ΠΕΡΙΛΗΨΗ

ΑΞΙΟΠΙΣΤΙΑ ΔΕΔΟΜΕΝΩΝ ΣΤΟ INTERNET OF THINGS ΜΕΣΩ ΤΕΧΝΟΛΟΓΙΩΝ BLOCKCHAIN ΚΑΙ SELF-SOVEREIGN IDENTITIES

ΚΩΝΣΤΑΝΤΙΝΟΣ ΔΗΜΗΤΡΙΑΔΗΣ ΣΠΥΡΙΔΩΝ ΠΑΝΑΓΙΩΤΑΚΗΣ

Στο Internet of Things (IoT) δισεκατομμύρια συσκευές παράγουν και μεταδίδουν συνεχώς δεδομένα. Σε εφαρμογές όπου η προέλευση των δεδομένων αποτελεί σημαντική παράμετρο αξιοπιστίας, δεν αρκεί απλώς να ληφθεί μια μέτρηση· πρέπει να μπορεί να ταυτοποιηθεί η συσκευή που την έστειλε και να επαληθευτεί ότι η μέτρηση δεν έχει αλλοιωθεί. Σε αυτό το πλαίσιο, τεχνολογίες Self-Sovereign Identity (SSI), όπως τα Decentralized Identifiers και τα Verifiable Credentials, παρέχουν στη συσκευή μια κρυπτογραφικά επαληθεύσιμη ταυτότητα. Επιπλέον, τεχνολογίες permissioned blockchain, όπως το Hyperledger Indy, μπορούν να αποτελέσουν σημείο αναφοράς για τη δημοσίευση των δημόσιων αντικειμένων εμπιστοσύνης που απαιτούνται για την έκδοση, την επαλήθευση και την ανάκληση του διαπιστευτηρίου. Παρόλα αυτά, σε συστήματα IoT συνεχούς τηλεμετρίας, η δημιουργία αποδείξεων εγκυρότητας του διαπιστευτηρίου από τον holder εκ μέρους της συσκευής και η επαλήθευσή τους στην πλευρά της υποδομής μπορούν να αποδειχθούν ιδιαίτερα κοστοβόρες. Με αφορμή αυτό, στην παρούσα εργασία σχεδιάστηκε, υλοποιήθηκε και αξιολογήθηκε ένα λειτουργικό σύστημα συνεχούς IoT τηλεμετρίας, βασισμένο σε DIDs, AnonCreds, Hyperledger Indy, DIDComm και ACA-Py agents, με δύο συσκευές Raspberry Pi Zero 2 W στον ρόλο των IoT συσκευών που δημιουργούν συνεχώς δεδομένα τηλεμετρίας. Πάνω σε αυτό σχεδιάστηκαν και αξιολογήθηκαν πέντε διαφορετικές πολιτικές αναφορικά με τη συχνότητα που εφαρμόζονται οι διαδικασίες επαλήθευσης της προέλευσης των δεδομένων: PER_MESSAGE, SESSION_TTL, HYBRID, BATCH και BATCH_TIME. Οι πολιτικές διαφέρουν ως προς τα χρονικά σημεία στα οποία ζητείται πλήρης επαλήθευση και ως προς τους μηχανισμούς ελέγχου των ενδιάμεσων μηνυμάτων μεταξύ δύο πλήρων επαληθεύσεων. Η πειραματική αξιολόγηση έγινε τόσο σε συνθήκες ασφαλούς λειτουργίας, όπου καταγράφηκαν μετρικές απόδοσης όπως η καθυστέρηση, ο μέσος χρόνος επεξεργασίας, η χρήση CPU και RAM που επιφέρουν οι συχνές πολιτικές επαλήθευσης, όσο και σε σενάριο μη ασφαλούς λειτουργίας, στο οποίο η συσκευή ξεκινά να στέλνει μετρήσεις με αλλοιωμένη υπογραφή. Στο δεύτερο σενάριο μετρήθηκαν ο χρόνος εντοπισμού των μη αυθεντικών μηνυμάτων, ο αριθμός όσων έγιναν δεκτά προτού γίνει αντιληπτή η παραβίαση, και ο χρόνος ανάκαμψης της συσκευής. Συνολικά εξετάστηκαν τρεις τοπολογίες: dedicated edge holder για κάθε IoT συσκευή, κοινός multitenant holder για τις δύο συσκευές και holder τοπικά πάνω στη φυσική συσκευή. Στην τοπολογία dedicated edge holder, οι υπόλοιπες πολιτικές παρουσίασαν, συγκριτικά με το baseline (PER_MESSAGE), μείωση της διάμεσης καθυστέρησης κατά περίπου 72–75%, μείωση του μέσου χρόνου επεξεργασίας ανά μήνυμα κατά 77% έως 96% και μείωση της χρήσης CPU σε verifier και holder κατά περίπου 66,2% έως 87,0%. Η πολιτική HYBRID κράτησε μηδενική έκθεση σε μηνύματα με μη έγκυρη υπογραφή, με κόστος παρόμοιο με εκείνο των SESSION_TTL, BATCH και BATCH_TIME. Όσον αφορά τη σύγκριση των τοπολογιών, αυτή του dedicated holder παρουσίασε τη χαμηλότερη καθυστέρηση σε όλες τις πολιτικές, με αυξημένο όμως κόστος υποδομής. Η τοπολογία του multitenant holder μείωσε τη μνήμη των holders στην υποδομή, αυξάνοντας ελαφρώς την καθυστέρηση, ενώ η τοπολογία του τοπικού holder δεν απαίτησε εξωτερικό κόμβο holder, αύξησε όμως αισθητά την καθυστέρηση και τον χρόνο επεξεργασίας. Συνολικά, η εργασία δείχνει ότι η πολιτική επαλήθευσης και η θέση του holder είναι δύο ξεχωριστές αλλά αλληλένδετες σχεδιαστικές αποφάσεις, που πρέπει να επιλέγονται με βάση το αποδεκτό παράθυρο έκθεσης, τις απαιτήσεις απόδοσης και τους διαθέσιμους πόρους.

Λέξεις κλειδιά: Self-Sovereign Identity, Verifiable Credentials, Internet of Things, AnonCreds, blockchain, πολιτικές επαλήθευσης