Αποδοτική Υλοποίηση Κρυπτοβιβλιοθήκης και επέκταση της σε blockchain τεχνολογίες

Σήμερα όλες οι ηλεκτρονικές υπηρεσίες που αναπτύσσονται στην Ελλάδα και στην Ευρωπαϊκή Ένωση πρέπει να συμμορφώνονται με τους εθνικούς και Ευρωπαϊκούς Νόμους Περί Προστασίας Δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ).

Λόγω της υποχρέωσης όλων των ηλεκτρονικών παροχών να είναι σύννομοι με τον Νομό για την προστασία των προσωπικών δεδομένων το τελευταίο διάστημα έχουν προσελκύσει το ενδιαφέρον της επιστημονικής κοινότητας και της βιομηχανίας τεχνολογίες για την προστασία της ιδιωτικότητας του χρήστη (Privacy Enhancing Technologies-PETs). Πρόσφατα αναπτύχθηκε και μια βιβλιοθήκη που ενσωμάτωσε και την blockchain τεχνολογία ώστε οι τεχνολογίες αυτές να προσφέρουν πιο αποδοτικές και εύχρηστες ηλεκτρονικές υπηρεσίες.

Δυστυχώς, όμως η υιοθέτηση των παραπάνω τεχνολογιών αιχμής από τους παρόχους ηλεκτρονικών υπηρεσιών παραμένει περιορισμένη λόγω της δύσκολής ενσωμάτωσης τους, της υποβάθμισης της απόδοσης και της ευχρηστίας των παρεχόμενων υπηρεσιών. Οι δυνατότητές που μπορεί να παρέχουν οι τεχνολογίες PETs εάν αξιοποιηθούν από τις ηλεκτρονικές υπηρεσίες θα αλλάξουν την ποιότητα και την αξιοπιστία των ηλεκτρονικών συναλλαγών παρέχοντας στους χρήστες ασφαλείς συναλλαγές που θα προστατεύουν τα προσωπικά τους δεδομένα.

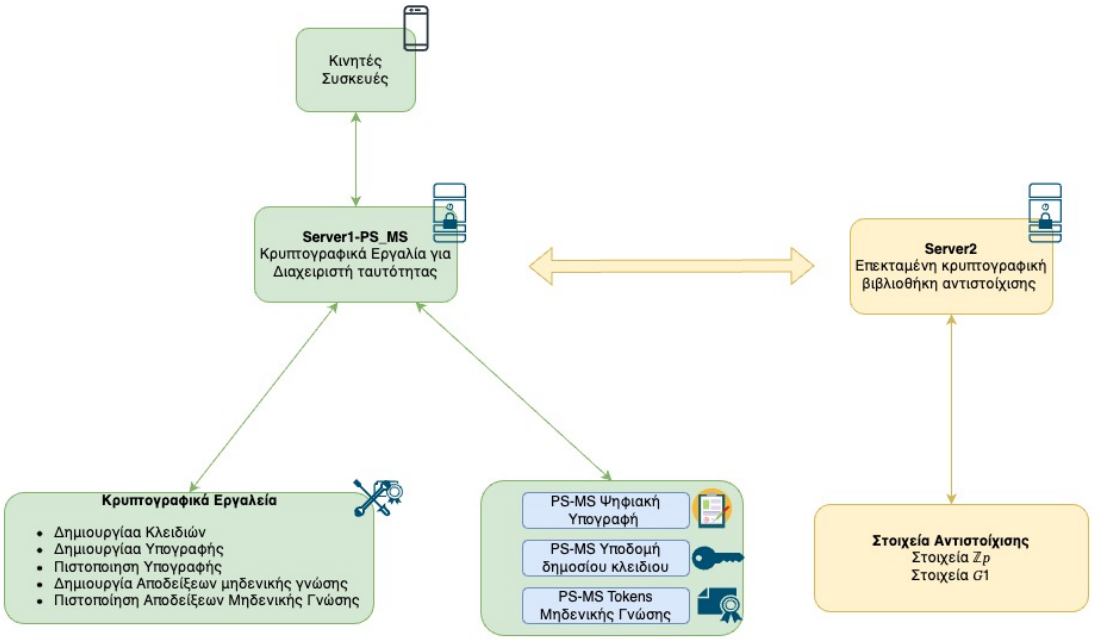
Η πρόταση "Αποδοτική Υλοποίηση Κρυπτοβιβλιοθήκης» που χρηματοδοτήθηκε από την Ε.Λ.Λ.Α.Κ στοχεύει στην επέκταση της "blockchain" τεχνολογίας ώστε να μπορεί αξιόπιστα να διαφυλάττει την ιδιωτικότητα του χρήστη και ταυτόχρονα να προσφέρει ένα αποδοτικό και ευέλικτο περιβάλλον χρήστη που να μπορεί να υποστηρίξει πολυάριθμες ηλεκτρονικές υπηρεσίες και εφαρμογές όπως: η ηλεκτρονική διακυβέρνηση (π.χ. επιτυγχάνοντας έτσι την απλοποίηση του χαρτιού με την αντικατάσταση εγγράφων σε χαρτί από αντίστοιχα ηλεκτρονικά έγγραφα, χωρίς να χρειάζεται να εγκαταλείψει την ασφάλεια), ή άλλες, όπως, ενδεικτικά, οι έξυπνες πόλεις, το ηλεκτρονικό εμπόριο ή ο έλεγχος φυσικής πρόσβασης σε περιορισμένους χώρους.

Προς αυτή την κατεύθυνση προτείνουμε την επέκταση μιας ευρέως διαδεδομένης κρυπτογραφικής βιβλιοθήκης της OLYMPUS ώστε να παρέχει νέες προχωρημένες, ασφαλέστερες και αποδοτικότερες υπηρεσίες για την διαχείρισης της ταυτότητας των χρηστών με την χρήση της τεχνολογίας blockchain.

Επιπλέον θα διερευνηθεί τόσο η πρακτική, όσο και η θεωρητική πλευρά της ανάπτυξης επιτυχημένων κρυπτογραφικών βιβλιοθηκών με βάση τις ελλειπτικές καμπύλες (GNUCrypto) για την υποστήριξη υπηρεσιών διαχείρισης ταυτότητας με την χρήση της blockchain τεχνολογίας. Σήμερα η ανωνυμοποιηση του χρήστη αλλά και η προστασία της ιδιωτικότητας του μπορεί να επιτευχθεί μόνο με την χρήση της υποδομής δημοσίου κλειδιού (Public Key Infrastructure (PKI)) που δυστυχώς δεν αποτελεί και την πιο αποδοτική μορφή κρυπταλγορίθμων, για ’αυτό και όλες οι υλοποιήσεις χρησιμοποιούν την κρυπτογράφηση με βάση τις ελλειπτικές καμπύλες (ECC) καθώς παράγει πιο αποδοτικούς κρυπταλγοριθμούς. Μια από τις βασικότερες βιβλιοθήκες που χρησιμοποιείται για την ανάπτυξη εργαλείων κρυπτογραφίας που βασίζονται σε ελλειπτικές καμπύλες είναι η GNU-Crypto βιβλιοθήκη. Πληθώρα κρυπτογραφικών βιβλιοθηκών έχουν αναπτυχθεί που επεκτείνουν την GNU-Crypto βιβλιοθήκη ώστε να υλοποιήσουν την αντιστοίχισης πάνω σε ελλειπτικές καμπύλες με βάση την GNU-Crypto βιβλιοθήκη.

Αναλυτικότερα σχεδιάζοντας αποδοτικότερες δομές δεδομένων θα υλοποιηθεί η βιβλιοθήκη που θα πραγματοποιεί την αντιστοίχιση πάνω στις ελλειπτικές καμπύλες και θα μετρηθεί η απόδοση της βιβλιοθήκης σε δοκιμαστική εφαρμογή που χρησιμοποιεί την τεχνολογία blockchain για την διαχείριση ταυτότητας των χρηστών με βάση τον κώδικα OLYMPUS. Έχουμε επιλέξει να εφαρμόσουμε και να αξιολογήσουμε τις βελτιστοποιήσεις που θα αναπτυχθούν σε μια σύγχρονη βιβλιοθήκη (OLYMPUS) που χρησιμοποιεί blockchain τεχνολογία για την υλοποίηση κατανεμημένων υπηρεσιών διαχείρισης ταυτότητας διατηρώντας ταυτόχρονα την ανωνυμία των χρηστών.

Στο παρακάτω σχήμα περιγράφεται η αρχιτεκτονική του συστήματος για την υλοποίηση της επέκτασης της βιβλιοθήκης OLYMPUS και της αξιολόγησης της απόδοσης και της ευχρηστίας στην διαχείριση ταυτότητας των χρηστών.



Σχήμα: Αρχιτεκτονική Συστήματος

Η τεχνολογία blockchain που μπορεί να παρέχει μια κατανεμημένη πιστοποίηση του χρήστη σε συνδυασμό με την αποδοτική εφαρμογή των κρυπτογραφικών πράξεων θα οδηγήσει στον σχεδιασμό ενός εύχρηστου και ευέλικτου περιβάλλοντος χρήστη για την υποστήριξη πολυάριθμων ηλεκτρονικών υπηρεσιών και εφαρμογών που δύναται να επιφέρει πολλά οφέλη στις δημόσιες υπηρεσίες στην Ελλάδα. Ακολουθούν ορισμένοι τομείς στους οποίους μπορεί να εφαρμοστεί η παραγόμενη βελτιστοποιημένη βιβλιοθήκη:

- **Κτηματολόγιο:** Οι υποστηριζόμενες ηλεκτρονικές υπηρεσίες μπορούν να χρησιμοποιηθούν για τη παροχή ηλεκτρονικών υπηρεσιών για την πιστοποίηση της ιδιοκτησίας με μια ασφαλή και διαφανή μεθοδολογία. Με αυτό τον τρόπο θα είναι εφικτή η καταγραφή της ιδιοκτησίας και των συναλλαγών ακινήτων σε μια αλυσίδα μπλοκ, παρέχοντας μια αποτελεσματικότερη διαδικασία που αποτρέπει τις απάτες και τις αμφισβητήσεις.
- **Συστήματα ψηφοφορίας**: Η βελτιστοποιημένη βιβλιοθήκη μπορεί να χρησιμοποιηθεί από εφαρμογές ψηφοφορίας αυξάνοντας τη διαφάνεια και την ακεραιότητα της δημοκρατικής διαδικασίας. Με την παρεχόμενη τεχνολογία θα είναι εφικτή η ασφαλής καταγραφή της ψήφου σε μια αμετάβλητη αλυσίδα μπλοκ, που θα αποτρέπει οποιαδήποτε απόπειρα αλλοίωσης ή παραποίησης. Το βασικό πλεονέκτημα αυτής της καινοτόμας τεχνολογίας έγκειται στην

ικανότητά της να ενισχύει την ακλόνητη εμπιστοσύνη στην εκλογική διαδικασία.

- **Διαχείριση της αλυσίδας εφοδιασμού:** Η παρεχόμενη βιβλιοθήκη μπορεί να χρησιμοποιηθεί από οποιαδήποτε εφαρμογή διαχείρισης της αλυσίδας παραγωγής προϊόντων επιτρέποντας την απρόσκοπτη παρακολούθηση και εντοπισμό των εμπορευμάτων σε κάθε στάδιο, ενισχύοντας έτσι τη διαφάνεια και μειώνοντας σημαντικά τον κίνδυνο παραποιημένων προϊόντων. Η εφαρμογή της σε τομείς όπως η γεωργία έχει τεράστια αξία, καθώς διασφαλίζει τη διατήρηση της προέλευσης και της ποιότητας των προϊόντων, ενισχύοντας τελικά την εμπιστοσύνη και την αξιοπιστία σε ολόκληρο τον κλάδο.
- **Αρχεία υγειονομικής περίθαλψης:** Στον κλάδο της υγειονομικής περίθαλψης, διευκολύνεται η ασφαλή και απρόσκοπτη ανταλλαγή αρχείων υγείας ασθενών μεταξύ διαφόρων παρόχων υγειονομικής περίθαλψης. Με την αξιοποίηση της βελτιστοποιημένης κρυπτο-βιβλιοθήκης, η ανταλλαγή ιατρικών πληροφοριών μπορεί να γίνει πιο αποτελεσματική, οδηγώντας σε βελτιωμένη φροντίδα των ασθενών και ελαχιστοποίηση των διοικητικών περιπλοκών. Επιπλέον με την αλυσίδα μπλοκ, τα αρχεία υγειονομικής περίθαλψης μπορούν να προσεγγιστούν με ασφάλεια και με απόλυτη ακρίβεια, προωθώντας ένα πιο εκσυγχρονισμένο και διασυνδεδεμένο οικοσύστημα υγειονομικής περίθαλψης.
- **Διαχείριση ταυτότητας:** Μέσω των συστημάτων ταυτότητας , οι πολίτες μπορούν να διατηρούν μια επαληθευμένη ψηφιακή ταυτότητα αποθηκευμένη σε μια αλυσίδα μπλοκ (blockchain), απλοποιώντας την πρόσβαση σε δημόσιες υπηρεσίες και εξορθολογίζοντας τις γραφειοκρατικές διαδικασίες.
- **Φορολογία και διαχείριση εσόδων:** Με την εισαγωγή της βελτιστοποιημένης κρυπτο-βιβλιοθήκης σε εφαρμογές για την διαχείριση εσόδων θα αναβαθμιστούν οι οικονομικές συναλλαγές. Οι παρεχόμενες ασφαλείς, διαφανείς και πιστοποιημένες συναλλαγές θα οδηγήσουν τελικά σε μια πιο ισχυρή και αξιόπιστη διαδικασία διαχείρισης εσόδων.
- **Δημόσιες συμβάσεις:** Οι δημόσιες συμβάσεις διαδραματίζουν καίριο ρόλο στη λειτουργία των κυβερνητικών συστημάτων παγκοσμίως. Περιλαμβάνει την απόκτηση αγαθών, υπηρεσιών και έργων από δημόσιους φορείς μέσω μιας διαφανούς και ανταγωνιστικής διαδικασίας. Ωστόσο, η διαδικασία αυτή αντιμετωπίζει συχνά προκλήσεις όπως η έλλειψη διαφάνειας, η πιθανή

διαφθορά και οι δυσκολίες στην εξασφάλιση της δικαιοσύνης. Με τις υποστηριζόμενες τεχνολογίες, οι διαδικασίες σύναψης δημόσιων συμβάσεων μπορούν να ενισχυθούν όσον αφορά τη διαφάνεια και τη δικαιοσύνη.

Η ανάπτυξη της «Αποδοτικής Κρυπτοβιβλιοθήκης» απαιτεί προσεκτικό σχεδιασμό και συνεργασία των ενδιαφερόμενων μερών για να διασφαλιστεί η επιτυχής εφαρμογή. Συνοψίζοντας η χρήσης της κρυπτοβιβλιοθήκης στον δημόσιο τομέα θα διαδραματίσει ζωτικό ρόλο στη διασφάλιση ασφαλών και αξιόπιστων ψηφιακών συναλλαγών και επικοινωνιών. Επίσης χρησιμοποιώντας την κρυπτοβιβλιοθήκη, οι υπηρεσίες και τα ιδρύματα μπορούν να διασφαλίσουν ευαίσθητα δεδομένα, να προστατεύσουν από μη εξουσιοδοτημένη πρόσβαση και να επαληθεύσουν τη γνησιότητα και την ακεραιότητα των ψηφιακών εγγράφων και συναλλαγών. Τέλος με την υιοθέτηση της θα μπορέσει ο δημόσιος τομέας να τηρήσει υψηλά τα πρότυπα προστασίας δεδομένων, ιδιωτικότητας και ασφάλειας, προωθώντας την εμπιστοσύνη στις ηλεκτρονικές συναλλαγές και τις αλληλεπιδράσεις με πολίτες, επιχειρήσεις και άλλους κυβερνητικούς φορείς.