υπολογίζει ο χρήστης την στιγμή της αυθεντικοποίησης, τότε η απόσταση τους υπολογίζεται ως εξής:

  $$(D + r) = E(y_1^2 + y_2^2 + r) + E(2 * x_1 * y_1) + E(2 * x_2 * y_2) + E(x_1^2) + E(x_2^2)$$

  Η απόσταση αυτή περιέχει και την τυχαία τιμή r. Η πλατφόρμα δημιουργεί αυτή την τυχαία τιμή, την προσθέτει στο κρυπτογραφημένο άθροισμα τετραγώνων $(E(y_1^2+y_2^2+r))$ που έχει αποθηκευμένο στην βάση(με την δυνατότητα που μας δίνει η ομομορφική κρυπτογράφηση) και την στέλνει στον χρήστη όταν την χρειαστεί για να γίνει η σύγκριση των φωτογραφιών. Καθώς η πλατφόρμα παραλάβει την τελική απόσταση μετά την σύγκριση που έκανε ο χρήστης, αφαιρεί την τυχαία τιμή r

  - Υπολογίζοντας
    * Τον αντίστροφο της r με την συνάρτηση **invmod**
    * Και προσθέτοντας τον στην απόσταση

  Και τελικά γίνεται η αποθήκευση την απόστασης χωρίς την τυχαία τιμή.

- **Κατά την εγγραφή**

  Ο χρήστης εφόσον κάνει την ανάλυση της εικόνας, αποστέλλει στην πλατφόρμα τα εξής δεδομένα. Έστω από την ανάλυση έχουμε πάρει το διάνυσμα $x = [x_1, x_2]$:

  - $E(x_1^2 + x_2^2)$, (Άθροισμα τετραγώνων)
  - $E(x_1)$,
  - $E(x_2)$.

  Αυτές οι τιμές βγαίνουν από τον γενικό τύπο του Ευκλείδη, όπου έγιναν κάποιες τροποποιήσεις που χρειάστηκαν για να μπορούν να γίνουν αργότερα οι πράξεις μεταξύ των απλών κειμένων και κρυπτοκειμένων.

  ***Βέβαια οι εικόνες έχουν διανύσματα με 13 μεταβλητές, όπου ακολουθείτε οι ίδια διαδικασία απλά με περισσότερους υπολογισμούς.**

****Μπροστά στις μεταβλητές που χρησιμοποιούνται παραπάνω, Ε σημαίνει πως αναφερόμαστε σε κρυπτογραφημένα δεδομένα.**

6. ΥΛΟΠΟΙΗΣΗ

6.1 Από την μεριά της πλατφόρμας

Παρακάτω φαίνεται η χρήση της **Flask**, όταν ο χρήστης ρωτάει συνεχώς την πλατφόρμα εάν υπάρχει εγγραφή γι' αυτόν και αναλόγως με το είδος της εγγραφής που θέλει να κάνει ο χρήστης γυρίζει τα αντίστοιχα δεδομένα:

```
@app.route('/UserAsking/<username>/<site_id>', methods=['GET', 'POST'])
def user_asking(username, site_id):
    for i in site_requests:
        if (username + "_" + site_id == i):
            if (site_requests[i][3] == 0):
                return (sites[2], sites[0], site_requests[username+"_"+site_id][3])
            elif (site_requests[i][3] == 1):
                return (site_requests[i][1], sites[2], site_requests[i][3], request(username, site_id))
    return ("We dont have request for you")
```

Επεξήγηση του κώδικα: Ο χρήστης καλεί το URL που προβάλετε στην πρώτη γραμμή με τα αντίστοιχα δεδομένα που χρειάζεται και η πλατφόρμα με την συνάρτηση user.asking ελέγχει με προσπέλαση στον πίνακα site.requests αν υπάρχει εγγραφή για τον χρήστη με την συνθήκη **if** και με μια δεύτερη **if** ελέγχει το είδος της διαδικασίας που επέλεξε ο χρήστης ώστε να επιστρέψει τις αντίστοιχες τιμές και δεδομένα.

Παρακάτω προβάλετε το κομμάτι που η πλατφόρμα προσθέτει την τυχαία τιμή **r** στο άθροισμα των τετραγώνων και έτσι αποστέλει τα δεδομένα που χρειάζεται ο χρήστης κατά την αυθεντικοποίηση:

```
@app.route('/request/<username>/<site_id>', methods=['GET', 'POST'])
def request(username,site_id):
    for i in site_requests:
        if (i == username + '_' + site_id):
            r = random.randint(1,101)
            pub_key = sites[site_id][1]
            encr_r = encrypt(pub_key, r)
            athr_tetra_me_r = e_add(pub_key, data[username+"_"+site_id][2], encr_r)

            return (site_id, pub_key, site_requests[username+'_'+site_id][3], athr_tetra_me_r, data[username+"_"+site_id][3])
        else:
            return ('We dont have a request for you')
```

Επεξήγηση του κώδικα: Αυτή η συνάρτηση καλείται εφόσον ο χρήστης θέλει να κάνει αυθεντικοποίηση, έτσι στην ερώτηση που κάνει ο χρήστης στον πίνακα για να μάθει εάν υπάρχει εγγραφή γι αυτόν(σε αυτό το κομμάτι γίνεται αυτό ο έλεγχος):

```
elif (site_requests[i][3] == 1):
    return (site_requests[i][1], sites[2], site_requests[i][3], request(username, site_id))
```

Τότε καλείται αυτή η συνάρτηση για να γυρίσει πίσω τα δεδομένα που χρειάζεται ο χρήστης

για να κάνει την σύγκριση. Στην γραμμή 8 του κώδικα παίρνει το δημόσιο κλειδί καθώς και την τυχαία τιμή και κάνουμε την πρόσθεση του στο κρυπτογραφημένο άθροισμα.

Στην πλατφόρμα, υπάρχει και μια συνάρτηση που ελέγχει τις αιτήσεις στον πίνακα site.requests και εάν έχουν υπερβεί το χρονικό όριο των δύο λεπτών από την στιγμή που προσπάθησε ο χρήστης να κάνει κάποια ενέργεια, τότε διαγράφει αυτές τις εγγραφές:

```
def checking_requests(username, site_id):
    timestamp = str(datetime.datetime.now()).split('.')[0]

    if ((site_requests[username + '_' + site_id][2] - timestamp) >= 120):
         del site_requests["username + '_' + site_id"]

    return 0
```

Επεξήγηση κώδικα: Αυτό το κομμάτι εκτελείται κάθε ένα μικρό χρονικό διάστημα και καθαρίζει τον πίνακα των αιτήσεων εάν υπάρχουν παλιές εγγραφές σε αυτόν. Στην συνθήκη if παίρνει την διαφορά από την χρονική στιγμή που είναι αποθηκευμένη στην βάση δεδομένων και εκείνη την χρονική στιγμή που εκτελείται αυτό το κομμάτι κώδικα, εάν η διαφορά αυτή είναι μεγαλύτερη από δύο λεπτά τότε πηγαίνει και διαγράφει την συγκεκριμένη εγγραφή.

6.2 Από την μεριά του χρήστη

Με την συγκεκριμένη συνάρτηση γίνεται η αναγνώριση του προσώπου χρησιμοποιώντας την βιβλιοθήκη της OpenCV:

```
def detect_faces(image):
    #print("Detecting faces.......")
    cascPath = r'C:\Users\qkiri\PycharmProjects\Thesis\haarcascade_frontalface_default.xml'

    faceCascade = cv2.CascadeClassifier(cascPath)
    #gray = cv2.imread(image, 0)
    faces = faceCascade.detectMultiScale(
        image,
        scaleFactor=1.3,
        minNeighbors=5,
        minSize=(30,30),
        flags=cv2.CASCADE_SCALE_IMAGE
    )

    print("Found {0} faces!".format(len(faces)))

    for (x, y, w, h) in faces:
        cv2.rectangle(image, (x, y), (x+w, y+h), (0, 255, 0), 2)

    #cv2.imshow("Faces found", image)
    #cv2.waitKey(0)
    return faces
```

Επεξήγηση κώδικα: Εδώ ο κώδικας αναγνωρίζει τα πρόσωπα μέσα στην φωτογραφία, με την βοήθεια του αρχείου **"haarcascade.frontalface.default.xml"** που υποδικνύει τις θέσεις των βασικών σημείων του προσώπου ώστε να προσαρμοστεί ο κώδικας για να κάνει την ανάλυση και να βγάλει τα σημαντικότερα σημεία του προσώπου.

Εδώ βλέπουμε τον κώδικα που αναλύει την εικόνα και βγάζει το τελικό διάνυσμα S:

```
def calculate_S(evectors , mean_img_col):
    i = 1
    #images_S = []
    print('calculate S for Picture Number {}'.format(i))
    #path_to_img = 'C:\Users\qkiri\PycharmProjects\PictureInisialization\\burst_0.jpg'
    path_to_img = r'C:\Users\qkiri\PycharmProjects\Thesis\\burst_0.jpg'
    img = cv2.imread(path_to_img, 0)
    faces = detect_faces(img)
    cropped_image = crop_image(faces, path_to_img)
    resized_img = resize_image(cropped_image)
    images_S = picture_analysis(evectors, mean_img_col, resized_img)
    return (images_S)
```

Επεξήγηση κώδικα: Η φωτογραφία που έχει βγει και έχει αποθηκευτεί στο συγκεκριμένο μονοπάτι περνάει μέσα από όλες τις συναρτήσει ώστε να γίνει ασπρόμαυρή, να αναγνωρίσει το πρόσωπο, να κόψει την υπόλοιπη φωτογραφία και να κρατήσει μόνο το χρήσιμο κομμάτι που είναι το πρόσωπο, να κάνω αναπροσαρμογή της φωτογραφίας στις διαστάσεις που θέλει για να την επεξεργαστεί και τελικά να βγάλει το S. Έτσι φτάνει και στην διαδικασία της σύγκρισης όπου γίνεται με την σύγκριση των δύο διανυσμάτων βγάζοντας την **Ευκλείδεια απόσταση** τους:

```
def euclidean_distance(image1_S, image2_S):
    print('AND THE SCORE BETWEEN THE IMAGES IS...')
    #print(image1_S[0], image2_S[0])
    #print(type(image1_S[0]), type(image2_S[0]))
    sum = 0
    for i in range(0, 13):
        sq = (float(image1_S[i]) - float(image2_S[i]))**2
        sum = sum + sq

    sum = math.pow(sum, 1.0/2)
    #print(sum)
    return sum
```

Το κύριο κομμάτι κώδικα του χρήστη είναι αυτό που ο χρήστης ρωτάει συνέχεια αν υπάρχει εγγραφή γι αυτόν στον πίνακα και αναλόγως με την απάντηση που παίρνει, αν είναι εγγραφή ή αυθεντικοποίηση, εκτελεί και τις αντίστοιχες εντολές:

```
url_ask = "http://192.168.1.125:5010/UserAsking/" + username + "/" + site_id
apantisi_gia_eggrafi = requests.get(url_ask)
print (apantisi_gia_eggrafi)
if (apantisi_gia_eggrafi[2] == 0):
      flag = 1
      show_webcam(1)
      current_image_S = calculate_S(evectors, mean_img_col)
      apostoli_stoixeiwn = registration(username, site_id, pub_key, current_image_S)
elif (apantisi_gia_eggrafi[2] == 1):
      flag = 1
      show_webcam(1)
      current_image_S = calculate_S(evectors,mean_img_col)
      athr_tetra_me_r = url_ask[3][3]
      saved_images_S = url_ask[3][4]
      apostoli_apostasis_me_r = authentication(username, site_id, pub_key, current_image_S, athr_tetra_me_r, saved_images_S)
else:
      print ("Den exw eggrafi gia sena")
```

Επεξήγηση κώδικα:

- Όταν ο χρήστης πάρει απάντηση πως έχει κάνει αίτηση για εγγραφή τότε τραβάει την φωτογραφία στην εντολή 6, υπολογίζει το S και τελικά καλέι την συνάρτηση registration:

```
def registration(username,site_id, pub,current_image_S):        #prepei na tin ftiaxw
    encrypted_y = {}
    athroisma_tetragwnwn_y = 0
    for i in range(0, 12):
        tetragwno = current_image_S[i] * current_image_S[i]
        athroisma_tetragwnwn_y = athroisma_tetragwnwn_y + tetragwno


    encrypted_athr = encrypt(pub, athroisma_tetragwnwn_y)
    for i in range(0, 12):
        encrypted_y[i] = encrypt(pub, current_image_S[i])

    #encrypted_y1 = encrypt(pub, current_image_S[0])
    #encrypted_y2 = encrypt(pub, current_image_S[1])

    url = "http://192.168.1.125:5010/register/" + username + "/" + site_id + "/" + encrypted_athr + "/" + encrypted_y
    r = requests.get(url)
    print (r)
```

Εδώ υπολογίζει το άθροισμα τετραγώνω και στέλνει στην βάση δεδομένων αυτό, καθώς και έναν πίνακα με τις 13 τιμές του S.

- Όταν ο χρήστης πάρει απάντηση πως έχει κάνει αίτηση για αυθεντικοποίηση τότε

τραβάει φωτογραφία, υπολογίζει το S και εφόσον έχει πάρει τα δεδομένα που χρειάζεται, άθροισμα τετραγώνων με την τυχαία τιμή και την αποθηκευμένη φωτογραφία, καλεί την συνάρτηση authentication:

```
def authentication(username, site_id, pub, current_S, athroisma_tetragwnwn_y_me_r, encrypted_y):
      ginomeno_x_y = {}
      for i ir range(0, 12):
            ginomeno_x_y[i] = e_mul_const(pub, e_mul_const(pub, encrypted_y[3][i + 1], current_S[i]), 2)
      encrypted_x_tetragwno = {}
      for i ir range(0, 12):
            encrypted_x_tetragwno[i] = encrypt(pub, current_S[i]*current_S[i])
      sum = e_add(pub, athroisma_tetragwnwn_y_me_r, ginomeno_x_y[0])
      for i ir range(1, 12):
            sum = e_add(pub, sum, ginomeno_x_y[i])
      for j ir range(0, 12):
            sum = e_add(pub, sum, encrypted_x_tetragwno[j])
      apostasi_me_r = sum

      url = "http://192.168.1.125:5010/finalDist/" + "/" + username + "/" + site_id + "/" + apostasi_me_r
      r = requests.get(url)
      print (r)
```

Εδώ με τις τέσσερις επαναλήψεις ο κώδικας βρίσκει την τελική απόσταση, με τις πράξεις μεταξύ των τιμών των διανυσμάτων που κάνει, και τελικά στέλνει την τελική απόσταση στην βάση δεδομένων.

6.3 Από την μεριά της ιστοσελίδας

Παρακάτω η ιστοσελίδα ρωτάει συνεχώς τον χρήστη εάν υπάρχει κάποια εγγραφή στον πίνακα με τις τελικές αποστάσεις:

```
while(flag == 0):
    url_ask = 'http://192.168.1.125:5010/SiteCommun/' + username + '/' + site
    apantisiApoSiteCommun = requests.get(url_ask)
    if (apantisiApoSiteCommun.text != 'There is no record for you'):

        for i in sites[site]:
            if (str(type(i)) == "<class 'paillier.paillier.PrivateKey'>"):
                priv_key = i
        flag = 1



        distance = decrypt(priv_key, apantisiApoSiteCommun[3])
        if (distance <=2000 ):
            return 'You are in'
        else:
            return 'We cant authenticate you'
    time.sleep(5)
```

Επεξήγηση του κώδικα: Με την επανάληψη που χρησιμοποιεί, εφόσον βρεθεί εγγραφή στην συνθήκη **if** που έχει, τότε κατευθείαν παίρνει το δημόσιο κλειδί, αποκρυπτο-

γραφεί την τελική απόσταση για τον συγκεκριμένο χρήστη - ιστοσελίδα και τελικά ελέγχει αν είναι μέσα στο όριο που έχει οριστεί. Αυτή η επανάληψη εκτελείται κάθε 5 δευτερόλεπτα εφόσον δεν βρεθεί εγγραφή.

Μετά από διάφορες προσπάθειες και συγκρίσεις μεταξύ φωτογραφιών, στην φάση που η ιστοσελίδα λαμβάνει την τελική απόσταση και αυθεντικοποιεί τον χρήστη θετικά ή αρνητικά έχει τεθεί ένα **όριο**.

```
distance = decrypt(priv_key, apantisiApoSiteCommun[3])
if (distance <=2000 ):
    return 'You are in'
else:
    return 'We cant authenticate you'
```

Επεξήγηση του κώδικα: Εφόσον γίνει αποκρυπτογράφηση της απόστασης, ελέγχει με το όριο να είναι στο 2000 με την συνθήκη **if** και ο χρήστης εκτελεί την διαδικασία της αυθεντικοποίησης.

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερασματικά η υλοποίηση της πλατφόρμας, ικανοποίησε σε μεγάλο βαθμό τον αρχικό στόχο της έρευνας πάνω στην μελέτη για την δημιουργία πλατφόρμας με σκοπό την εφαρμογή της πάνω σε υπάρχοντες ιστοσελίδες για την αυθεντικοποίηση του ατόμου με βάση τα βιομετρικά του χαρακτηριστικά και συγκεκριμένα το πρόσωπο του.

Το συνεργατικό μοντέλο που υφίσταται, τριών οντοτήτων, χρήστη - πλατφόρμα - ιστοσελίδα, δείχνει να διατηρεί την ιδιωτικότητα των δεδομένων των χρηστών και να υπάρχει μια σωστή κατανομή για την διακίνηση των δεδομένων.

Η πλατφόρμα είναι ικανή να κάνει όλους τους υπολισγμούς που χρειάζεται μεταξύ των δεδομένων των χρηστών, χωρίς να μαθαίνει ποτέ το περιεχόμενο αυτών των πληροφοριών και είναι ικανή να μεταβιβάζει τα δεδομένα, από την μια πλευρά της υλοποίησης στην άλλη(από τον χρήστη στην ιστοσελίδα) κατά τον ίδιο τρόπο, καθώς τα δεδομένα αυτά είναι κρυπτογραφημένα.

Η μεθοδολογία που χρησιμοποίησαμε αν και χρήζει περαιτέρω βελτιώσεις, έχει τις βάσεις ώστε να γίνει ένα ολοκληρομένο σύστημα αυθεντικοποίησης το οποίο θα εφαρμόζεται σε ιστοσελίδες και θα αντικαθιστά τις συμβατικές μεθόδους αυθεντικοποίησης.

Έτσι, υλοποίηση και εκτέλεση του αλγορίθμου μας οδήγησαν στα εξής συμπεράσματα:

- Η ιδιωτικότητα των δεδομένων δεν παραβιάζεται καθ’ όλη την διάρκεια της διαδικασίας(εγγραφής ή αυθεντικοποίησης)
- Όλα τα δεδομένα διαχειρίζονται από την πλατφόρμα και έτσι δεν υπάρχει επικοινωνία μεταξύ χρήστη και ιστοσελίδας, ώστε να υπάρχει απόλυτος έλεγχος της κίνησης των δεδομένων
- Διευκόλυνση χρήστη κατά την είσοδο του σε ένα σύστημα
- Εξοικονόμηση χρόνου
- Αποφυγή λαθών
- Αύξηση της ασφάλειας

Όσον αφορά την μελλοντική έρευνα και ανάπτυξη πάνω στο ήδη υλοποιημένο μοντέλο, αυτή παρουσιάζει αρκετά ενδιαφέροντα σημεία.

Έτσι, θα ήταν πολύ χρήσιμη η υλοποίηση μιας Android εφαρμογής για την πλευρά του χρήστη, ώστε την στιγμή που θα χρειαζόταν ο χρήστης να εγγραφή ή να αυθεντικοποιηθεί να χρησιμοποιούσε την συσκευή του για να ακολουθήσει την διαδικασία. Αυτό θα διευκόλυνε τον χρήστη ώστε να μπορεί να συνδέεται με τον ίδιο τρόπο και από το smartphone του, αυτό δεν θα περιόριζε την πλατφόρμα για χρήση μόνο από έναν ηλεκτρονικό υπολογιστή.

Επίσης θα πρέπει να δημιουργηθεί και ο κώδικας που είναι υπεύθυνος για την επικοινωνία της ιστοσελίδας με την πλατφόρμα, γραμμένο σε HTML, μια απλή φόρμα συμπλήρωσης στοιχείων του χρήστη που θα καλεί κάποιες URL διευθύνσεις(**Flask**). Με αυτόν τον τρόπο θα γίνεται η ανταλλαγή των δεδομένων μεταξύ ιστοσελίδας και πλατφόρμας. Αυτός θα είναι ο κώδικας που θα εφαρμόζεται στην ιστοσελίδα ώστε αυτή να μπορεί να έχει τα προνόμια την υλοποίησης και να παρέχει στους χρήστες της την βιομετρική αυθεντικοποίηση με βάση το πρόσωπο.

Τέλος, αυτό που θα ολοκλήρωνε την παρούσα υλοποίηση δεν θα μπορούσε να είναι κάτι άλλο πέρα από την ανάπτυξη μιας ολοκληρωμένης πλατφόρμας βασισμένης στην προτεινόμενη μεθοδολογία και την εφαρμογή της σε πραγματικές ιστοσελίδες, ώστε να δοκιμαστεί ο τρόπος της αυθεντικοποίησης με πραγματικά δεδομένα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Joppe W Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In *IMA International Conference on Cryptography and Coding*, pages 45–64. Springer, 2013.

[2] Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure remote authentication using biometric data. In *annual international conference on the theory and applications of cryptographic techniques*, pages 147–163. Springer, 2005.

[3] Paul M Burger. Biometric authentication system, April 17 2001. US Patent 6,219,439.

[4] Jan Camenisch, Anna Lysyanskaya, and Mira Meyerovich. Endorsed e-cash. In *2007 IEEE Symposium on Security and Privacy (SP'07)*, pages 101–115. IEEE, 2007.

[5] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster packed homomorphic operations and efficient circuit bootstrapping for tfhe. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 377–408. Springer, 2017.

[6] Gu Chunsheng and Gu Jixing. Cryptanalysis of the smart-vercauteren and gentry-halevi's fully homomorphic encryption. *International Journal of Security and Its Applications*, 6(2):103–108, 2012.

[7] Angsuman Das and Avishek Adhikari. An efficient ind-cca2 secure paillier-based cryptosystem. *Information Processing Letters*, 112(22):885–888, 2012.

[8] Léo Ducas and Daniele Micciancio. Fhew: bootstrapping homomorphic encryption in less than a second. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 617–640. Springer, 2015.

[9] Marc Fischlin. The cramer-shoup strong-rsa signature scheme revisited. In *International Workshop on Public Key Cryptography*, pages 116–129. Springer, 2003.

[10] Craig Gentry and Dan Boneh. *A fully homomorphic encryption scheme*, volume 20. Stanford University Stanford, 2009.

[11] Craig Gentry et al. Fully homomorphic encryption using ideal lattices. In *Stoc*, volume 9, pages 169–178, 2009.

[12] Craig Gentry, Shai Halevi, and Nigel P Smart. Better bootstrapping in fully homomorphic encryption. In *International Workshop on Public Key Cryptography*, pages 1–16. Springer, 2012.

[13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Annual Cryptology Conference*, pages 75–92. Springer, 2013.

[14] James Irwin, Dan Page, and Nigel P Smart. Instruction stream mutation for non-deterministic processors. In *Proceedings IEEE International Conference on Application-Specific Systems, Architectures, and Processors*, pages 286–295. IEEE, 2002.

[15] Mike Ivanov. Mike ivanov. paillier. *https://github.com/mikeivanov/paillier*.

[16] Payal V Parmar, Shraddha B Padhar, Shafika N Patel, Niyatee I Bhatt, and Rutvij H Jhaveri. Survey of various homomorphic encryption algorithms and schemes. *International Journal of Computer Applications*, 91(8), 2014.

[17] Fabio Roli, Luca Didaci, and Gian Luca Marcialis. Adaptive biometric systems that can improve with use. In *Advances in Biometrics*, pages 447–471. Springer, 2008.

[18] Arun Ross and Anil K Jain. Multimodal biometrics: an overview. In *2004 12th European Signal Processing Conference*, pages 1221–1224. IEEE, 2004.

[19] Sai Sri Sathya, Praneeth Vepakomma, Ramesh Raskar, Ranjan Ramachandra, and Santanu Bhattacharya. A review of homomorphic encryption libraries for secure computation. *arXiv preprint arXiv:1812.02428*, 2018.

[20] P Thorsteinson and GGA Ganesh. Asymmetric cryptography. *.NET Security and Cryptography*, pages 99–125, 2003.

[21] Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 24–43. Springer, 2010.