Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΥΔΕ ΕΤΑΚ
ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020 ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ανάπτυξη Μεθοδολογιών και Ενσωματωμένων Λύσεων Ασφάλειας για Τεχνολογίες Internet of Things σε ηλεκτρονικές Υπηρεσίες Υγείας – ΜΕΛΙΤΥ (Τ1ΕΔΚ-01958)

Εργαλεία ελέγχου της ασφάλειας συστημάτων IoMT

ΕΝΟΤΗΤΑ ΕΡΓΑΣΙΑΣ ΕΡΓΟΥ:	**ΕΕ4**
ΚΩΔΙΚΟΣ ΠΑΡΑΔΟΤΕΟΥ:	**Π4.6**
ΕΚΔΟΣΗ:	**Τελική**
ΚΑΤΑΣΤΑΣΗ:	***Υποβληθείσα***
ΗΜΕΡΟΜΗΝΙΑ ΟΛΟΚΛΗΡΩΣΗΣ:	**30/11/2021**
ΥΠΕΥΘΥΝΟΣ ΦΟΡΕΑΣ:	**CENSUS**
ΣΥΜΜΕΤΕΧΟΝΤΕΣ ΦΟΡΕΙΣ	**Πανεπιστήμιο Πειραιά**

Πίνακας Περιεχόμενων

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

1 Εισαγωγή

1.1 Σκοπός και στόχοι του παραδοτέου

Σκοπός του παραδοτέου η παρουσίαση των εργαλείων ασφάλειας που αναπτύχθηκαν στο πλαίσιο του έργου. Τα εν λόγω εργαλεία βασίζονται στην ερευνητική διαδικασία που αναπτύχθηκε στα παραδοτέα Π4.1-Π4.5 και Π3.3 καθώς και στις αντίστοιχες ερευνητικές δημοσιεύσεις. Στόχος των εργαλείων αυτών είναι να καλύψουν τα βασικά κενά ασφαλείας που προκύπτουν από τις προηγούμενες φάσεις της μελέτης (Π3.1, Π3.2, Π3.4).

Σημειώνεται ότι σύμφωνα με το Τεχνικό Δελτίου του έργου, βασικός σκοπός του παραδοτέου αυτού είναι η ανάπτυξη του λογισμικού των εργαλείων ασφάλειας. Ο πηγαίος και ο εκτελέσιμος κώδικας των εργαλείων λογισμικού που αναπτύχθηκαν στο πλαίσιο του παραδοτέου Π4.6 βρίσκεται στο φάκελο **ΕΕ4/ΠΕ46/software** σε επιμέρους υποφακέλους, καθένας εκ των οποίων περιλαμβάνει κάθε ένα από τα εργαλεία λογισμικού που αναπτύχθηκαν στο πλαίσιο του έργου ΜΕΛΙΤΥ.

Στην ενότητα εργασίας ΕΕ5 και ειδικότερα στο παραδοτέο Π5.1, γίνεται η αναλυτική περιγραφή της εφαρμογής και δοκιμής των παραπάνω εργαλείων.

1.2 Δομή του παραδοτέου

Στο κεφάλαιο 2 θα γίνει μια σύντομη επισκόπηση του εργαλείου χαρτογράφησης melic, το οποίο στοχεύει στην αυτοματοποιημένη χαρτογράφηση δικτύων και στην αυτοματοποίηση της συλλογής στοιχείων χαρτογράφησης.

Στο κεφάλαιο 3 θα παρουσιαστεί το εργαλείο ανάλυσης επικινδυνότητας Attack Path Risk Finder (APRF). Το εργαλείο APRF λαμβάνει ως είσοδο δεδομένα δικτύων και συστημάτων, ώστε να υπολογίσει τον πληροφοριακό κίνδυνο που προκύπτει για όλα τα μονοπάτια επίθεσης προς κρίσιμα ιατρικά συστήματα.

Στο κεφάλαιο 4 θα παρουσιαστεί μία υποδομή υλοποιημένη με τεχνολογία blockchain με σκοπό τον έλεγχο πρόσβασης σε ιατρικά δεδομένα. Η εν λόγω υποδομή (Hierarchical Multiblockchan) βασίζεται στα ερευνητικά αποτελέσματα των παραδοτέων Π4.1, Π4.4 και Π4.5, και προσφέρει λεπτομερή έλεγχο πρόσβασης σε ιατρικά δεδομένα που παράγονται από ιατρικές συσκευές.

2 Το εργαλείο Χαρτογράφησης Δικτύων Melicc

2.1 Συνοπτική περιγραφή του εργαλείου

Το εργαλείο Χαρτογράφησης Δικτύων Melicc έχει αναπτυχθεί στο πλαίσιο του έργου ‘ΜΕΛΙΤΥ’. Έχει πάρει το όνομά του από το έργο ΜΕΛΙΤΥ και την λειτουργία του διακομιστή (server) ως σύστημα εντολών και ελέγχου (Command and Control). Το εργαλείο αυτό καλύπτει την ανάγκη για συλλογή δεδομένων και πληροφοριών με σκοπό τη διασφάλιση των προτύπων ασφάλειας, στην επικοινωνία και την λειτουργία διασυνδεδεμένων συσκευών που εξυπηρετούν ιατρικούς σκοπούς και όχι μόνο, σε περιβάλλον ιατρικής περίθαλψης. Με βάση τις παραπάνω σκέψεις δημιουργείται ένα ευέλικτο εργαλείο που μπορεί να χρησιμοποιηθεί για την αλληλεπίδραση μεταξύ συστημάτων κάθε είδους, την εκτέλεση εντολών και τη συλλογή των αποτελεσμάτων τους. Η γλώσσα υλοποίησης είναι η Python, καθώς είναι ευανάγνωστη, προορίζεται για γρήγορη πρωτοτυποποίηση και μπορεί να εκτελεστεί σε κάθε σύστημα που παρέχει έναν διερμηνευτή της γλώσσας. Συνεπώς, γίνεται αντιληπτο οτι βασικός στόχος του

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εργαλείου ‘melicc’ είναι να βοηθά τους διαχειριστές συστημάτων να παρέχουν απομακρυσμένη βοήθεια στους υπαλλήλους, να συλλέγει πληροφορίες όπως δείκτες συμβιβασμού (IOC) από συνδεδεμένες συσκευές και να διασφαλίζει συνολικές πρακτικές ασφάλειας.

Συνοψίζοντας, το εργαλείο Melicc προσφέρει:

- τη δυνατότητα εντοπισμού κενών ασφαλείας,
- τη συλλογή πληροφοριών για την αποτίμηση των κινδύνων που ελλοχεύουν στα συστήματα υπό εξέταση,
- τη δυνατότητα εφαρμογής κανόνων ασφαλείας,
- τη δυνατότητα αναβάθμισης λογισμικού και εφαρμογής ενημερώσεων ασφαλείας.

Η αναλυτική περιγραφή του εργαλείου, καθώς και τα αποτελέσματα της δοκιμής του θα παρουσιαστούν στο παραδοτέο Π5.1.

2.2 Αποθετήριο κώδικα του εργαλείου melicc

Ο πλήρης πηγαίος κώδικας του εργαλείου melic βρίσκεται στο φάκελο **ΕΕ4/ΠΕ46/software/MELICC.**

3 Εργαλείο Υπολογισμού Κινδύνων Attack Path Risk Finder

3.1 Συνοπτική περιγραφή του εργαλείου

Στο πλαίσιο του ερευνητικού έργου ΜΕΛΙΤΥ και πιο συγκεκριμένα στο πλαίσιο του Π3.3 (σχετική δημοσίευση: Stellios, Ioannis, Panayiotis Kotzanikolaou, and Christos Grigoriadis. "Assessing IoT enabled cyber-physical attack paths against critical systems." *Computers & Security* 107 (2021): 102316), αναπτύχθηκε ένα πειραματικό εργαλείο υπολογισμού ρίσκου ψηφιακών και φυσικών μονοπατιών επιθέσεων. Το εργαλείο έχει αναπτυχθεί στην προγραμματιστική γλώσσα Python 3.7 και λειτουργεί ως εργαλείο γραμμής εντολών. Περιλαμβάνει υλοποιήσεις των βιβλιοθηκών pandas,cvss, cvsslib,requests, xmltodict και json. Κατά την εκτέλεση, το εργαλείο δέχεται ως είσοδο csv αρχεία που περιλαμβάνουν λεξικά για την επεξεργασία δεδομένων βάσεων αδυναμιών και δυο csv αρχεία που περιλαμβάνουν στοιχεία για το σύστημα υπό διερεύνηση, το devices.csv και το networks.csv όπου καταγράφονται λεπτομέρειες για τις ενεργές συσκευές και δίκτυα, τα οποία αργότερα μετατρέπονται σε πλαίσια δεδομένων (Dataframes) της βιβλιοθήκης pandas. Ο εκάστοτε ερευνητής ασφαλείας καλείται να συμπληρώσει αυτά τα αρχεία με πληροφορίες για το σύστημα που μελετά όπως:

- Το λειτουργικό σύστημα και οι εφαρμογές που είναι εγκατεστημένα σε μια συσκευή.
- Οι διεπαφές της κάθε συσκευής και το δίκτυο με το οποίο επικοινωνούν.
- Η φυσική τοποθεσία και η ανάλογη κατηγορία τύπου πρόσβασης που της αναλογεί, σε συνδυασμό με την εγγύτητα της συσκευής με άλλες συσκευές του συστήματος.
- Τα δικαιώματα εκτέλεσης της συσκευής σε συσκευές που είναι συνδεδεμένη.
- Η τεχνολογία που χρησιμοποιεί και η συχνότητα εκπομπής ενός δικτύου.
- Οι διασυνδέσεις μεταξύ διαφορετικών δικτύων και το επίπεδο ασφαλείας(CIA) που εφαρμόζεται στο πλαίσιο των μεταξύ τους επικοινωνιών.

Όπως αναφέρθηκε στην προηγούμενη ενότητα, το εργαλείο melic μπορεί να προσφέρει μερική αυτοματοποίηση της συλλογής των παραπάνω δεδομένων. Η αναλυτική περιγραφή του εργαλείου, καθώς και τα αποτελέσματα της δοκιμής του, παρουσιάζονται στο παραδοτέο Π5.1.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

3.2 Αποθετήριο κώδικα του εργαλείου APRF

Ο πλήρης πηγαίος κώδικας του εργαλείου APRF βρίσκεται στο φάκελο **ΕΕ4/ΠΕ46/software/APRF.**

4 Υποδομή Hierarchical Multi Blockchain για τον έλεγχο πρόσβασης ιατρικών δεδομένων

4.1 Συνοπτική περιγραφή της πλατφόρμας Hierarchical Multi Blockchain

Στο πλαίσιο του έργου ΜΕΛΙΤΥ αναλύθηκε και αναπτύχθηκε ένα σύστημα διασύνδεσης οργανισμών (από εδώ και στο εξής, εμπλεκόμενα μέρη), με το οποίο επιτυγχάνεται η ασφαλής και διάφανης λήψη, επεξεργασία και μεταφορά πληροφορίας από έναν εμπλεκόμενο που συμμετέχει στο σύστημα, προς έναν άλλον. Το σύστημα μπορεί και μεταφέρει πληροφορία η οποία αφορά ευαίσθητα δεδομένα ή ευαίσθητες λειτουργίες πληροφοριακών συστημάτων ή «έξυπνων» συσκευών ενός εμπλεκόμενου μέρους. Η υλοποίηση του συστήματος ενέχει χαρακτηριστικά πολυεπίπεδου ελέγχου πρόσβασης σε ιατρικά δεδομένα και αναπτύχθηκε στα πλαίσια των παραδοτέων Π4.1, Π4.4 και Π4.5, καθώς και των σχετικών ερευνητικών δημοσιεύσεων που αντιστοιχούν στα παραδοτέα αυτά. Η συγκεκριμένη πλατφόρμα δίνει τη δυνατότητα, σε πληροφοριακά συστήματα όπου συμμετέχουν πολλοί εμπλεκόμενοι, να ανταλλάσσουν ευαίσθητη πληροφορία προστατεύοντας την εμπιστευτικότητα, ακεραιότητα καθώς και την αυθεντικότητα αυτής, ενώ ταυτόχρονα αξιοποιεί την τεχνολογία Blockchain ώστε όλοι οι εμπλεκόμενοι να έχουν εικόνα των ενεργειών που συνέβησαν στην ευαίσθητη πληροφορία ή στις ευαίσθητες λειτουργίες των συστημάτων.

Ως **ευαίσθητα δεδομένα** ορίζουμε τα δεδομένα αυτά τα οποία δεν επιδέχονται ελεύθερης πρόσβασης από τα εμπλεκόμενα μέρη που συμμετέχουν στο σύστημα. Πιο συγκεκριμένα, ευαίσθητα δεδομένα που θα λαμβάνονται στο σύστημα από τα εμπλεκόμενα μέρη, θα διακινούνται και θα αποθηκεύονται σε αυτό θα πρέπει να λαμβάνουν ιδιαίτερης προσοχής, αφού η πρόσβασή τους θα πρέπει να είναι οριοθετημένη και η λήψη τους να πλαισιώνεται από σαφείς πολιτικές και ελέγχους που θα επιτρέπουν ή θα απαγορεύουν σε μία οντότητα που ανήκει σε ένα εμπλεκόμενο μέρος να λάβει πρόσβαση σε αυτά. Για παράδειγμα, ευαίσθητα δεδομένα εμπεριέχει το ιατρικό ιστορικό ενός ασθενούς, ο οποίος μπορεί να βρίσκεται υπό παρακολούθηση σε μία κλινική δομή ενός ιατρικού οργανισμού (εμπλεκόμενο μέρος) που συμμετέχει στο σύστημα και για τον οποίο η λήψη αυτών των πληροφοριών θα πρέπει να οριοθετείται και να προστατεύεται, προκειμένου πρόσβαση να λαμβάνουν μόνο πιστοποιημένες, επικυρωμένες οντότητες του συστήματος που τους επιτρέπεται η πρόσβαση και αξιοποίηση της προστατευμένης πληροφορίας.

Ως **ευαίσθητες λειτουργίες** ή ενέργειες ορίζουμε τις λειτουργίες αυτές οι οποίες μπορούν να εκτελεστούν από ένα εμπλεκόμενο μέρος στην υποδομή του και, στην περίπτωση που αυτές έχουν παραποιηθεί/αλλοιωθεί, να κινδυνέψει ή γενικότερα να επηρεαστεί ο ανθρώπινος ή άλλος παράγοντας τον οποίο αυτές αφορούν και στον οποίο επιδρά η χρήση τους ή ακόμη και να ασκήσουν επιπτώσεις σε τρίτα μέρη τα οποία μπορούν να έχουν άμεση ή έμμεση σχέση με αυτές. Για παράδειγμα, εκτός των επιπτώσεων που μπορούν να έχουν στον χρήστη τους (π.χ. σε έναν ασθενή), η χρήση μίας συσκευής σε μία κλινική μονάδα και η εγκατάσταση παραποιημένου λογισμικού, θα μπορούσε να επηρεάσει αρνητικά ακόμη και τον κατασκευαστή της (π.χ. ως προς τη φήμη, αξιοπιστία κ.λπ.). Συνεπώς, κρίνεται αναγκαίο το σύστημα να διαχειρίζεται τις πληροφορίες οι οποίες σχετίζονται με ευαίσθητες λειτουργίες που υλοποιούνται στις υποδομές των εμπλεκόμενων μερών με γνώμονα την ασφάλεια, την ακεραιότητα και τη διαθεσιμότητά τους.

Σκοπός και στόχος του προτεινόμενου συστήματος είναι η διαφανής, έγκυρη καθώς και έγκαιρη μεταφορά κρίσιμης πληροφορίας μεταξύ των εμπλεκόμενων μερών που συμμετέχουν σε αυτό. Κάθε εμπλεκόμενο μέρος θα μπορεί ανεξάρτητα να επιβεβαιώσει την διακινούμενη πληροφορία και, λόγω της φύσης του συστήματος η οποία στηρίζεται στη Blockchain τεχνολογία, θα είναι πρακτικά αδύνατο αυτή

Ευρωπαϊκή Ένωση Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΥΔΕ ΕΤΑΚ
ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020 ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

να αλλοιωθεί. Επιπλέον, πρόσβαση στην πληροφορία θα λαμβάνουν μόνον οι οντότητες που έχουν τα απαραίτητα δικαιώματα και διαπιστευτήρια. Για την επίτευξη των παραπάνω, το σύστημα θα πρέπει να παρέχει λειτουργίες μέσα από τις οποίες τα εμπλεκόμενα μέρη θα συμφωνούν τους κανονισμούς και τις πολιτικές με τις οποίες η πρόσβαση στα δεδομένα και η εξασφάλιση της ακεραιότητας τους, θα επιτυγχάνεται. Κάθε δομική λειτουργία του συστήματος, η οποία συντελεί στο τελικό αποτέλεσμα, θα πρέπει να καταγράφεται με ασφαλή τρόπο και οι καταγραφές αυτές να γίνονται διαθέσιμες στα εμπλεκόμενα μέρη που αφορούν, με γνώμονα τη διαφάνεια η οποία προσφέρεται στο σύστημα με την αξιοποίηση της τεχνολογίας του Blockchain.

Συγκεκριμένα, τα πέντε (5) δομικά στοιχεία του συστήματος, τα οποία υποστηρίζονται από την τεχνολογία του Blockchain, είναι:

- Διαφάνεια (Transparency), με την έννοια ότι όλες οι κρίσιμες ενέργειες θα πρέπει να καταγράφονται και να είναι διαθέσιμες στα εμπλεκόμενα μέρη του συστήματος τα οποία αφορούν
- Εμπιστευτικότητα (Confidentiality), δηλαδή τα εμπλεκόμενα μέρη να μπορούν να εμπιστευτούν στο σύστημα τα κρίσιμα και ευαίσθητα δεδομένα και λειτουργίες τους – Οποιαδήποτε πρόσβαση στις πληροφορίες αυτές, προϋποθέτει την έγκριση του κατόχου τους
- Αυθεντικότητα (Authenticity), δηλαδή οι πληροφορίες και τα δεδομένα που θα διακινούνται στο σύστημα, να μπορούν εύκολα να ελεγχθούν για την ορθότητα, την αυθεντικότητα και την εγκυρότητά τους
- Αυτοματισμός των λειτουργιών, προκειμένου το σύστημα να μην απαιτεί την ύπαρξη του ανθρώπινου παράγοντα ώστε να επιβεβαιώνει και να διεκπεραιώνει τις ενέργειες που του έχουν ζητηθεί από τα εμπλεκόμενα μέρη
- Δυναμική διαχείριση κρυπτογραφικών στοιχείων τα οποία επιτρέπουν την ασφαλή παράδοση περιεχομένου σε άτομα που συμμετέχουν σε δυναμικές ομάδες (π.χ. γιατροί εν εφημερία)

Στο σύστημα αναπτύσσονται πέντε (5) σενάρια χρήσης, μέσω των οποίων διαφαίνονται μερικές από τις κύριες δυνατότητες του, όπως αυτές είναι:

- Δημιουργία αιτήματος για τη λήψη πληροφοριών από τα εμπλεκόμενα μέρη
- Αυθεντικοποίηση και Εξουσιοδότηση οντότητας
- Συγκέντρωση και αξιοποίηση ρόλων οντότητας (μόνιμων και προσωρινών, π.χ. Γιατρός, Ερευνητής (Μόνιμοι ρόλοι) και Ωράριο βάρδιας εργασίας, Θεράπων ιατρός ασθενούς (Προσωρινοί ρόλοι))
- Προώθηση αιτήματος στο αρμόδιο Domain Blockchain
- Λήψη δεδομένων και πληροφοριών, που αφορούν το αίτημα, από τις Βάσεις Δεδομένων των εμπλεκόμενων μερών του συστήματος
- Μερική και Πλήρης αποκρυπτογράφηση δεδομένων
- Προώθηση των ληφθέντων πληροφοριών από τα εμπλεκόμενα μέρη, που αφορούν ένα αίτημα μίας οντότητας, στην οντότητα αυτή.

Επίσης, το σύστημα επιτρέπει την αποστολή και την παραλαβή ευαίσθητης πληροφορίας (ή την αποστολή/παραλαβή ευαίσθητων εντολών/αποτελεσμάτων) όπου τόσο η αίτηση όσο και τα αποτελέσματα μπορούν να είναι αναγνώσιμα μόνο από τις οντότητες που ο οργανισμός τους έχει ορίσει δυναμικά ότι θα είχαν πρόσβαση σε τέτοια πληροφορία. Ως δυναμική αξίωση πρόσβασης ορίζεται η δυνατότητα του συστήματος να επιτρέπει την άντληση και την πρόσβαση σε πληροφορία μόνο από οντότητες οι οποίες έχουν λάβει την κατάλληλη έγκριση από το εμπλεκόμενο μέρος στο οποίο ανήκουν, μέσω πολιτικών. Οι πολιτικές αυτές μπορούν να ανανεώνονται από το καθένα εμπλεκόμενο μέρος, οποιαδήποτε στιγμή, σύμφωνα με τις εκάστοτε ανάγκες και συνθήκες. Για παράδειγμα, ένας γιατρός ο οποίος ανήκει σε ένα εμπλεκόμενο μέρος του συστήματος (π.χ. ιατρικό οργανισμό), μπορεί να λάβει το ιατρικό ιστορικό ενός ασθενή ο οποίος χρήζει ιατρικής παρακολούθησης, μόνο εφόσον ικανοποιεί τουλάχιστον μία από τις παρακάτω δύο συνθήκες:

1. Εάν ο γιατρός είναι ο θεράπων ιατρός του ασθενούς
2. Εάν ο γιατρός αυτός είναι *γιατρός εν εφημερία*, για τη χρονική περίοδο (ωράριο εργασίας/εφημερίας) όπου ο ασθενής χρήζει παρακολούθησης

Οι παραπάνω δύο συνθήκες εκτελούνται και ελέγχονται αυτόματα από το σύστημα, μέσω των εξατομικευμένων πολιτικών του κάθε εμπλεκόμενου μέρους. Στο συγκεκριμένο παράδειγμα,

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αξιοποιούνται οι πολιτικές του ιατρικού οργανισμού στον οποίο ανήκει ο γιατρός αυτός ο οποίος επιθυμεί να λάβει πρόσβαση στα δεδομένα του ασθενούς. Όπως γίνεται αντιληπτό, ένα εξαιρετικά σημαντικό σημείο της προτεινόμενης υλοποίησης είναι πως οι πολιτικές αυτές δεν απαιτούν καμία άλλη ενέργεια από τα εμπλεκόμενα μέρη, πέραν της ανανέωσής τους, αφού αξιοποιούνται αυτόματα από το σύστημα, χωρίς να απαιτούν την ύπαρξη του ανθρώπινου παράγοντα κατά τη λήψη αποφάσεων και γενικότερα κατά την εκτέλεση κρίσιμων ενεργειών.

Αναλύοντας τα παραπάνω, μπορούμε να εξάγουμε τις βασικές-θεμελιώδεις παραδοχές οι οποίες υποστηρίζουν τις λειτουργίες του συστήματος:

- Το σύστημα αποτελείται από πολλά εμπλεκόμενα μέρη, διαφορετικών αναγκών, τρόπου διοίκησης, αξιών κ.ο.κ.. Συνεπώς, θα πρέπει να υπάρχει σαφής διαχωρισμός μεταξύ των εμπλεκόμενων μερών του συστήματος και το καθένα να λογίζεται ως μοναδικό, με δικές του εσωτερικές λειτουργίες και πολιτικές.
- Κάθε θεμελιώδης λειτουργία του συστήματος, θα πρέπει να λαμβάνεται υπόψιν ως κρίσιμη και οι εισροές, οι επεξεργασίες και οι εκροές που υπάρχουν και συμβαίνουν σε αυτές, να διέπονται από διαφάνεια, αξιοπιστία και ασφάλεια. Η τελική και συνολική αξιοπιστία του συστήματος, κρίνεται από τα τρία αυτά χαρακτηριστικά.
- Όλα τα δεδομένα και πληροφορίες που διακινούνται στο σύστημα, λογίζονται και λαμβάνονται υπόψιν ως κρίσιμα και ευαίσθητα.
- Η αποτελεσματικότητα του συστήματος κρίνεται και βασίζεται στη συντονισμένη και διακεκριμένη πρόσβαση στις πληροφορίες και τα δεδομένα που αυτό αντλεί από τα εμπλεκόμενα μέρη και διαχειρίζεται.
- Είναι αναγκαία η ύπαρξη λειτουργιών και μηχανισμών που θα διαχειρίζονται την διακεκριμένη πρόσβαση στις πληροφορίες που διαθέτουν τα εμπλεκόμενα μέρη και μπορούν να αντληθούν μέσω του συστήματος. Η πρόσβαση στις πληροφορίες αυτές θα επιτυγχάνεται μέσω πολιτικών (κοινών και εξατομικευμένων) που θα επιτρέπουν τη δυναμική διαχείριση των διαπιστευτηρίων και δικαιωμάτων των οντοτήτων (π.χ. Γιατροί, Ερευνητές κ.λπ.) που ανήκουν σε ένα εμπλεκόμενο μέρος (π.χ. ιατρικό οργανισμό) και επιθυμούν να λάβουν και να αξιοποιήσουν πληροφορίες που μπορούν να ληφθούν από τα εμπλεκόμενα μέρη.

Η αναλυτική περιγραφή του εργαλείου, καθώς και τα αποτελέσματα της δοκιμής του, θα παρουσιαστούν στο παραδοτέο Π5.1.

4.2 Αποθετήριο κώδικα της υποδομής Hierarchical Multi-blockchain

Ο πλήρης πηγαίος κώδικας του εργαλείου HMBC βρίσκεται στο φάκελο **ΕΕ4/ΠΕ46/software/HMBC.**

Ευρωπαϊκή Ένωση Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΥΔΕ ΕΤΕΑΚ
ΕΠΑνΕΚ 2014–2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020 ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

5 Οπισθόφυλλο

«Η εργασία υλοποιήθηκε στο πλαίσιο της Δράσης ΕΡΕΥΝΩ – ΔΗΜΙΟΥΡΓΩ - ΚΑΙΝΟΤΟΜΩ και συγχρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση και εθνικούς πόρους μέσω του Ε.Π. Ανταγωνιστικότητα, Επιχειρηματικότητα & Καινοτομία (ΕΠΑνΕΚ) (κωδικός έργου:Τ1ΕΔΚ-01958)»

This research has been co-financed by the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH – CREATE – INNOVATE (project code:T1EDK-01958)

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης