IoTFeds

Κατανεμημένες Αγορές Δεδομένων για IoT Ομοσπονδίες
Distributed Data Marketplaces for IoT Federations

Π2.2 – Αναφορά Μηχανισμών Διαφήμισης, Ανακάλυψης και Ασφαλούς Πρόσβασης σε Πόρους IoT

ΔΡΑΣΗ ΕΘΝΙΚΗΣ ΕΜΒΕΛΕΙΑΣ:
«ΕΡΕΥΝΩ-ΔΗΜΙΟΥΡΓΩ-ΚΑΙΝΟΤΟΜΩ Β' ΚΥΚΛΟΣ»
«ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ, ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ & ΚΑΙΝΟΤΟΜΙΑ» (ΕΠΑνΕΚ)
Ειδική Υπηρεσία Διαχείρισης Επιχειρησιακού Προγράμματος Ανταγωνιστικότητα Επιχειρηματικότητα και Καινοτομία (ΕΥΔ ΕΠΑνΕΚ)
Ειδική Υπηρεσία Διαχείρισης και Εφαρμογής Δράσεων στους τομείς Έρευνας, Τεχνολογικής Ανάπτυξης και Καινοτομίας
(ΕΥΔΕ ΕΤΑΚ)

Έργο	IoTFeds
Κωδικός Έργου	Τ2ΕΔΚ-02178
Ενότητα Εργασίας	ΕΕ2 (Δ2.3, Δ2.4)
Υπεύθυνος Ενότητας	ΕΚΕΤΑ
Υπεύθυνος Παραδοτέου	ΕΚΕΤΑ
Έκδοση Παραδοτέου	1.0
Ημερομηνία	30/06/2023

Συντονιστές Παραδοτέου
Ευάγγελος Αθανασάκης, ΕΚΕΤΑ
Σοφία Πολυμένη, ΕΚΕΤΑ
Ζήσης Σακελλαρίου, ΕΚΕΤΑ
Γεώργιος Σπανός, ΕΚΕΤΑ
Αβραάμ Τεπελίδης, ΕΚΕΤΑ
Γεώργιος Χαρμάνας, ΕΚΕΤΑ

Υπεύθυνοι Συγγραφής
Απόστολος Νάσιου, ICOM
Δημήτριος Λασκαράτος, ICOM
Ήλια Πιέτρη, ICOM
Κωνσταντίνος Τσάκαλος, ICOM
Μαρία Τσαρουχά, ICOM
Μάριος Χαραλαμπίδης, ICOM
Στέλιος Γκούσκος, TERRACOM
Δήμητρα Καραδήμου ΟΠΑ
Γεώργιος Νταρζάνος ΟΠΑ
Αθανάσιος Παπαϊωάννου ΟΠΑ
Γεώργιος Σταμούλης ΟΠΑ

Ακρωνύμια

Ακρωνύμιο	Ορισμός
ABAC	Attribute Based Access Control
ACC	Access Control Contract
BaaS	Blockchain as a Service
BBSE	Blockchain-Based Search Engine
CF	Collaborative Filtering
CTR	Click-Through Rate
Dapps	Decentralized Applications
DHT	Distributed Hash Table
DIP	Developer Incentive Protocol
DLT	Distributed Ledger Technology
GB	Gradient Boosting
GBT	Gradient Boosting Tree
HLF	Hyperledger Fabric
ID	Identification
IoT	Internet of Things
KSI	Keyless Signature Infrastructure
MPC	Multi-Party Computation
NF	Nebulas Force
NR	Nebulas Rank
OAMC	Object Attribute Management Contract
P2P	Peer-to-Peer
PKG	Private Key Generator
PMC	Policy Management Contract
PR	Page Rank
QoE	Quality of Experience
QoS	Quality of Service
RS	Recommender System
SAMC	Subject Attribute Management Contract
SAN	Smart Advertising Network
SERP	Search Engine Results Pages
SSL	Secure Sockets Layer
TOR	The Onion Routing
UI	User Interface
WRS	Weighted Random Sampling
XGBoost	Extreme Gradient Boosting
ZKP	Zero-Knowledge Proof
EE	Ενότητα Εργασίας

Σύνοψη Παραδοτέου

Το παρόν έγγραφο αποτελεί παραδοτέο για το έργο IoTFeds, το οποίο χρηματοδοτείται από το Επιχειρησιακό Πρόγραμμα «Ανταγωνιστικότητα, Επιχειρηματικότητα & Καινοτομία» (ΕΠΑνΕΚ) υπό τη δράση εθνικής εμβέλειας «Ερευνώ – Δημιουργώ – Καινοτομώ Β’ Κύκλος» του ΕΣΠΑ (2014-2020). Στόχος του παραδοτέου είναι η παρουσίαση των αποτελεσμάτων και των δραστηριοτήτων που έχουν ολοκληρωθεί μέχρι στιγμής στα πλαίσια της ΕΕ2 – «Ομοσπονδίες IoT και Διαλειτουργικότητα». Στόχος του έργου IoTFeds είναι να προτείνει μια λύση που επιτρέπει σε μικρές εταιρείες IoT (πάροχοι ή/και καταναλωτές δεδομένων IoT) να συνεργαστούν, ώστε να καλύψουν κοινές ανάγκες και συλλογικά να λειτουργήσουν μια ελεγχόμενη αγορά για την ανταλλαγή των IoT δεδομένων.

Για το σκοπό αυτό, το συγκεκριμένο παραδοτέο (Π2.2 – «Αναφορά Μηχανισμών Διαφήμισης, Ανακάλυψης και Ασφαλούς Πρόσβασης σε Πόρους IoT») επικεντρώνεται στην τεκμηρίωση του σχεδιασμού και της ανάπτυξης των προτεινόμενων μηχανισμών διαφήμισης κα ανακάλυψης πόρων, καθώς και των απαραίτητων μηχανισμών ασφαλείας για τη διαχείριση αυτών. Πιο συγκεκριμένα, το πρώτο κομμάτι του εγγράφου εκκινεί με την διερεύνηση του σχετικού τεχνολογικού πλαισίου και περιλαμβάνει την παρουσίαση και περιγραφή υφιστάμενων blockchain μηχανισμών ανακάλυψης και διαφήμισης πόρων, καθώς και λύσεις ασφαλούς πρόσβασης σε δεδομένα στο blockchain από τη σύγχρονη βιβλιογραφία. Σκοπός του συγκεκριμένου κεφαλαίου είναι η παρουσίαση μεθόδων που θα χρησιμοποιηθούν ως βάση για τη μετέπειτα υλοποίηση των αντίστοιχων μηχανισμών της IoTFeds πλατφόρμας.

Το υπόλοιπο μέρος του παραδοτέου Π2.2 εστιάζει την περιγραφή και την ανάλυση των βασικών μηχανισμών που καλούνται να υλοποιηθούν στα πλαίσια του έργου IoTFeds σχετικά με τη σύνθεση των προϊόντων δεδομένων και την ανακάλυψη, τη διαφήμιση, αλλά και την ασφαλή πρόσβαση σε αυτά. Η ανάλυση των μηχανισμών αυτών διακρίνεται σε ξεχωριστά κεφάλαια που παρουσιάζουν την ακριβή προσέγγιση που ακολουθήθηκε από κάθε βασικό σύστημα της IoTFeds πλατφόρμας (symbIoTe και BaaS).

Τέλος, το συγκεκριμένο έγγραφο ολοκληρώνεται με κάποια βασικά συμπεράσματα και μελλοντικές εργασίες για επόμενες δράσεις και ΕΕ.

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

1 Εισαγωγή

Στόχος του συγκεκριμένου παραδοτέου είναι η τεκμηρίωση του σχεδιασμού και της ανάπτυξης των μηχανισμών διαφήμισης και ανακάλυψης IoT πόρων μέσα σε μια ομοσπονδία, καθώς και των blockchain μηχανισμών ασφαλούς πρόσβασης και διαχείρισης πόρων IoT. Στις ενότητες που ακολουθούν γίνεται εξερεύνηση του τεχνολογικού υποβάθρου αναφορικά με υφιστάμενα συστήματα αναζήτησης και διαφήμισης πόρων, καθώς επίσης και μηχανισμών ασφαλούς πρόσβασης σε αυτούς. Στη συνέχεια, ακολουθεί αναλυτική περιγραφή των μηχανισμών που υλοποιούνται στα πλαίσια του έργου IoTFeds σχετικά με την αναζήτηση, διαφήμιση και ασφαλή πρόσβαση και διαχείριση πόρων και δεδομένων IoT.

1.1 Αντικείμενο του Παραδοτέου

Στο συγκεκριμένο παραδοτέο παρουσιάζονται εκτενώς οι προτεινόμενοι μηχανισμοί ανακάλυψης, διαφήμισης και ασφαλούς πρόσβασης σε πόρους και προϊόντα δεδομένων IoT, τα οποία διατίθενται μέσω της IoTFeds πλατφόρμας και των σχετικών αγορών αυτής.

Η ανάλυση των προαναφερθέντων μηχανισμών στο συγκεκριμένο παραδοτέο αποτελεί συνέχεια των μηχανισμών διαχείρισης των IoT ομοσπονδιών που περιγράφηκαν αναλυτικά στο προηγούμενο παραδοτέο Π2.1 – «Αναφορά Μηχανισμών Διαχείρισης Ομοσπονδιών IoT και Σημασιολογικής Διαλειτουργικότητας».

Αναλυτικότερα, οι βασικοί στόχοι που εκπληρώθηκαν στο συγκεκριμένο παραδοτέο είναι οι εξής:

- Μελέτη του τεχνολογικού υποβάθρου παρόμοιων μηχανισμών, καθώς και υφιστάμενων αλγορίθμων.
- Περιγραφή και ανάλυση των μηχανισμών κατανεμημένης αναζήτησης και διαφήμισης πόρων και προϊόντων δεδομένων στην IoTFeds πλατφόρμα.
- Περιγραφή και ανάλυση των μηχανισμών ασφαλούς πρόσβασης σε δεδομένα, τόσο στο symbIoTe, όσο και στο BaaS, στα πλαίσια της IoTFeds πλατφόρμας.

Το παραδοτέο αυτό περιγράφει τους ενημερωμένους μηχανισμούς και διεπαφές που εμπλέκονται στις δραστηριότητες των Δ2.3 και Δ2.4 και αφορούν τα ενδιάμεσα λογισμικά Blockchain as a Service (BaaS) και symbIoTe, όπως αυτά υλοποιήθηκαν, τροποποιήθηκαν ή και επεκτάθηκαν στα πλαίσια αυτών. Πιο συγκεκριμένα, όπως αναφέρθηκε και σε προηγούμενα παραδοτέα, οι επεκτάσεις του υποσυστήματος BaaS εντοπίζονται στην υλοποίηση κατάλληλων έξυπνων συμβολαίων για τη διαχείριση IoT δεδομένων, παρόχων, ομοσπονδιών, αλλά και αγορών δεδομένων, ενώ αντίστοιχα, το ήδη υπάρχον ενδιάμεσο λειτουργικό symbIoTe επεκτείνεται ώστε να υποστηρίζεται η συνδεσιμότητά του με τα έξυπνα συμβόλαια του BaaS.

1.2 Υπόβαθρο

Το υπόβαθρο για το συγκεκριμένο παραδοτέο του έργου IoTFeds σχετίζεται με τις προηγούμενες δύο δράσεις (Δ2.1 – «Διαχείριση Ομοσπονδίας IoT» της ΕΕ2 και Δ1.3 – «Αρχιτεκτονική Συστήματος και Τεχνολογίες» της ΕΕ1) και παραδοτέα (Π2.1 – «Αναφορά Μηχανισμών Διαχείρισης Ομοσπονδιών IoT και Σημασιολογικής Διαλειτουργικότητας» και Π1.3 – «Τελική Αρχιτεκτονική Συστήματος και Επιλεγμένες Τεχνολογίες»).

Πιο συγκεκριμένα, το παραδοτέο Π2.2 προκύπτει από τις δραστηριότητες της ΕΕ2 – «Ομοσπονδίες IoT και Διαλειτουργικότητα», όπου περιλαμβάνονται οι ακόλουθοι στόχοι σε αντιστοίχιση με τις ορισμένες δράσεις:

- Σχεδιασμός και ανάπτυξη μηχανισμών για τη διαχείριση μιας ομοσπονδίας IoT (Δ2.1).
- Σχεδιασμός και ανάπτυξη μηχανισμών για τη σημασιολογική διαλειτουργικότητα μεταξύ των ετερογενών πλατφορμών IoT (Δ2.2).
- Σχεδιασμός και ανάπτυξη μηχανισμών για την κατανεμημένη διαφήμιση και ανακάλυψη ομόσπονδων πόρων IoT (Δ2.3).
- Σχεδιασμός και ανάπτυξη μηχανισμών για την ασφαλή και ελεγχόμενη πρόσβαση στους πόρους IoT (Δ2.4).
- Σχεδιασμός και ανάπτυξη μηχανισμών φήμης και εμπιστοσύνης για την εύρυθμη λειτουργία της ομοσπονδίας IoT (Δ2.5).

1.3 Δομή του Παραδοτέου

Ολοκληρώνοντας την εισαγωγή του παραδοτέου Π2.2, το υπόλοιπο κείμενο δομείται ως εξής:

- Το Κεφάλαιο 2 περιλαμβάνει τη μελέτη και εξερεύνηση της πρόσφατης βιβλιογραφίας αναφορικά με παρόμοιους μηχανισμούς ανακάλυψης πόρων, διαφήμισης και ασφαλούς πρόσβασης σε δεδομένα, καθώς επίσης και υφιστάμενων αλγορίθμων ταξινόμησης για την υλοποίηση του μηχανισμού διαφήμισης.
- Το Κεφάλαιο 3 περιλαμβάνει την περιγραφή των μηχανισμών κατανεμημένης αναζήτησης της IoTFeds πλατφόρμας, παρουσιάζοντας τόσο τους μηχανισμούς και τα κριτήρια αναζήτησης στο υποσύστημα symbIoTe, όσο και τους μηχανισμούς κατανεμημένης αναζήτησης που υλοποιούνται από το υποσύστημα BaaS. Στο συγκεκριμένο κεφάλαιο παρουσιάζονται μόνο οι μηχανισμοί αναζήτησης ομόσπονδων πόρων IoT.
- Το Κεφάλαιο 4 σχετίζεται με την περιγραφή των μηχανισμών διαφήμισης ομόσπονδων πόρων IoT της IoTFeds πλατφόρμας, περιλαμβάνοντας επιπλέον και τον τρόπο αλληλεπίδρασής τους με μηχανισμούς φήμης και εμπιστοσύνης. Τονίζεται ότι στο συγκεκριμένο κεφάλαιο γίνεται αναφορά μόνο στους μηχανισμούς διαφήμισης ομόσπονδων πόρων IoT.
- Το Κεφάλαιο 5 περιγράφει τον τρόπο σύνθεσης των προϊόντων στην IoTFeds πλατφόρμα.
- Το Κεφάλαιο 6 περιλαμβάνει την περιγραφή των μηχανισμών αναζήτησης προϊόντων στην IoTFeds πλατφόρμα, παρουσιάζοντας τους αντίστοιχους μηχανισμούς που παρέχονται τόσο από το off-chain (marketplace), όσο και από το on-chain σύστημα (BaaS).
- Το Κεφάλαιο 7 παρουσιάζει τους μηχανισμούς που έχουν αναπτυχθεί τόσο off-chain (marketplace), όσο και on-chain (BaaS) για τη διαφήμιση των προϊόντων στην IoTFeds πλατφόρμα. Στο τέλος του συγκεκριμένου κεφαλαίου παρέχεται και ένα διάγραμμα ακολουθίας που περιγράφει τη ροή όλης της διαδικασίας αναζήτησης και διαφήμισης προϊόντων.
- Το Κεφάλαιο 8 περιλαμβάνει την περιγραφή των μηχανισμών ασφαλούς πρόσβασης σε δεδομένα IoT, οι οποίοι διατίθενται από τα βασικά συστήματα της IoTFeds πλατφόρμας (symbIoTe και BaaS) και περιλαμβάνουν μηχανισμούς ABAC, καθώς και έξυπνα συμβόλαια βάσει χρονικών περιορισμών.
- Τέλος, το Κεφάλαιο 9 παρέχει γενικά συμπεράσματα για τον τρόπο που τα αποτελέσματα αυτού του παραδοτέου θα χρησιμοποιηθούν σε επόμενα στάδια εργασιών καθώς συνεχίζει η υλοποίηση της IoTFeds πλατφόρμας και ολοκληρώνεται το αντίστοιχο έργο.

2 Εξερεύνηση Τεχνολογικού Υποβάθρου

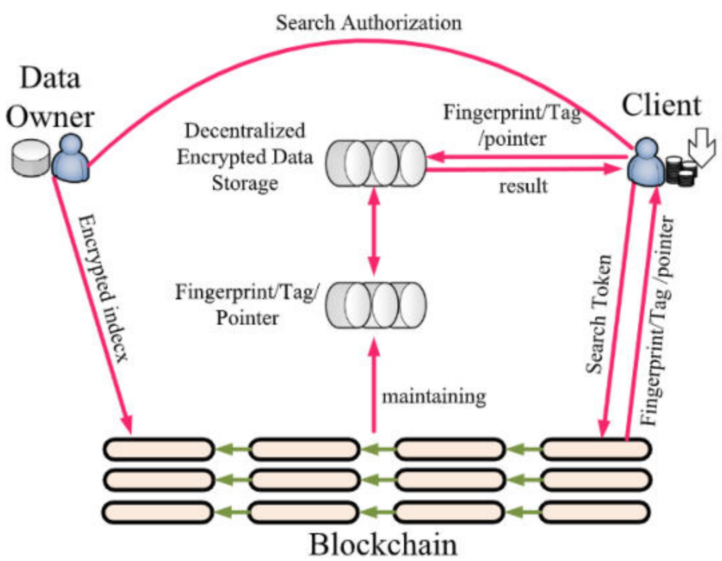
Στο συγκεκριμένο κεφάλαιο του παραδοτέου παρέχεται μια σύντομη περιγραφή βασικών blockchain μηχανισμών αναζήτησης και ανακάλυψης πόρων, διαφήμισης, καθώς επίσης και ασφαλούς πρόσβασης σε δεδομένα, όπως αυτοί παρουσιάζονται στη σχετική βιβλιογραφία. Η ανάλυση των συγκεκριμένων μηχανισμών έχει ως στόχο την παρουσίαση του ερευνητικού πλαισίου που θα αποτελέσει την βάση για τη μετέπειτα υλοποίηση των αντίστοιχων μηχανισμών της πλατφόρμας IoTFeds.

2.1 Blockchain Μηχανισμοί Ανακάλυψης Πόρων

Οι μηχανές αναζήτησης (search engines) αποτελούν τα ισχυρότερα εργαλεία που παρέχονται στο χρήστη για την αναζήτηση πληροφοριών στο Διαδίκτυο. Δεδομένου ότι τα παραδοσιακά συστήματα αναζήτησης δεν είναι πλέον επαρκή και κατάλληλα για τη διαχείριση του μεγάλου όγκου των online δεδομένων, προτάθηκε η σημασιολογική αναζήτηση, της οποίας σκοπός είναι η χρήση νοήματος για τη βελτίωση της εμπειρίας αναζήτησης του χρήστη (Sudeepthi, Anuradha, & Babu, 2012). Οι μηχανές αναζήτησης επίσης κατατάσσονται σε κεντρικοποιημένες (centralized), που είναι η πιο ευρεία κατηγορία αλλά ενέχει περιορισμούς, και αποκεντρικοποιημένης (decentralized), όπως αυτές αναλύονται στην υπο-ενότητα 2.1.2.

2.1.1 Κατανεμημένη Αναζήτηση στο Blockchain

Κατά τη διαδικασία της αναζήτησης σε ένα blockchain δίκτυο, το κρυπτογραφημένο σύνολο δεδομένων αποθηκεύεται με κατανεμημένο και αποκεντρικοποιημένο τρόπο στη βάση (offline), ενώ η κρυπτογραφημένη λέξη-κλειδί, δακτυλικό αποτύπωμα ή ετικέτα ή δείκτης, διατηρείται στο blockchain δίκτυο (online), είτε στην περίπτωση που αυτό είναι ελεγχόμενης πρόσβασης (permissioned), είτε μη ελεγχόμενης πρόσβασης (permissionless). Ως αποτέλεσμα, η κρυπτογραφημένη λέξη-κλειδί μπορεί να χρησιμοποιηθεί για αναζήτηση των αντίστοιχων κρυπτογραφημένων εγγράφων που βρίσκονται στην κατανεμημένη βάση δεδομένων, σύμφωνα με τη διαδικασία που περιγράφεται στην Εικόνα 1.



Εικόνα 1: Δομή συστημάτων αναζήτησης με λέξεις-κλειδιά (Tang, Lu, Xiang, Shi, & Gu, 2022).

2.1.1.1 Συστήματα Κατανεμημένης Αναζήτησης με Λέξεις-Κλειδιά

Η μελέτη των (Do & Ng, 2017) προτείνει την υλοποίηση ενός συστήματος ασφαλούς κατανεμημένης αναζήτησης που υποστηρίζει αναζήτηση βάσει λέξεων-κλειδιών σε μια κατανεμημένη βάση. Στη συγκεκριμένη προσέγγιση, στο blockchain δίκτυο δε γίνεται αποθήκευση δεδομένων, αλλά αντίθετα διατηρείται μόνο το δακτυλικό αποτύπωμα ώστε να επιτρέπεται κάθε φορά η σύνδεση του χρήστη στην υπηρεσία. Το προτεινόμενο σχήμα αναζήτησης ελέγχει αν η λέξη-κλειδί (δακτυλικό αποτύπωμα) αντιστοιχίζεται με το κρυπτογραφημένο κείμενο εντός των έξυπνων συμβολαίων ή των blockchain peers. Για τη διατήρηση της ασφάλειας των δεδομένων, το σύστημα αξιοποιεί τον αλγόριθμο «Proof of Retrievability» για τη διασφάλιση της ακεραιότητας των αποθηκευμένων δεδομένων και πραγματοποιεί ανώνυμο έλεγχο πρόσβασης για το χρήστη του συστήματος για να αποκτήσει διαπιστευτήρια. Ωστόσο, αξίζει να σημειωθεί ότι η συγκεκριμένη μελέτη δεν προσφέρει αξιολόγηση των προσφερόμενων αποτελεσμάτων και της συνολικής απόδοσης του προτεινόμενου συστήματος.

Μια άλλη μελέτη των (Tahir & Rajarajan, 2018) παρουσιάζει ένα νέο πλαίσιο για τη διατήρηση του απορρήτου των δεδομένων και τη βελτίωση της αποτελεσματικότητας της αναζήτησης λέξεων-κλειδιών σε κρυπτογραφημένα δεδομένα σε ένα permissioned δίκτυο blockchain. Το προτεινόμενο framework εγγυάται την ασφάλεια των δεδομένων καθ' όλη τη διαδικασία της αναζήτησης μέσω της ύπαρξης κατάλληλων έξυπνων συμβολαίων, οπότε εντοπίζεται και επιστρέφεται μόνο ένα σύνολο κρυπτογραφημένων αναγνωριστικών συναλλαγών, τα οποία πρέπει να αποκρυπτογραφηθούν για να ανακτηθεί το αναγνωριστικό της συναλλαγής. Ωστόσο, σε περίπτωση που επιστρέφονται πολλαπλά αναγνωριστικά συσχετισμένων συναλλαγών, απαιτείται η διαδοχική διέλευση των συσχετιζόμενων μπλοκ δεδομένων, γεγονός που απαιτεί πολύ χρόνο. Τέλος, και σε αυτή τη μελέτη δεν παρέχεται αξιολόγηση ή σύγκριση των αποτελεσμάτων με άλλες προσεγγίσεις, συνεπώς η απόδοση του συστήματος παραμένει άγνωστη.

Δεδομένου ότι πολλαπλά ερωτήματα μπορεί να κοστίζουν περισσότερο στον τελικό χρήστη του συστήματος, η μελέτη των (Jiang, Duan, & Wu, 2019) προτείνει ένα νέο συνεργατικό σχήμα αναζήτησης βασισμένο σε blockchain δίκτυα για αγορές δεδομένων. Στο συγκεκριμένο framework, το κόστος τιμολόγησης για κάθε ερώτημα (query) δίνεται είτε στον κάτοχο των δεδομένων, ο οποίος πληρώνεται για την ιδιοκτησία των δεδομένων που παρέχει, είτε στον πελάτη, ο οποίος ανταμείβεται με την εκτέλεση της αναζήτησης, χάρη στην εκτέλεση των έξυπνων συμβολαίων. Μέσω της ενσωμάτωσης πολλαπλών queries σε μια συγκεκριμένη ομάδα, το συνολικό κόστος του δικτύου μπορεί να μειωθεί, δεδομένου του περιορισμού ότι το εκάστοτε query δεν περιλαμβάνει μεγαλύτερο αριθμό λέξεων-κλειδιών σε σχέση με κάποιο από τα αρχικά (originals). Παρόλα αυτά, η συγκεκριμένη μελέτη εστιάζει μόνο σε συγκεκριμένες λέξεις-κλειδιά και δεν επιτρέπει το συνδυασμό και άλλων χαρακτηριστικών, όπως παράγοντες χώρου ή χρόνου.

Τέλος, στη μελέτη των (Cai, Weng, Yuan, & Wang, 2018) προτείνεται ένα δυναμικό σύστημα για τη διεξαγωγή κρυπτογραφημένης αναζήτησης με λέξεις-κλειδιά. Το προτεινόμενο framework διατηρεί τη θέση του αρχείου και της αντίστοιχης αναζήτησής του από το χρήστη, ώστε αυτά να βρίσκονται στην ίδια peer υπηρεσία και να επιτυγχάνεται ελαχιστοποίηση της επιβάρυνσης (overhead) της επικοινωνίας με το query της αναζήτησης. Επιπλέον, το προτεινόμενο σύστημα χρησιμοποιεί έξυπνα συμβόλαια για την καταγραφή των καταχωρήσεων (logs) της κρυπτογραφημένης αναζήτησης στο blockchain δίκτυο και προτείνει ένα δίκαιο πρωτόκολλο για τη διαχείριση τυχόν διαφορών που μπορεί να προκύψουν μεταξύ των χρηστών, αλλά και την έκδοση δίκαιων πληρωμών. Τέλος, συγκροτείται μια επιτροπή διαιτησίας με την προϋπόθεση ότι περισσότεροι από τα 2/3 των peers που συμμετέχουν είναι έμπιστοι.

2.1.2 Μηχανές Αναζήτησης Βασισμένες στο Blockchain

Όπως έχει ήδη αναφερθεί σε προηγούμενα παραδοτέα, το blockchain αποτελεί μία αλυσίδα (chain) από μπλοκ (blocks) δημιουργώντας ένα αποκεντρικοποιημένο δίκτυο όπου επιτυγχάνεται η ασφαλής αποθήκευση δεδομένων. Βασικά χαρακτηριστικά κάθε blockchain δικτύου αποτελούν η διαφάνεια, η δυνατότητα ελέγχου, η σταθερότητα και η αποκεντρικοποιημένη αρχιτεκτονική του, με αποτέλεσμα να αποτελεί ασφαλέστερη λύση σε σχέση με άλλα συμβατικά δίκτυα ή βάσεις δεδομένων (RapidInnovation, 2021). Για το λόγο αυτό αποτελεί την κατάλληλη πλατφόρμα για την ανάπτυξη μιας αποκεντρικοποιημένης μηχανής αναζήτησης ή Blockchain-Based Search Engine (BBSE).

Πιο συγκεκριμένα, μια BBSE βασίζεται σε ένα P2P δίκτυο και δε διαθέτει μόνο έναν διακομιστή, αλλά οι επιμέρους εργασίες κατανέμονται μεταξύ πολλών ομότιμων κόμβων (peers) με αποκεντρικοποιημένο τρόπο, σε αντίθεση με τις κεντρικοποιημένες μηχανές αναζήτησης. Όταν πραγματοποιείται μια αναζήτηση από το χρήστη, το σύστημα πραγματοποιεί αναζήτηση στο κατάστιχο (ledger), εμφανίζει τα αποτελέσματα στο χρήστη και, στη συνέχεια, τα στοιχεία της συγκεκριμένης αναζήτησης κωδικοποιούνται και αποθηκεύονται στον ledger.

Καθώς η συγκεκριμένη κατηγορία μηχανών αναζήτησης προτάθηκε για την αντιμετώπιση προβλημάτων απορρήτου που παρουσιάζονται σε κεντρικοποιημένες μηχανές αναζήτησης, τα βασικά τους πλεονεκτήματα μπορούν να περιγραφούν ως εξής:

- *Αποκεντρικοποίηση:* Λόγω του συγκεκριμένου χαρακτηριστικού του blockchain δικτύου, και οι BBSE, κατ' επέκταση, είναι κατανεμημένες σε διάφορους διακομιστές, με αποτέλεσμα να μην επιτρέπεται ο κεντρικοποιημένος έλεγχος των δεδομένων.
- *Ανωνυμία:* Καμία οντότητα του δικτύου δε δύναται να διεκδικήσει δεδομένα χρηστών ή να παραβιάσει την ασφάλεια του δικτύου. Το συγκεκριμένο πλεονέκτημα σχετίζεται επίσης με το αντίστοιχο χαρακτηριστικό του blockchain δικτύου. Επιπρόσθετα, οι BBSE παρέχουν στους χρήστες ιδιωτικά κλειδιά για τη διασφάλιση των δεδομένων τους.
- *Αμεροληψία:* Οι συγκεκριμένες μηχανές αναζήτησης είναι αμερόληπτες και δε διαστρεβλώνονται από πολιτικές ή επί πληρωμή διαφημίσεις.

Στις υπο-ενότητες που ακολουθούν παρουσιάζονται κάποιες υπάρχουσες λύσεις BBSE, οι οποίες ωστόσο βρίσκονται ακόμα σε πρώιμο στάδιο ανάπτυξης.

2.1.2.1 Nebulas

Το Nebulas προτάθηκε ώστε να επιτρέπει σε όλους τους χρήστες να επωφεληθούν δίκαια από μια αποκεντρικοποιημένη συνεργασία (Nebulas, 2017). Η συγκεκριμένη μηχανή αναζήτησης περιλαμβάνει ένα δίκτυο blockchain που χρησιμοποιείται για την αναζήτηση (indexing) και την ταξινόμηση των αποκεντρικοποιημένων εφαρμογών (decentralized applications, Dapps), έξυπνων συμβολαίων, πληροφοριών, καθώς και εξωτερικών δικτύων blockchain.

Το συγκεκριμένο framework εισήγαγε νέες τεχνολογίες όπως το Nebulas Rank (NR), το οποίο είναι ένα εργαλείο που επιτρέπει στους χρήστες να αναζητούν και να χρησιμοποιούν πολύτιμες πληροφορίες μέσα στο εκάστοτε blockchain δίκτυο. Πιο συγκεκριμένα, το NR ανέπτυξε μία μετρική που επιτρέπει την ταξινόμηση των blockchain εφαρμογών βάσει μιας καθολικής μέτρησης της αξίας τους, κατατάσσοντας διευθύνσεις, έξυπνα συμβόλαια, Dapps και άλλες blockchain οντότητες που βασίζονται στη ρευστότητα, τη διάδοση περιουσιακών στοιχείων και τη διαδραστικότητα μεταξύ των χρηστών, χρησιμοποιώντας αρχεία on-chain συναλλαγών. Άλλες τεχνολογίες που επίσης περιλαμβάνονται στο Nebulas framework είναι το Developer Incentive Protocol (DIP), το Nebulas Force (NF), καθώς επίσης και η προσέγγισή του για το on-chain consensus που καλείται Proof of Devotion.

2.1.2.2 BitClave

Το BitClave αποτελεί μια ανοιχτή, δημόσια και αποκεντρικοποιημένη πλατφόρμα που επιτρέπει στους χρήστες να χρησιμοποιούν και να μοιράζονται τα δεδομένα τους με επιλεκτικό τρόπο (BitClave, 2017). Η συγκεκριμένη πλατφόρμα επιτρέπει την άμεση επικοινωνία μεταξύ πελάτη και επιχείρησης, χωρίς την ύπαρξη κάποιου μεσάζοντα, καθώς οι τελικοί χρήστες, οι επιχειρήσεις και όλα τα μέλη του δικτύου αποτελούν τους βασικούς συμμετέχοντες της πλατφόρμας. Επιπλέον, οι τελικοί χρήστες ελέγχουν την ταυτότητά τους καθώς και ποιος έχει πρόσβαση στα δεδομένα τους. Ταυτόχρονα, καθώς το BitClave παρέχει στους χρήστες άκρως στοχευμένες προωθήσεις βάσει προσωπικών πληροφοριών που κοινοποιούν οι ίδιοι οικειοθελώς, μπορούν να εξοικονομήσουν χρόνο λαμβάνοντας προσφορές που ταιριάζουν ιδανικά στις ανάγκες τους.

Η λύση του BitClave επιτρέπει σε μεγάλες και μικρές επιχειρήσεις να συνεργάζονται σε ένα οικοσύστημα. Χάρη την προτεινόμενη τεχνολογία αναζήτησης που επιτρέπει στους πωλητές να πληρώνουν απευθείας για τα αποτελέσματα, οι χρήστες και οι πάροχοι δεδομένων ανταμείβονται για την αξία των δεδομένων τους, η οποία καθορίζεται βάσει μετατροπών και όχι κλικ. Οι καταναλωτές της πλατφόρμας επωφελούνται από ανταμοιβές σε μετρητά και αγορά εμπορευμάτων σε χαμηλότερο κόστος, ενώ παράλληλα έχουν οι ίδιοι τον έλεγχο των δεδομένων τους.

Συνεπώς, η τεχνολογία του BitClave επιτρέπει τον επαναπροσδιορισμό μιας πιο ανοιχτής και ουσιαστικής πλατφόρμας για άτομα και εταιρίες, ενώ παράλληλα επιτρέπει την επεκτάσιμη, ασφαλή και ανώνυμη αναζήτηση ενός μεγάλου συνόλου δεδομένων, καθώς και τη διασφάλιση αυτών.

2.1.2.3 Presearch

Το Presearch αποτελεί ένα πλήρες οικοσύστημα για την υποστήριξη του token PRE και την παροχή υπηρεσιών αποκεντρικοποιημένης αναζήτησης (PreSearch, 2017). Το συγκεκριμένο οικοσύστημα περιλαμβάνει tokens έρευνας, υπηρεσίες αποκεντρικοποιημένης αναζήτησης, κόμβους Presearch, την αγορά Presearch, καθώς και το Ethereum blockchain.

Στην περίπτωση των κεντρικοποιημένων μηχανών αναζήτησης, οι χρήστες χάνουν την κυριότητα των προσωπικών τους δεδομένων, ενώ αντίθετα στην πλατφόρμα του Presearch, οι αναζητήσεις δημιουργούν tokens για τον εκάστοτε χρήστη που εκτελεί τη συγκεκριμένη αναζήτηση, είτε τα προσωπικά του δεδομένα είναι δημόσια είτε όχι. Κάθε χρήστης της πλατφόρμας μπορεί να λαμβάνει token επιβράβευσης κατά την αναζήτηση ως μέλος της ομάδας Presearch ή προσκαλώντας και νέα μέλη να ενταχθούν στην πλατφόρμα.

Ένα επιπλέον χαρακτηριστικό της συγκεκριμένης πλατφόρμας αποτελούν και οι διαφανείς διαφημίσεις. Λόγω της μεγάλης σημασίας του τρόπου διενέργειας της αναζήτησης από την πλευρά του χρήστη, η οποία βασίζεται σε μεγάλο βαθμό στη λέξη-κλειδί που εισάγεται, η πλατφόρμα Presearch δύναται να προσελκύσει αγοραστές και να εκκινήσει την κυκλοφορία ενός δικτύου διαφήμισης staking λέξεων-κλειδιών.

2.1.3 Μηχανές Αναζήτησης Βασισμένες στο Blockchain σε Ευφυή Περιβάλλοντα

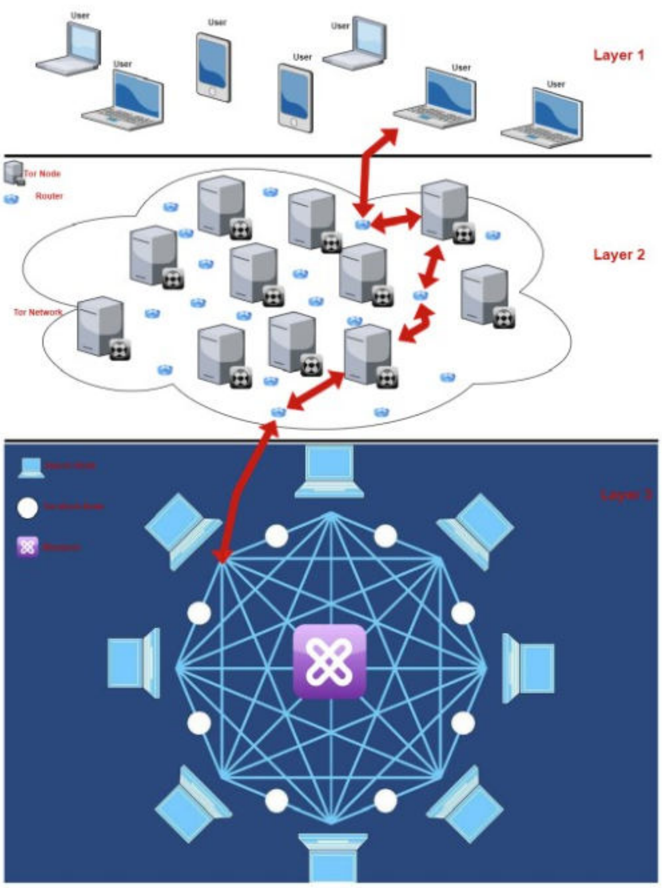
Στην περίπτωση των ευφυών συστημάτων, οι μηχανές αναζήτησης διαφέρουν αρκετά σε σχέση με τις περιπτώσεις που παρουσιάστηκαν στην προηγούμενη υπο-ενότητα 2.1.2. Η ετερογένεια, η αλληλεπίδραση με άλλες εφαρμογές, ο τεράστιος αριθμός πρωτοκόλλων ανταλλαγής δεδομένων, αλλά και το απόρρητο των δεδομένων αποτελούν κρίσιμες προκλήσεις για ένα ευφυές περιβάλλον (Matz & Götz, 2020). Συνεπώς, στα συγκεκριμένα περιβάλλοντα είναι απαραίτητο ένα κατανεμημένο σύστημα αναζήτησης το οποίο θα δύναται να παρέχει εξατομικευμένα και με επίγνωση του περιβάλλοντος (context-aware) αποτελέσματα.

Λύση στο συγκεκριμένο πρόβλημα μπορεί να δοθεί από τις BBSE λόγω της παροχής εξατομικευμένων αποτελεσμάτων αναζήτησης. Όπως προαναφέρθηκε, βασικό πρόβλημα στις ευφυείς εφαρμογές αποτελούν η αποκάλυψη των δεδομένων των χρηστών και η παραβίαση του απορρήτου τους, τα οποία ωστόσο φαίνεται να λύνονται με την ενσωμάτωση των BBSE, οι οποίες επιτρέπουν πλέον την κρυπτογράφηση των δεδομένων αυτών και την τοπική τους επεξεργασία.

2.1.3.1 Κατανεμημένη Ανώνυμη Αναζήτηση

Μια λύση στα προβλήματα ασφαλείας στις μηχανές αναζήτησης δίνεται από τους (Raza, Han, & Hwang, 2020) με την υλοποίηση μιας κατανεμημένης μηχανής αναζήτησης που προσφέρει ασφάλεια, ιδιωτικότητα και ανωνυμία στους χρήστες της. Πιο συγκεκριμένα, για το σχεδιασμό του προτεινόμενου framework χρησιμοποιήθηκαν οι τεχνολογίες του κατανεμημένου καθολικού (distributed ledger), καθώς και η τεχνική του onion routing (TOR) για τη διασφάλιση της ανωνυμίας των χρηστών της πλατφόρμας. Επιπλέον, προτείνεται ένας νέος consensus αλγόριθμος που καλείται «Proof of Randomness» και αποτελεί ασφαλέστερη και αποδοτικότερη λύση σε σχέση με άλλους αλγορίθμους. Τέλος, παρέχεται ανάλυση της τελικής απόδοσης και παρεχόμενης ασφάλειας του προτεινόμενου framework, μέσω προσομοιώσεων.

Όσον αφορά την αρχιτεκτονική της προτεινόμενης λύσης, το μοντέλο αποτελείται από τέσσερις διαφορετικούς τύπους συμμετεχόντων, το χρήστη, τους κόμβους TOR, τους κόμβους αναζήτησης και τους μπλοκ κόμβους TOR. Όπως φαίνεται και στην Εικόνα 2, το συνολικό μοντέλο διακρίνεται σε τρία επιμέρους εννοιολογικά επίπεδα. Πιο συγκεκριμένα, το επίπεδο 1 αποτελείται από τους χρήστες, το επίπεδο 2 αποτελείται από τους κόμβους TOR, ενώ το επίπεδο 3 περιλαμβάνει τους κόμβους αναζήτησης και τους μπλοκ κόμβους TOR.



Εικόνα 2: Γενικό μοντέλο αρχιτεκτονικής του προτεινόμενου framework για κατανεμημένη ανώνυμη αναζήτηση (Raza, Han, & Hwang, 2020).

Παράλληλα, για κάθε έναν από τους συμμετέχοντες του συστήματος ορίζεται και ένας διαφορετικός ρόλος. Αναλυτικότερα, ως χρήστης μπορεί να θεωρηθεί οποιοσδήποτε επιθυμεί να αναζητήσει περιεχόμενο στην προτεινόμενη μηχανή αναζήτησης μέσω του προγράμματος περιήγησης. Οι χρήστες συνδέονται με τους κόμβους TOR του επιπέδου 2 μέσω των ειδικά σχεδιασμένων προγραμμάτων περιήγησης που χρησιμοποιούν. Από την άλλη πλευρά, βασικός σκοπός των κόμβων TOR είναι η υλοποίηση του onion routing, όπου το αίτημα κάθε χρήστη δρομολογείται από τους κόμβους στο mempool στο επίπεδο 3. Οι συγκεκριμένοι κόμβοι μεταφέρουν τις σελίδες-αποτελέσματα αναζήτησης (Search Engine Results Pages, SERP) στο χρήστη, από το επίπεδο 3 στο επίπεδο 1. Τέλος, όσον αφορά το επίπεδο 3, οι κόμβοι αναζήτησης εκτελούν αναζήτηση για αποτελέσματα σχετικά με query κάθε συναλλαγής, ενώ οι μπλοκ κόμβοι TOR εμπλέκονται στο Proof of Randomness για την ολοκλήρωση της ταξινόμησης των παρεχόμενων στο χρήστη αποτελεσμάτων.

2.2 Μηχανισμοί Διαφήμισης Ομόσπονδων Πόρων

Οι τεχνικές εξελίξεις στον τομέα του IoT και της ασύρματης τεχνολογίας νέας γενιάς συμβάλλουν στην αναδιαμόρφωση της βιομηχανίας διαφήμισης (Zhu, et al., 2019). Πιο συγκεκριμένα, τα συστήματα διαφημίσεων ή προτάσεων που είναι βασισμένα σε blockchain δίκτυα συμβάλλουν στην αποτελεσματικότερη προσέγγιση των καταναλωτών από τους εκάστοτε παρόχους, συμβάλλοντας ταυτόχρονα και στη διατήρηση της ανωνυμίας των χρηστών, καθώς και των προσωπικών τους δεδομένων.

2.2.1 Διαφήμιση σε Ομοσπονδίες

Ένα θεμελιώδες ζήτημα που εντοπίζεται στις ψηφιακές διαφημίσεις είναι η συχνή αδυναμία της επαλήθευσης της προβολής της συγκεκριμένης διαφήμισης, το οποίο μπορεί να επιλυθεί με τη σχεδίαση μιας υποδομής κατανεμημένου καθολικού (Distributed Ledger Technology, DLT), η οποία θα εξυπηρετεί τόσο τους παρόχους όσο και τους καταναλωτές (Joo, Kim, Ghose, & Wilbur, 2022). Με αυτόν τον τρόπο, η επαλήθευση της προβολής της εκάστοτε διαφήμισης δεν είναι συνυφασμένη με τα οικονομικά κίνητρα του αντίστοιχου παρόχου, με αποτέλεσμα το φαινόμενο του αποκλεισμού των διαφημίσεων να μετριάζεται.

Τα βασικά χαρακτηριστικά ενός συστήματος διαφήμισης βασισμένο σε DLT είναι τα εξής:

- *Δομή:* Σχετίζεται με το ποιον καλείται να εξυπηρετήσει τελικά το προτεινόμενο δίκτυο.
- *Συμμετοχή και Διακυβέρνηση:* Σχετίζεται με το ποιος κατέχει, ελέγχει και συντηρεί το τελικό προτεινόμενο δίκτυο.
- *Διαφάνεια:* Σχετίζεται με το ποιος έχει δυνατότητα να παρακολουθεί τα παρεχόμενα δεδομένα.
- *Όροι Ανταλλαγών:* Σχετίζεται με τις αγοραπωλησίες που πραγματοποιούνται ενός του δικτύου από τους χρήστες, καθώς και τον αντίστοιχο τρόπο και σκοπό κάθε αγοραπωλησίας.

Στις υπο-ενότητες που ακολουθούν παρουσιάζονται τα χαρακτηριστικά και η αρχή λειτουργίας των δύο βασικών κατηγοριών δικτύων που χρησιμοποιούνται για διαφημίσεις στα blockchain δίκτυα, έξυπνα δίκτυα διαφήμισης (Smart Advertising Networks, SANs) και τα δίκτυα προτάσεων (Recommender Systems, RSs).

2.2.1.1 Δίκτυα Διαφήμισης Βασισμένα σε Blockchain

Ένα έξυπνο δίκτυο διαφήμισης από συνδεδεμένα ευφυή αντικείμενα, όπως έξυπνα οχήματα ή οικιακές συσκευές, μπορεί να συμβάλλει στην αποτελεσματικότερη προσέγγιση των καταναλωτών από τους εκάστοτε παρόχους μέσω των αντίστοιχων διαφημιστικών καναλιών. Παράλληλα, χάρη στο μεγάλο όγκο των δεδομένων που περιλαμβάνονται στα συγκεκριμένα δίκτυα, κάθε πάροχος μπορεί να δημιουργήσει συμπεριφορικά προφίλ για κάθε χρήστη για την παροχή εξατομικευμένων διαφημίσεων.

Πρακτικά, η διαχείριση ενός δικτύου διαφημίσεων γίνεται από έναν τρίτο διαμεσολαβητή (broker), ο οποίος είναι υπεύθυνος για τη συλλογή όλων των συμπεριφορικών δεδομένων κάθε χρήστη του δικτύου και τη δημιουργία των αντίστοιχων προφίλ προτιμήσεων τους (Liu, Huang, Ni, Lin, & Shen, 2020). Παράλληλα, οι πάροχοι δεδομένων έχουν τη δυνατότητα επιλογής ενός συνόλου λέξεων-κλειδιών ως πολιτικές στόχευσης, ενώ στη συνέχεια βασίζονται στον ενδιάμεσο broker για τη μετάδοση των διαφημίσεων των προϊόντων τους στον τελικό ενδιαφερόμενο χρήστη. Με την ολοκλήρωση της διάδοσης των διαφημίσεων, ο broker χρεώνει ανά προβολή τους παρόχους σε περίπτωση που κάποιος χρήστης του δικτύου δει τη συγκεκριμένη διαφήμιση ή ανά κλικ σε περίπτωση που κάποιος χρήστης κάνει κλικ στο σύνδεσμο ανακατεύθυνσης της διαφήμισης.

Ωστόσο, το πρόβλημα της διαφημιστικής διαφάνειας εξακολουθεί να παραμένει ανοιχτή πρόκληση για τα έξυπνα δίκτυα διαφήμισης. Συνεπώς, για την ανάκτηση της εμπιστοσύνης των χρηστών του δικτύου, αρκετές μελέτες της σύγχρονης βιβλιογραφίας προτείνουν την παροχή κατάλληλων εργαλείων διαχείρισης προσωπικών προφίλ στους χρήστες από τον ενδιάμεσο broker. Επιπλέον, κάθε broker παρέχει στους χρήστες του δικτύου επιλογές «εξηγήσεων διαφάνειας» σχετικά με το λόγο που ο κάθε χρήστης μπορεί να λαμβάνει συγκεκριμένες διαφημίσεις. Ωστόσο, σε πολλές περιπτώσεις εξηγήσεις αυτού του τύπου παραμένουν ελλιπείς και άρα ανεπαρκείς για τους χρήστες. Για την αντιμετώπιση του συγκεκριμένου προβλήματος, έχουν μελετηθεί προσεγγίσεις που προτείνουν τη χρήση αξιόπιστου υλικού (Li, Li, Chen, & Xia, 2015), αλλά και επεκτάσεις διαφάνειας (Parra-Arnau, Achara, & Castelluccia, 2017) από την πλευρά του χρήστη ή εισάγουν έναν ανεξάρτητο οργανισμό για την ενίσχυση της διαφάνειας του συνολικού δικτύου (Venkatadri, Mislove, & Gummadi, 2018). Παρόλα αυτά, ακόμα και η ενιαία αρχή μπορεί να θεωρηθεί αναξιόπιστη σε ορισμένες περιπτώσεις ή να είναι δύσκολο να παρέχεται αποτελεσματική λογοδοσία έναντι του αντίστοιχου διαφημιστικού παραπτώματος. Ως αποτέλεσμα, είναι απαραίτητη η ύπαρξη μιας αποκεντρικοποιημένης αρχιτεκτονικής για την επιβολή δημόσιας επαληθεύσιμης διαφάνειας και την επιβολή αποτελεσματικής λογοδοσίας εντός του δικτύου.

Λύση στο συγκεκριμένο πρόβλημα μπορεί να δοθεί με τη σχεδίαση ενός κατανεμημένου consensus μηχανισμού (Liu & Chen, 2017). Καθώς το blockchain είναι ένας δημόσιος ledger που περιλαμβάνει μπλοκ από P2P συναλλαγές σε ένα πλήρως κατανεμημένο δίκτυο, έχει την ικανότητα να διασφαλίζει συνεπείς και διαφανείς προβολές με αποτέλεσμα να μπορεί να χρησιμοποιηθεί ως ένα αξιόπιστο περιβάλλον για την εκτέλεση έξυπνων συμβολαίων. Πιο συγκεκριμένα, ο broker μπορεί να αποθηκεύει όλες τις πολιτικές των παρόχων δεδομένων και να σχεδιάσει έξυπνα συμβόλαια για την υλοποίηση παράδοσης των διαφημίσεων στους τελικούς χρήστες. Με αυτό τον τρόπο, επιτυγχάνεται αφενός η αποκεντρικοποιημένη διαφάνεια του δικτύου και, αφετέρου, η αυτόματη λογοδοσία όλων των μελών του δικτύου κατά τον εντοπισμό οποιουδήποτε παραπτώματος.

2.2.1.2 Συστήματα Συστάσεων Βασισμένα σε Blockchain

Τα συστήματα συστάσεων, τα οποία αρχικά εμφανίστηκαν ως λύσεις εξατομίκευσης περιεχομένου για τον Ιστό, επεκτάθηκαν γρήγορα και εφαρμόστηκαν και σε άλλους τομείς IoT όπως η υγεία, οι έξυπνες πόλεις, η ευφυής γεωργία, κ.λπ. Συνεπώς, η ενσωμάτωση του IoT αύξησε και την ανάγκη ύπαρξης μεγάλου βαθμού εμπιστοσύνης στις δημιουργούμενες συστάσεις των δικτύων. Δεδομένου ότι η εμπιστοσύνη είναι μία από τις κύριες απαιτήσεις για την αποδοχή της τεχνολογίας των συστημάτων προτάσεων, καθίσταται ιδιαίτερα σημαντική η ύπαρξη εμπιστοσύνης τόσο στους παρόχους δεδομένων και τους χρήστες του δικτύου, ώστε να διασφαλίζεται η ύπαρξη αμεροληψίας (Mohammadi, Rahmani, Darwesh, & Sahafi, 2019), όσο και στους αλγορίθμους συστάσεων, για να είναι ανθεκτικοί σε κακόβουλες επιθέσεις (Du, και συν., 2018).

Η ύπαρξη του αποκεντρικοποιημένου ledger σε κάθε blockchain δίκτυο για την καταγραφή των συναλλαγών συμβάλλει στη διατήρηση της ανωνυμίας, της ακεραιότητας και της ασφάλειας των δεδομένων, καθιστώντας το ιδανικό περιβάλλον για την ανάπτυξη δικτύων προτάσεων. Καθώς στα συστήματα συστάσεων οι προτάσεις δημιουργούνται για κάθε χρήστη βάσει ιστορικών δεδομένων και αναζητήσεων, τα συστήματα αυτά συγκεντρώνουν τεράστιο όγκο δεδομένων χρηστών, τα οποία είναι, συνήθως, απόρρητα. Κατά συνέπεια, για τη διατήρηση του απορρήτου του χρήστη και την αύξηση της παρεχόμενης ασφάλειας από το δίκτυο, γίνεται χρήση διαφόρων κρυπτογραφικών στρατηγικών συμπεριλαμβανομένων των κρυπτογραφικών συναρτήσεων κατακερματισμού (cryptographic hash functions) (Lu, 2019), της κρυπτογραφίας δημόσιου κλειδιού (public key cryptography) (He, Yu, Zhang, & Bao, 2017) και των κρυπτογραφικών διευθύνσεων (Li, Barenji, & Huang, 2018).

Ένα από τα βασικά πλεονεκτήματα των συγκεκριμένων δικτύων είναι η ύπαρξη των αποκεντρικοποιημένων δεδομένων, χάρη στα οποία επιτυγχάνεται ελαχιστοποίηση του κινδύνου της πλήρους ανάκτησης του προφίλ ενός χρήστη ακόμα και σε περίπτωση που λίγοι ή ακόμα και ένας κόμβος του δικτύου παραβιαστεί. Οι υποδομές για υπογραφές χωρίς κλειδιά (Keyless Signature Infrastructures, KSIs) και τα SSL πιστοποιητικά που έχουν αναπτυχθεί για τα blockchain δίκτυα επιτρέπουν στους χρήστες την επαλήθευση της ακεραιότητας των δεδομένων και των υπογραφών τους χωρίς να χρειάζεται να αποκαλύψουν κάποιο κλειδί. Όλα τα παραπάνω, σε συνδυασμό και με την ανθεκτικότητα της αρχιτεκτονικής των δικτύων P2P, αποτελούν εγγυήσεις για ασφαλή και απρόσκοπτη επεξεργασία δεδομένων σε συστήματα προτάσεων (Niranjanamurthy, Nithya, & Jagannatha, 2019).

2.2.2 Αλγόριθμοι Ταξινόμησης Παρεχόμενων Αποτελεσμάτων

Η συνεχής χρήση των αγορών δεδομένων σε διάφορες εφαρμογές οδηγεί κατ’ επέκταση και στην ανάγκη ενσωμάτωσης κατάλληλων μηχανισμών ταξινόμησης (ranking) των προϊόντων που περιλαμβάνονται εντός της αγοράς της εκάστοτε πλατφόρμας (Demsyn-Jones, 2022). Καθώς οι μηχανές αναζήτησης αποτελούν βασικό κομμάτι μιας αγοράς δεδομένων (Joachims, et al., 2007), στόχος της χρήσης των συγκεκριμένων μηχανισμών είναι η βελτιστοποίηση του μηχανισμού διαφήμισης των προϊόντων της αγοράς δεδομένων, λαμβάνοντας υπόψη μετρικές όπως η συχνότητα εμφάνισης ενός συγκεκριμένου προϊόντος, η ημερομηνία καταχώρισής του στο σύστημα, η συχνότητα επιλογής του από άλλους καταναλωτές, η βαθμολογία του προϊόντος κ.ά.

Η εφαρμογή των κατάλληλων αλγορίθμων ταξινόμησης έχει διττό ρόλο σε ένα σύστημα, καθώς μπορεί να επιφέρει θετικά αποτελέσματα τόσο για το ίδιο το σύστημα, όσο και για τους χρήστες του συστήματος, οι οποίοι είναι σε θέση να αξιολογήσουν την ευρωστία των παρεχόμενων αποτελεσμάτων. Από τη μία πλευρά, ο πάροχος των δεδομένων επιθυμεί τα δεδομένα που παρέχει να εμφανίζονται όσο το δυνατόν σε περισσότερους καταναλωτές με όσο το δυνατόν υψηλότερη κατάταξη. Από την άλλη πλευρά, και οι ίδιοι οι χρήστες θα πρέπει να γνωρίζουν για τους αλγορίθμους ταξινόμησης που χρησιμοποιούνται από το σύστημα, προκειμένου να είναι σε θέση να αξιολογούν και οι ίδιοι την ευρωστία του συστήματος, καθώς και την ορθότητα των αποτελεσμάτων της αναζήτησής τους.

Επιπλέον, η χρήση των αλγορίθμων ταξινόμησης βοηθά τους καταναλωτές να υπολογίζουν τη χρησιμότητα των αποτελεσμάτων σε σχέση με την αναζήτηση και τα αποτελέσματα που περιμένουν οι ίδιοι. Για παράδειγμα, σε καταναλωτές που επιθυμούν να αγοράσουν περιβαλλοντικά δεδομένα για την περιοχή τους, το σύστημα θα πρέπει να επιστρέφει πρώτα τα πιο πρόσφατα αποτελέσματα ή τα αποτελέσματα που βρίσκονται σε κοντινότερη απόσταση με το χρήστη σε σχέση με όλα τα υπόλοιπα δεδομένα που περιλαμβάνονται στο σύστημα.

Συνεπώς, οι αλγόριθμοι ταξινόμησης έχουν ιδιαίτερη σημασία, κυρίως σε συστήματα αγορών, για διαφημίσεις, καθώς συμβάλλουν στην ταξινόμησης και την εμφάνιση των αποτελεσμάτων αναζήτησης των χρηστών της πλατφόρμας βάσει είτε συνάφειας, είτε δημοτικότητας, είτε κέρδους, ή ακόμα και συνδυασμού αυτών. Χάρη στους συγκεκριμένους αλγορίθμους καθορίζεται ποια στοιχεία ή ποιες υπηρεσίες είναι πιθανότερο να ενδιαφέρουν ένα χρήστη βάσει των κριτηρίων αναζήτησης που έχει εισάγει ο ίδιος ή βάσει της συμπεριφοράς της περιήγησής του στην πλατφόρμα. Ως αποτέλεσμα, οι αλγόριθμοι ταξινόμησης συμβάλλουν στην αύξηση της ορατότητας και της δυνατότητας ανακάλυψης προϊόντων ή υπηρεσιών, γεγονός που μπορεί να οδηγήσει σε υψηλότερες πωλήσεις και έσοδα από την πλευρά των παρόχων και αυξημένη ικανοποίηση από την πλευρά των καταναλωτών.

Στη σύγχρονη βιβλιογραφία διατίθεται πληθώρα αλγορίθμων ταξινόμησης, από τους οποίους οι πιο συνήθεις περιλαμβάνουν τους Page Rank, Collaborative Filtering και Gradient Boosting. Οι συγκεκριμένοι αλγόριθμοι αναλύονται στις υπο-ενότητες που ακολουθούν.

2.2.2.1 Page Rank

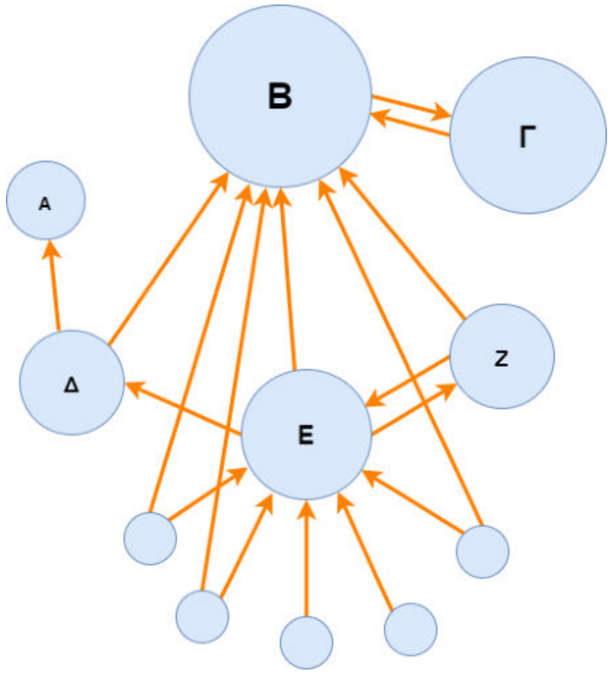
Ο αλγόριθμος Page Rank (PR) αποτελεί έναν αλγόριθμο ταξινόμησης που αναπτύχθηκε από την Google και μετρά τη σημασία και τη συνάφεια των ιστοσελίδων με βάση τον αριθμό και την ποιότητα των συνδέσμων που οδηγούν σε αυτές (Rogers, 2002). Πιο συγκεκριμένα, λειτουργεί αναλύοντας ένα web graph, το οποίο είναι ένας χάρτης συνδέσμων μεταξύ ιστοσελίδων.

Η αρχιτεκτονική του συγκεκριμένου αλγορίθμου ταξινόμησης περιλαμβάνει τις ακόλουθες μονάδες:

1. *Web graph:* Κατευθυντικός γράφος που αναπαριστά τη δομή των ιστοσελίδων και των μεταξύ τους συνδέσεων. Κάθε ιστοσελίδα αναπαρίσταται ως κόμβος του γράφου και οι μεταξύ τους συνδέσεις ως ακμές που συνδέουν τους κόμβους.
2. *Υπολογισμός κατάταξης ιστοσελίδας:* Περιλαμβάνει επαναληπτικό υπολογισμό μιας βαθμολογίας κατάταξης για κάθε ιστοσελίδα, η οποία βασίζεται στις αντίστοιχες βαθμολογίες των ιστοσελίδων που συνδέονται με αυτή. Ο υπολογισμός των βαθμολογιών αυτών περιλαμβάνει και έναν παράγοντα απόσβεσης (damping factor) που εμποδίζει τις βαθμολογίες να γίνουν πολύ ακραίες.
3. *Ενημέρωση κατάταξης ιστοσελίδας:* Οι βαθμολογίες κατάταξης ιστοσελίδας ενημερώνονται μετά από κάθε επανάληψη του υπολογισμού της κατάταξης της ιστοσελίδας. Η ενημέρωση της κατάταξής τους, περιλαμβάνει την αντικατάσταση των προηγούμενων βαθμολογιών με τις νέες βαθμολογίες.
4. *Αποτελέσματα αναζήτησης:* Οι βαθμολογίες κατάταξης μιας ιστοσελίδας χρησιμοποιούνται για την κατάταξη των αποτελεσμάτων αναζήτησης για ένα συγκεκριμένο κριτήριο. Οι σελίδες με τις υψηλότερες βαθμολογίες κατάταξης εμφανίζονται υψηλότερα στα αποτελέσματα αναζήτησης, υποδεικνύοντας ότι είναι πιο σχετικές και σημαντικές για το κριτήριο αναζήτησης.

Στην Εικόνα 3 παρουσιάζεται μια αναπαράσταση του γράφου του αλγορίθμου PR, όπου το μέγεθος κάθε κόμβου αναπαριστά τη βαθμολογία του. Η βαθμολογία σε κάθε ιστοσελίδα εκχωρείται με βάση τον αριθμό και την ποιότητα των ακμών που δείχνουν προς αυτήν, ενώ η ποιότητα μιας ακμής καθορίζεται από τη σημασία της ιστοσελίδας που περιέχει τη συγκεκριμένη ακμή. Ως αποτέλεσμα, οι ιστοσελίδες που κρίνονται σημαντικές λαμβάνουν μεγαλύτερη βαρύτητα (βάρος) στον υπολογισμό της βαθμολογίας κατάταξης, η οποία μεταβιβάζεται και στις ιστοσελίδες με τις οποίες αυτή συνδέεται. Παράλληλα, σημαντικό ρόλο στη βαθμολογία παίζει και ο αριθμός των εξερχόμενων ακμών. Ιστοσελίδες με πολλές εξερχόμενες ακμές μεταφέρουν μικρότερο βάρος σε κάθε μεμονωμένο κόμβο, ενώ αντίθετα ιστοσελίδες με λιγότερες εξερχόμενες ακμές μεταφέρουν μεγαλύτερο βάρος.

Βάσει όλων των παραπάνω, στον γράφο στην Εικόνα 3, η ιστοσελίδα B έχει την υψηλότερη βαθμολογία από τις υπόλοιπες ιστοσελίδες γιατί διαθέτει τις περισσότερες εισερχόμενες ακμές, ενώ η υψηλή βαθμολογία της ιστοσελίδας Γ οφείλεται στη μεταβίβαση βαθμολογίας από την ιστοσελίδα Β.



Εικόνα 3: Κατάταξη ιστοσελίδων από τον αλγόριθμο ταξινόμησης Page Rank.

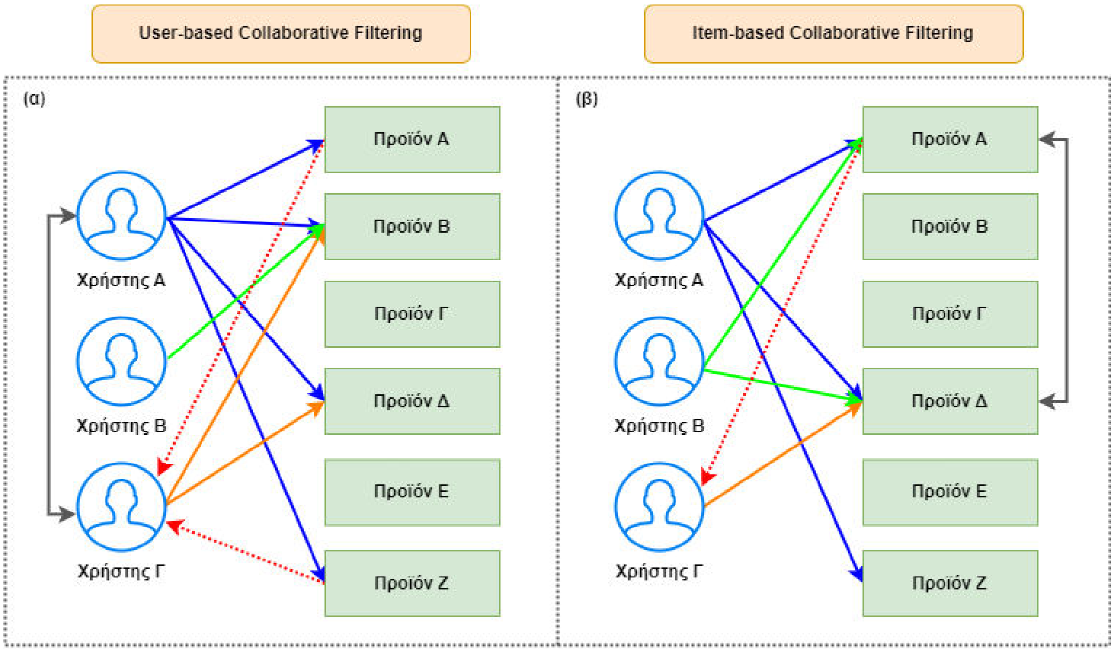
Ολοκληρώνοντας, η αρχιτεκτονική του συγκεκριμένου αλγορίθμου έχει σχεδιαστεί για να παρέχει έναν αποτελεσματικό και αποδοτικό τρόπο κατάταξης ιστοσελίδων με βάση της συνάφεια και τη σημασία τους σε ένα συγκεκριμένο κριτήριο αναζήτησης.

2.2.2.2 Συνεργατικό Φιλτράρισμα

Ο αλγόριθμος του Συνεργατικού Φιλτραρίσματος (Collaborative Filtering, CF) είναι ένας αλγόριθμος μηχανικής μάθησης που χρησιμοποιείται σε πλατφόρμες ηλεκτρονικού εμπορίου όπως η Amazon για να προτείνει προϊόντα στους καταναλωτές βάσει του ιστορικού περιήγησης και των προηγούμενων αγορών τους. Ο συγκεκριμένος αλγόριθμος αναλύει τα δεδομένα των καταναλωτών με στόχο τον προσδιορισμό συμπεριφορικών μοτίβων και προτιμήσεών τους και, στη συνέχεια, χρησιμοποιεί αυτές τις πληροφορίες για την παροχή εξατομικευμένων προτάσεων προϊόντων (Herlocker, Konstan, & Riedl, 2000).

Ο συγκεκριμένος αλγόριθμος μπορεί να διακριθεί σε δύο βασικούς τύπους, βάσει χρήστη (user-based) και βάσει προϊόντος (item-based). Πιο συγκεκριμένα, ο user-based αλγόριθμος προτείνει προϊόντα σε έναν χρήστη βάσει των προτιμήσεων άλλων χρηστών που έχουν παρόμοια χαρακτηριστικά με αυτόν. Η συγκεκριμένη διαδικασία περιλαμβάνει τον εντοπισμό χρηστών με παρόμοιες προτιμήσεις με αυτές του χρήστη-στόχου και τη σύσταση προϊόντων που έχουν επίσης αγοράσει και αυτοί οι χρήστες. Από την άλλη πλευρά, ο item-based αλγόριθμος συνιστά προϊόντα σε έναν χρήστη βάσει της ομοιότητάς τους με άλλα αντικείμενα που έχει επιλέξει ο συγκεκριμένος χρήστης στο παρελθόν. Η συγκεκριμένη διαδικασία περιλαμβάνει τον εντοπισμό παρόμοιων προϊόντων με εκείνα που είχε επιλέξει ο χρήστης στο παρελθόν και τη σύσταση αυτών στο χρήστη.

Ο αλγόριθμος CF λειτουργεί δημιουργώντας έναν πίνακα αλληλεπιδράσεων ενός χρήστη με ένα προϊόν, όπως φαίνεται στην Εικόνα 4, όπου κάθε σειρά αντιπροσωπεύει ένα χρήστη, κάθε στήλη αντιπροσωπεύει ένα προϊόν και οι εγγραφές αντιπροσωπεύουν την αλληλεπίδραση του χρήστη με το κάθε προϊόν (π.χ. μια βαθμολογία, μια αγορά ή μια προβολή). Ο συγκεκριμένος πίνακας χρησιμοποιείται στη συνέχεια για τον εντοπισμό προτύπων και τη διατύπωση προτάσεων με βάση τα μοτίβα αυτά. Στην Εικόνα 4 περιγράφονται δύο ενδεικτικά παραδείγματα διαφήμισης προϊόντων με χρήση CF, με βάση το χρήστη (α) και με βάση το προϊόν (β), και οι κόκκινες διακεκομμένες γραμμές αντιπροσωπεύουν τις προτάσεις του αλγορίθμου στους χρήστες.



Εικόνα 4: Διαφήμιση με χρήση του αλγορίθμου Συνεργατικού Φίλτρου: (α) user-based CF και (β) item-based CF.

Ολοκληρώνοντας, ο αλγόριθμος CF χρησιμοποιείται για την παροχή εξατομικευμένων προτάσεων στους χρήστες με βάση προηγούμενη συμπεριφορά τους και τις προτιμήσεις τους. Πρόκειται για έναν αλγόριθμο που χρησιμοποιείται ευρέως στο ηλεκτρονικό εμπόριο, στα μέσα κοινωνικής δικτύωσης και σε συστήματα προτάσεων για τη βελτίωση της αφοσίωσης και της ικανοποίησης των χρηστών.

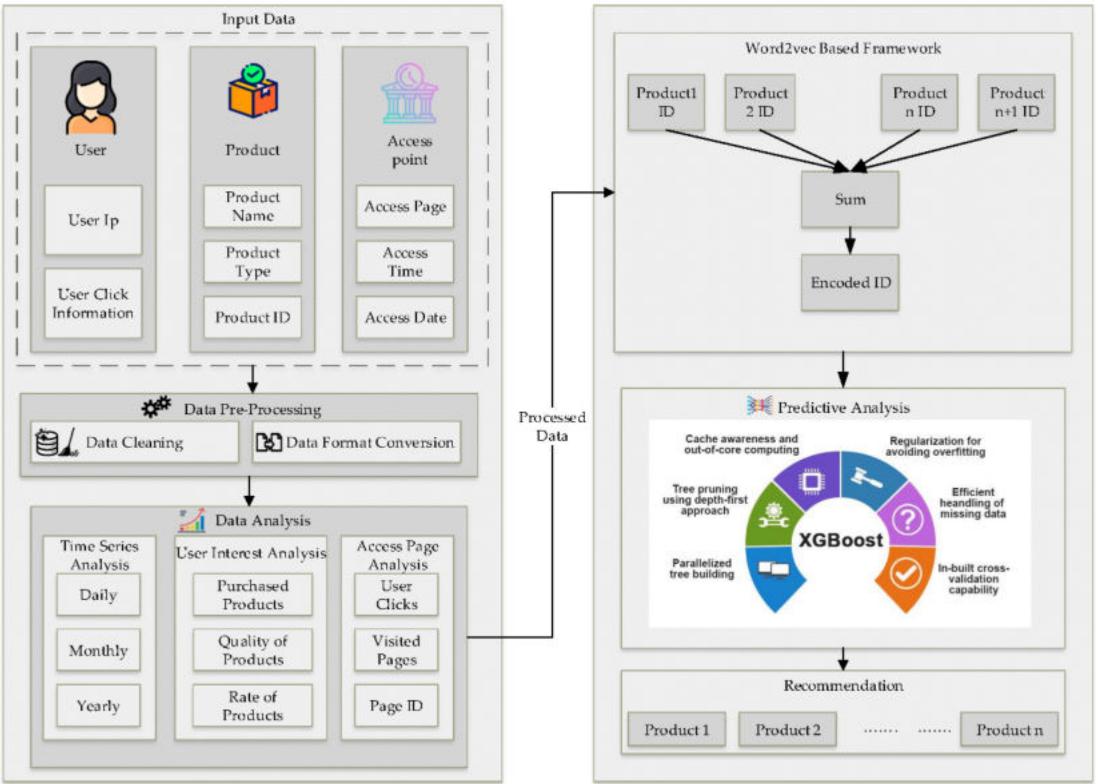
2.2.2.3 Gradient Boosting

Ο αλγόριθμος Gradient Boosting (GB) είναι ένας αλγόριθμος ταξινόμησης που επίσης χρησιμοποιείται στις διαδικτυακές διαφημίσεις. Προτείνεται για την πρόβλεψη της συμπεριφοράς των χρηστών με βάση προηγούμενα δεδομένα και χρησιμοποιείται συχνά για την πρόβλεψη της αναλογίας των κλικ προς τον αριθμό εμφανίσεων (Click-Through Rate, CTR) στις διαφημίσεις. Ο συγκεκριμένος αλγόριθμος ταξινόμησης είναι ιδιαίτερα αποτελεσματικός γιατί διαθέτει την ικανότητα εκμάθησης και προσαρμογής στις αλλαγές της συμπεριφοράς των χρηστών με την πάροδο του χρόνου, γεγονός που του επιτρέπει την εξαγωγή ακριβέστερων προβλέψεων και τη βελτίωση της συνάφειας των διαφημίσεων.

Σε εφαρμογές συστημάτων προτάσεων GB, συνήθως χρησιμοποιείται ένας πίνακας που περιλαμβάνει αλληλεπιδράσεις μεταξύ χρήστη και προϊόντος (user-item interactions), ο οποίος αναπαριστά το ιστορικό των αλληλεπιδράσεων ενός χρήστη με διαφορετικά προϊόντα. Ομοίως με τον αλγόριθμο CF, κάθε σειρά του συγκεκριμένου πίνακα αντιπροσωπεύει ένα χρήστη, κάθε στήλη αντιπροσωπεύει ένα προϊόν και οι εγγραφές αντιπροσωπεύουν την αλληλεπίδραση του χρήστη με το προϊόν (π.χ. αξιολόγηση ή αγορά του προϊόντος). Στη συνέχεια, γίνεται χρήση του πίνακα αυτού για την εκπαίδευση ενός μοντέλου Gradient Boosting Tree (GBT), όπου κάθε δέντρο απόφασης προβλέπει τη βαθμολογία ή την προτίμηση του χρήστη για ένα συγκεκριμένο στοιχείο.

Μια παραλλαγή του GB αλγορίθμου αποτελεί ο Extreme Gradient Boosting (XGBoost) αλγόριθμος που χρησιμοποιεί μια αποτελεσματικότερη υλοποίηση του αλγορίθμου και περιλαμβάνει πολλές πρόσθετες λειτουργίες, όπως κανονικοποίηση, επικύρωση (cross-validation) και πρόωρη διακοπή για την αποφυγή overfitting και τη βελτίωση της απόδοσης του μοντέλου. Ως αποτέλεσμα, ο συγκεκριμένος αλγόριθμος μπορεί να προβλέψει, να ταξινομήσει και να βελτιστοποιήσει το καθορισμένο σύστημα με την υψηλότερη ακρίβεια βάσει της δομής των δεδομένων. Τα προτεινόμενα προϊόντα στα συστήματα προτάσεων XGBoost περιέχουν το συνδυασμό των αποτελεσμάτων ταξινόμησης και πρόβλεψης και την εφαρμογή της τεχνικής του Συνεργατικού Φιλτραρίσματος, η οποία προαναφέρθηκε στην υπο-ενότητα 2.2.2.2.

Στην Εικόνα 5 παρουσιάζεται η αρχιτεκτονική ενός συστήματος προτάσεων βασισμένο στον αλγόριθμο XGBoost (Shahbazi, Hazra, Park, & Byun, 2020), η οποία περιλαμβάνει 6 επιμέρους επίπεδα. Πιο συγκεκριμένα, το πρώτο επίπεδο περιλαμβάνει τα δεδομένα εισόδου, ενώ το δεύτερο επίπεδο αποτελεί το επίπεδο ανάλυσης των δεδομένων που περνάνε από το επίπεδο εισόδου. Το τρίτο επίπεδο, η ανάλυση των δεδομένων, διακρίνεται σε τρεις επιμέρους φάσεις, την ανάλυση χρονοσειρών (time series analysis), την ανάλυση του ενδιαφέροντος του χρήστη (user interest analysis) και την ανάλυση της σελίδας πρόσβασης (access page analysis). Τα χαρακτηριστικά που προκύπτουν από τα αποτελέσματα της ανάλυσης περιλαμβάνουν τις πληροφορίες κλικ του χρήστη, κάθε προϊόν που αγόρασε ο χρήστης κ.λπ. Τα επεξεργασμένα δεδομένα, στη συνέχεια, περνούν στο τέταρτο επίπεδο (word2vec based framework) για τη δημιουργία της τεχνικής κωδικοποίησης word2vec. Τέλος, οι παραγόμενες πληροφορίες χρησιμοποιούνται ως είσοδος του μοντέλου XGBoost (πέμπτο επίπεδο), από το οποίο εξάγονται προτάσεις για το χρήστη, στο έκτο επίπεδο, βάσει παλαιότερων κλικ που έχει κάνει.



Εικόνα 5: Αρχιτεκτονική συστήματος προτάσεων βασισμένο σε GB αλγόριθμο (XGBoost) (Shahbazi, Hazra, Park, & Byun, 2020).

Συνοψίζοντας, ο αλγόριθμος GB αποτελεί έναν ισχυρό αλγόριθμο για τη δημιουργία συστημάτων προτάσεων, ο οποίος μπορεί να προσφέρει εξατομικευμένες προτάσεις στους χρήστες με βάση την παρελθοντική συμπεριφορά και τις προτιμήσεις τους. Έχει αποδειχτεί ότι επιτυγχάνει κορυφαίες επιδόσεις σε πολλές εφαρμογές και χρησιμοποιείται ευρέως στο ηλεκτρονικό εμπόριο και στα μέσα κοινωνική δικτύωσης.

2.3 Λύσεις Ασφαλούς Πρόσβασης σε Δεδομένα στο Blockchain

Η προσδοκία διασφάλισης της εμπιστοσύνης και της μείωσης των γενικών εξόδων για τα ευφυή συστήματα IoT έχει οδηγήσει στην ανάγκη για συνδυασμό των δύο τεχνολογιών, του blockchain και του IoT, ώστε αφενός να δημιουργείται μια δημόσια, επαληθεύσιμη, αποκεντρικοποιημένη και αξιόπιστη βάση δεδομένων και, αφετέρου να επιτρέπεται η ασφαλής και έμπιστη διασύνδεση μεγάλου αριθμού συσκευών σε ένα δίκτυο.

2.3.1 Ασφάλεια στο Blockchain

Τα κλασικά κεντρικοποιημένα συστήματα ελέγχου πρόσβασης δεδομένων παρουσιάζουν αρκετά προβλήματα, με βασικότερο τον κίνδυνο διαρροής των δεδομένων σε κάποιον τρίτο. Επιπλέον, καθώς υπάρχει μόνο μια κεντρική οντότητα υπεύθυνη για τον έλεγχο της πρόσβασης στα δεδομένα του συστήματος, ενέχεται ο κίνδυνος ενός σημείου αστοχίας (single point of failure).

Παρόλα αυτά, ακόμα και η μέθοδος κρυπτογράφησης βάσει χαρακτηριστικών (attribute-based encryption) μπορεί να παρουσιάσει προβλήματα απορρήτου, όπως διαρροή απορρήτου από τη γεννήτρια ιδιωτικού κλειδιού (Private Key Generator, PKG), αλλά και single point of failure όπως προαναφέρθηκε. Για το λόγο αυτό, οι (Wang, Zhang, & Zhang, 2018) προτείνουν την εισαγωγή ενός νέου πλαισίου για την κοινή χρήση των δεδομένων του δικτύου, αλλά και τον έλεγχο της πρόσβασης σε αυτά, ως λύση αντιμετώπισης του προαναφερθέντος προβλήματος χρησιμοποιώντας αποκεντρικοποιημένη αποθήκευση.

Από την άλλη πλευρά, οι τρέχουσες λύσεις για τη διαχείριση του ελέγχου πρόσβασης σε πολλούς διαχειριστικούς τομείς δεν είναι ιδιαίτερα αποτελεσματικές, καθώς δεν είναι επεκτάσιμες και εύκολα διαχειρίσιμες. Για το σκοπό αυτό, στη μελέτη των (Paillisse, και συν., 2019) προτείνεται η διανομή και η καταγραφή των πολιτικών πρόσβασης σε ένα permissioned blockchain δίκτυο.

Όσον αφορά την κοινή χρήση δεδομένων μεταξύ πολλών οργανισμών που μπορεί να περιλαμβάνονται στο ίδιο δίκτυο, και αυτή ενέχει κινδύνους για τα δεδομένα των χρηστών. Συνεπώς, στους συγκεκριμένους τύπους δικτύων βασικό μέλημα είναι η διατήρηση των προσωπικών δεδομένων που σχετίζονται, κυρίως, με την ταυτότητα των χρηστών τους. Στο συγκεκριμένο πλαίσιο, στη μελέτη των (Alansari, Paci, & Sassone, 2017) προτείνεται ένα σύστημα ελέγχου πρόσβασης δεδομένων, το οποίο βασίζεται στο μηχανισμό της συμμετρικής κρυπτογράφησης κλειδιού (symmetric key encryption). Το προτεινόμενο σύστημα ελέγχει τα χαρακτηριστικά όλων των χρηστών του δικτύου με χρήση κατάλληλων πολιτικών ελέγχου, με στόχο την εκχώρηση δικαιωμάτων πρόσβασης στα δεδομένα που ανήκουν στον ίδιο ομοσπονδιακό οργανισμό, ενώ παράλληλα τα χαρακτηριστικά των χρηστών παραμένουν ιδιωτικά.

Μια επιπρόσθετη κατηγορία που θα πρέπει επίσης να λαμβάνεται υπόψη σχετικά με την προστασία των προσωπικών δεδομένων των χρηστών αποτελούν και οι εφαρμογές κινητών συσκευών. Ένα ήδη υπάρχον σύστημα διαχείρισης ελέγχου πρόσβασης για τη συγκεκριμένη κατηγορία είναι το Enigma (Zyskind, Nathan, & others, 2015), το οποίο βασίζεται στο Ethereum blockchain και προτάθηκε για την αντιμετώπιση τριών βασικών προβλημάτων, της ιδιοκτησίας των δεδομένων, της διαφάνειας και της δυνατότητας ελέγχου των δεδομένων, αλλά και του ακριβούς ελέγχου πρόσβασης σε αυτά. Το συγκεκριμένο σύστημα διαχείρισης περιέχει τρεις κατανεμημένες βάσεις δεδομένων, ένα blockchain δίκτυο, έναν κατανεμημένο πίνακα κατακερματισμού (Distributed Hash Table, DHT) και έναν υπολογισμό πολλαπλών μερών (Multi-Party Computation, MPC), ο οποίος χρησιμοποιείται για τον κατακερματισμό των δεδομένων σε μικρότερα κομμάτια που δεν έχουν πλέον νόημα και τη διανομή αυτών μεταξύ των κόμβων του δικτύου. Συνεπώς, το προτεινόμενο σύστημα είναι σχεδιασμένο με τέτοιο τρόπο ώστε να επιτρέπεται ο έλεγχος των προσωπικών δεδομένων των χρηστών από τους ίδιους, καθιστώντας την όλη διαδικασία της πρόσβασης των δεδομένων διαφανή. Επιπλέον, δίνεται η δυνατότητα στους χρήστες να τροποποιούν ή να ανακαλούν τα δικαιώματα πρόσβασης στα προσωπικά τους δεδομένα χωρίς την εγκατάσταση της κινητής εφαρμογής.

2.3.2 Blockchain Μηχανισμοί Attribute Based Access Control

Ένα σύστημα ελέγχου πρόσβασης βάσει χαρακτηριστικών (Attribute Based Access Control, ABAC) μπορεί να χρησιμοποιηθεί για τον έλεγχο της πρόσβασης σε πόρους με βάση τα χαρακτηριστικά κάθε χρήστη του εκάστοτε δικτύου, τον πόρο του δικτύου στον οποίο αυτός έχει πρόσβαση, καθώς και το περιβάλλον στο οποίο πραγματοποιείται η πρόσβαση. Στα πλαίσια ενός blockchain δικτύου, ο ABAC μηχανισμός μπορεί να χρησιμοποιηθεί για τον έλεγχο της πρόσβασης σε δεδομένα που είναι αποθηκευμένα στο blockchain ή σε ορισμένα χαρακτηριστικά ενός Dapp.

Σε κάθε ABAC σύστημα, η πρόσβαση σε πόρους χορηγείται ή απορρίπτεται με βάση την αξιολόγηση ενός συνόλου χαρακτηριστικών, το οποίο μπορεί να περιλαμβάνει την ταυτότητα (ID) του χρήστη, το ρόλο ή τη συμμετοχή στην ομάδα του χρήστη, το πλαίσιο στο οποίο λαμβάνει χώρα η πρόσβαση, καθώς και οποιαδήποτε άλλη πληροφορία. Τα συγκεκριμένα χαρακτηριστικά, συνήθως, αποθηκεύονται σε μια πολιτική που ορίζει τους κανόνες για τον έλεγχο της πρόσβασης.

Υπάρχουν διάφοροι τρόποι που επιτρέπουν την εφαρμογή του ABAC μηχανισμού σε blockchain δίκτυα. Πιο συγκεκριμένα, μπορεί να υλοποιηθεί χρησιμοποιώντας έξυπνα συμβόλαια, τα οποία είναι αυτοεκτελούμενα και περιλαμβάνουν τους όρους της συμφωνίας μεταξύ αγοραστή και πωλητή, για την κωδικοποίηση των κανόνων για τον έλεγχο πρόσβασης και την αυτόματη επιβολή τους στο blockchain δίκτυο. Μια άλλη προσέγγιση εντοπίζεται στη χρήση του ABAC μηχανισμού σε συνδυασμό με αποδείξεις μηδενικής γνώσης (Zero-Knowledge Proofs, ZKPs), οι οποίες επιτρέπουν στο χρήστη να αποδείξει την κατοχή συγκεκριμένων χαρακτηριστικών, χωρίς ωστόσο να αποκαλύπτει τα ίδια τα χαρακτηριστικά. Το γεγονός αυτό καθίσταται ιδιαίτερα χρήσιμο σε καταστάσεις όπου είναι σημαντική η προστασία του απορρήτου των χρηστών, όπως συμβαίνει στα ευαίσθητα προσωπικά δεδομένα.

Συνοπτικά, ο ABAC μηχανισμός αποτελεί ένα ισχυρό εργαλείο για τον έλεγχο της πρόσβασης σε πόρους σε ένα blockchain δίκτυο, επιτρέποντας λεπτομερή έλεγχο σχετικά με το ποιος μπορεί να έχει πρόσβαση σε ποιους πόρους του δικτύου και υπό ποιες συνθήκες και μπορεί να εφαρμοστεί τόσο σε permissioned όσο και σε permissionless δίκτυα blockchain. Πιο συγκεκριμένα, στην περίπτωση ενός permissioned blockchain δικτύου, ο έλεγχος της πρόσβασης γίνεται συνήθως μέσω της χρήσης πιστοποιητικών ή άλλων μορφών ελέγχου ταυτότητας, οι οποίες επιτρέπουν μόνο εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στο σύστημα. Σε αυτή την περίπτωση, ο ABAC μηχανισμός μπορεί να χρησιμοποιηθεί για την περαιτέρω βελτίωση του ελέγχου πρόσβασης, καθορίζοντας χαρακτηριστικά που πρέπει να υπάρχουν στο πιστοποιητικό ενός χρήστη ή σε άλλα διαπιστευτήρια ελέγχου της ταυτότητάς του, προκειμένου να αποκτηθεί η πρόσβαση στους πόρους του δικτύου. Από την άλλη πλευρά, σε ένα permissionless δίκτυο blockchain, ο έλεγχος πρόσβασης πραγματοποιείται μέσω της χρήσης κρυπτογραφικών κλειδιών που χρησιμοποιούνται για την υπογραφή συναλλαγών. Οπότε, σε αυτή την περίπτωση, ο ABAC μηχανισμός υλοποιείται συμπεριλαμβάνοντας χαρακτηριστικά συναλλαγών που θα πρέπει να υπάρχουν σε κάθε συναλλαγή που πραγματοποιείται εντός του δικτύου.

Στις υπο-ενότητες που ακολουθούν παρουσιάζονται προσεγγίσεις από υλοποιημένους ABAC μηχανισμούς σε permissioned (ενότητα 2.3.2.1) και permissionless (ενότητα 2.3.2.2) δίκτυα blockchain.

2.3.2.1 Attribute Based Access Control σε Blockchain Δίκτυα Ελεγχόμενης Πρόσβασης

Η μελέτη των (Hardjono & Pentland, 2019) επικεντρώνεται στην επίλυση του προβλήματος της ταυτοποίησης και του ελέγχου πρόσβασης των χρηστών ενός permissioned blockchain δικτύου. Το προτεινόμενο σύστημα ChainAnchor παρέχει ανώνυμες αλλά επαληθεύσιμες ταυτότητες για οντότητες του blockchain δικτύου, καθώς επίσης και έλεγχο πρόσβασης στις οντότητες του δικτύου που επιθυμούν να πραγματοποιήσουν συναλλαγές εντός του δικτύου αυτού, ο οποίος επιβάλλεται μέσω των κόμβων συναίνεσης (consensus) με μια απλή αναζήτηση σε μία read-only λίστα που περιλαμβάνει δημόσια κλειδιά ανώνυμων μελών. Το ChainAnchor παρέχει επίσης τη δυνατότητα αποσύνδεσης των συναλλαγών που μπορεί να ανήκουν σε μια συγκεκριμένη οντότητα του δικτύου, με αποτέλεσμα η αντίστοιχη οντότητα να μπορεί να γνωστοποιεί προαιρετικά την ταυτότητά της σε περίπτωση που μια συναλλαγή μπορεί να τεθεί υπό αμφισβήτηση, χωρίς ωστόσο να επηρεάζεται η ανωνυμία των υπολοίπων συναλλαγών που έχουν πραγματοποιηθεί στο δίκτυο.

Μια άλλη μελέτη των (Rouhani, Belchior, Cruz, & Deters, 2021) προτείνει ένα κατανεμημένο σύστημα ABAC βασισμένο σε ένα permissioned blockchain δίκτυο για την παροχή αξιόπιστου ελέγχου όλων των προσπαθειών πρόσβασης στα δεδομένα του δικτύου. Πέρα από τη δυνατότητα ελέγχου της πρόσβασης, το προτεινόμενο σύστημα παρουσιάζει και ένα επίπεδο διαφάνειας που μπορεί να ωφελήσει τόσο τους αιτούντες πρόσβασης στους πόρους, όσο και τους ίδιους τους παρόχους των αντίστοιχων δεδομένων. Η υλοποίηση που παρουσιάζεται στη μελέτη είναι βασισμένη σε Hyperledger Fabric (HLF), οπότε και επιτυγχάνεται συνδυασμός υψηλής αποδοτικότητας του δικτύου με χαμηλό υπολογιστικό κόστος. Η επικύρωση της προτεινόμενης λύσης πραγματοποιείται μέσω μιας περίπτωσης χρήσης ψηφιακών βιβλιοθηκών (digital libraries), ενώ παράλληλα παρουσιάζεται λεπτομερής ανάλυση της απόδοσής της, λαμβάνοντας υπόψη διαφορετικούς consensus μηχανισμούς και βάσεις δεδομένων.

Τέλος, η μελέτη των (Zhang, Yutaka, Sasabe, & Kasahara, 2020) προτείνει ένα κατανεμημένο και αξιόπιστο framework ελέγχου πρόσβασης σε δεδομένα για έξυπνες πόλεις, συνδυάζοντας την τεχνολογία των έξυπνων συμβολαίων με το μηχανισμό ABAC. Πιο συγκεκριμένα, το προτεινόμενο framework περιλαμβάνει ένα συμβόλαιο διαχείρισης πολιτικών (Policy Management Contract, PMC), για τη διαχείριση των ABAC πολιτικών, ένα συμβόλαιο διαχείρισης χαρακτηριστικών θεμάτων (Subject Attribute Management Contract, SAMC), για τη διαχείριση των χαρακτηριστικών όλων των οντοτήτων του δικτύου που έχουν πρόσβαση σε κάποιο πόρο, ένα συμβόλαιο διαχείρισης χαρακτηριστικών αντικειμένων (Object Attribute Management Contract, OAMC), για τη διαχείριση των χαρακτηριστικών των πόρων, και, τέλος, ένα συμβόλαιο ελέγχου πρόσβασης (Access Control Contract, ACC), για την εκτέλεση του ελέγχου πρόσβασης στους πόρους. Το προτεινόμενο σύστημα είναι βασισμένο στο Ethereum blockchain.

2.3.2.2 Attribute Based Access Control σε Blockchain Δίκτυα Μη Ελεγχόμενης Πρόσβασης

Η μελέτη των (Liu, Liu, Zhang, & Yu, 2020) προτείνει ένα δίκαιο πρωτόκολλο επιλογής για την αναδιαμόρφωση μιας επιτροπής σε ένα permissionless blockchain δίκτυο, το οποίο αποτελείται από δύο επιμέρους φάσεις, τη διαδικασία εξόρυξης και την επιβεβαίωση της λίστας των νέων κόμβων. Οι συγγραφείς αναλύουν επίσης τον αντίκτυπο της καθυστέρησης του δικτύου και παρέχουν μια αυστηρή απόδειξη της διαδικασίας εξόρυξης. Παράλληλα, προτείνεται ένας κανόνας ψηφοφορίας κατωφλίου ως μηχανισμός άμυνας έναντι σε επιθέσεις λογοκρισίας των κόμβων του δικτύου και απόδειξης της ασφαλείας ολόκληρου του πρωτοκόλλου, συμπεριλαμβανομένων και των ιδιοτήτων ασφαλείας. Το προτεινόμενο πρωτόκολλο θα μπορούσε να έχει εφαρμογή και σε blockchain δίκτυα που βασίζονται σε διαφορετικές επιτροπές με διαφορετικές απαιτήσεις.

Αξίζει να σημειωθεί ότι υπάρχουν αρκετά διαθέσιμα ABAC frameworks που έχουν εφαρμοστεί σε permissionless blockchain δίκτυα, ενδεικτικά τα Hyperledger Aries και Sovrin. Πιο συγκεκριμένα, το Hyperledger Aries (HyperledgerFoundation, 2022), αποτελεί ένα framework ανοιχτού κώδικα, το οποίο επιτρέπει στους χρήστες τη δημιουργία και τη διαχείριση επαληθεύσιμων διαπιστευτηρίων, τα οποία με τη σειρά τους μπορούν να χρησιμοποιηθούν για την αναπαράσταση χαρακτηριστικών όπως ταυτότητα, προσόντα ή δικαιώματα, τα οποία μπορούν να χρησιμοποιηθούν με τη σειρά τους για τον έλεγχο της πρόσβασης σε πόρους του δικτύου. Μια παρόμοια πλατφόρμα αποτελεί και το Sovrin (Sovrin, 2022), το οποίο χρησιμοποιεί τον ABAC μηχανισμό για τον έλεγχο της πρόσβασης σε χαρακτηριστικά ταυτότητας και σχετικά δεδομένα, ενώ δίνεται η δυνατότητα στους χρήστες να δημιουργούν και να διαχειρίζονται επαληθεύσιμα διαπιστευτήρια που μπορούν να χρησιμοποιηθούν για την επαλήθευση της ταυτότητας και άλλων χαρακτηριστικών τους.

3 Ανακάλυψη Ομόσπονδων Πόρων IoT

Σε μια πλατφόρμα όπως αυτή του IoTFeds, η ανακάλυψη πόρων IoT που ανήκουν σε μια ομοσπονδία αποτελεί μια από τις πλέον χρήσιμες λειτουργίες για τους τελικούς χρήστες αφού τους επιτρέπει να αναζητούν και να ανακαλύπτουν πόρους που ικανοποιούν τις ανάγκες τους. Η αναζήτησή των IoT πόρων (resources/devices) μπορεί να πραγματοποιηθεί με βάση μια πληθώρα κριτηρίων, όπως για παράδειγμα με βάση την τοποθεσία ή τον τύπο των δεδομένων (περιγραφή).

Η πλατφόρμα του symbIoTe παρέχει ήδη έναν μηχανισμό αναζήτησης που εξυπηρετεί την αναζήτηση ομόσπονδων πόρων. Ωστόσο, δεν καλύπτει όλα τα πιθανά κριτήρια αναζήτησης, και ιδιαίτερα όταν αυτά αφορούν πληροφορία αποθηκευμένη στο blockchain (on-chain) όπως είναι η τιμολόγηση και οι βαθμοί φήμης που υπολογίζονται από το BaaS. Επομένως, η αναζήτηση ομόσπονδων πόρων με βάση το κριτήριο της φήμης και της τιμής καλύπτεται από το BaaS. Τέλος, η αναζήτηση προϊόντων καλύπτεται από το στοιχείο λογισμικού αγοράς – marketplace – με τα κριτήρια αναζήτησης για την τιμή και τη φήμη των προϊόντων να υλοποιούνται από το BaaS.

Όπως έχει ήδη αναφερθεί στο Κεφάλαιο 2, τα οφέλη της κατανεμημένης αναζήτησης είναι πολλά. Ο μηχανισμός αναζήτησης της IoTFeds πλατφόρμας αποτελεί μια κατανεμημένη αναζήτηση, όπως παρουσιάζεται στην ενότητα 3.1, μιας και υπάρχουν πολλαπλοί κόμβοι στους οποίους φιλοξενούνται τα δεδομένα που αποθηκεύονται, και επομένως η αναζήτηση λαμβάνει χώρα σε κάθε έναν από τους κόμβους.

Συνεπώς, η αναζήτηση στην IoTFeds πλατφόρμα γίνεται σε δύο επίπεδα. Στο πρώτο στάδιο, το symbIoTe/marketplace αναλαμβάνει να πραγματοποιήσει μια κατανεμημένη αναζήτηση ανάμεσα σε όλο το πλήθος των IoT πόρων/προϊόντων, για τα κριτήρια που υποστηρίζει, και έχει ως αποτέλεσμα μια λίστα IoT πόρων/προϊόντων που ικανοποιούν τα εκάστοτε κριτήρια. Στο δεύτερο επίπεδο, η λίστα αυτή λαμβάνεται από το BaaS, το οποίο ελέγχει την εγκυρότητα της λίστας και στη συνέχεια πραγματοποιεί μια επιπλέον αναζήτηση με βάση την τιμή ή/και τη φήμη τους, αν αυτή είναι απαραίτητη.

Κάθε ένας από αυτούς τους μηχανισμούς περιγράφεται αναλυτικά στις ακόλουθες ενότητες.

3.1 Μηχανισμοί και Κριτήρια Αναζήτησης στο off-chain Σύστημα

Το symbIoTe παρέχει μηχανισμούς αναζήτησης για IoT πόρους διαθέσιμους προς τρίτους καθώς και ομόσπονδους πόρους (πόρους διαμοιραζόμενους σε μία IoT ομοσπονδία) που αντιστοιχούν στα L1/L2 επίπεδα διαλειτουργικότητας (compliance levels) του symbIoTe. Στην ενότητα αυτή αρχικά παρουσιάζεται ο υπάρχοντας μηχανισμός αναζήτησης στο symbIoTe ο οποίος αποτέλεσε τη βάση για την ανάπτυξη των νέων διεπαφών στο σύστημα του IoTFeds. Οι διεπαφές που αναπτύχθηκαν ενσωματώνουν την επικοινωνία με το BaaS και περιγράφονται στη συνέχεια.

Στο symbIoTe η αναζήτηση βασίζεται στο endpoint <symbIoTe-core-url>/coreInterface/query το οποίο είναι κατασκευασμένο ώστε να δέχεται κατάλληλες παραμέτρους για την αναζήτηση IoT πόρων με βάση κάποια κριτήρια. Το αίτημα αναζήτησης (search request) πρέπει να συνοδεύεται από κατάλληλα κατασκευασμένους security headers για να είναι επιτυχές το αίτημα, καθώς αξιοποιούνται οι πολιτικές πρόσβασης/αναζήτησης (access and filtering policies) – ABAC μηχανισμοί - που ορίζονται κατά την καταχώρηση ενός IoT πόρου στο σύστημα.

Τα κριτήρια αναζήτησης που υποστηρίζονται παρουσιάζονται στον Πίνακας 1.

Πίνακας 1: Κριτήρια αναζήτησης για IoT πόρους (L1) με το symbIoTeAPI..

#	Κριτήριο αναζήτησης	Τύπος δεδομένων	Περιγραφή
1	platform_id	String	Το αναγνωριστικό της πλατφόρμας στην οποία θα αναζητηθούν οι πόροι.
2	platform_name	String	Το όνομα της επιθυμητής πλατφόρμας (όπου θα αναζητηθούν οι πόροι).
4	owner	String	Ο ιδιοκτήτης/οργανισμός των πόρων. (π.χ. icom1)
5	name	String	Το όνομα της IoT συσκευής/πόρου, εάν είναι γνωστό κατά την αναζήτηση.
6	id	String	Το αναγνωριστικό της IoT συσκευής/πόρου, εάν είναι γνωστό κατά την αναζήτηση.
7	description	String	Περιγραφή της IoT συσκευής/πόρου, που δόθηκε από τον ιδιοκτήτη της κατά την εγγραφή.
8	location_name	String	Τοποθεσία της IoT συσκευής/πόρου (π.χ. Europe/Athens).
9	location_lat	Double	Γεωγραφικό μήκος της τοποθεσίας της IoT συσκευής/πόρου.
10	location_long	Double	Γεωγραφικό πλάτος της τοποθεσίας της IoT συσκευής/πόρου.
11	max_distance	Integer	Μέγιστη απόσταση (σε μέτρα) από την επιθυμητή τοποθεσία των πόρων.
12	observed_property	List<String>	Λίστα με επιθυμητές παρατηρήσεις-μετρικές των πόρων. (π.χ. [humidity, temperature]
13	resource_type	String	Ο τύπος της επιθυμητής IoT συσκευής/πόρου (π.χ. http://www.symbiote-h2020.eu/ontology/core#StationarySensor)
14	should_rank	Boolean	True εάν οι πόροι θα επιστραφούν ταξινομημένοι με βάση τα κριτήρια αναζήτησης. Αλλιώς False.

Το symbIoTe παρέχει επιπλέον ένα endpoint για την υποστήριξη αναζητήσεων βασιζόμενων σε SPARQL queries με βάση εγγεγραμμένα μοντέλα πληροφορίας πλατφορμών. Αυτό το endpoint, < symbiotecore -url>/coreInterface/sparqlQuery δέχεται την ακόλουθη πληροφορία:

```
{
   "sparqlQuery" : "<sparql>",
   "outputFormat" : "<format>"
}
```

Πιθανά Output formats είναι: SRX, XML, JSON, SRJ, SRT, THRIFT, SSE, CSV, TSV, SRB, TEXT, COUNT, TUPLES, NONE, RDF, RDF_N3, RDF_XML, N3, TTL, TURTLE, GRAPH, NT, N_TRIPLES, TRIG

Ένα παράδειγμα χρήσης είναι το παρακάτω:

```
{
"sparqlQuery" : "PREFIX cim: <http://www.symbiote-h2020.eu/ontology/core#> PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#> SELECT ?res ?resourceName WHERE { ?res a cim:Resource. ?res rdfs:label ?resourceName . }",
   "outputFormat" : "TEXT"
}
```

Τέλος, το symbIoTe επιτρέπει την αναζήτηση ομόσπονδων IoT πόρων/συσκευών (πόρους που ανήκουν και διαμοιράζονται σε ομοσπονδίες που ανήκει μία IoT πλατφόρμα ενός οργανισμού). Η λειτουργικότητα αυτή παρέχεται από το στοιχείο λογισμικού Platform Registry (PR) του symbIoTe της εκάστοτε IoT πλατφόρμας που είναι μέλος μίας ή περισσότερων ομοσπονδίας. Το αίτημα αναζήτησης επιστρέφει τους ομόσπονδους πόρους που καλύπτουν τα κριτήρια αναζήτησης και με βάση τις πολιτικές φιλτραρίσματος του κάθε καταχωρημένου IoT πόρου στις ομοσπονδίες που συμμετέχει η πλατφόρμα αυτή. Μεταξύ των κριτηρίων αναζήτησης παρέχεται η δυνατότητα καθορισμού της/των επιθυμητών ομοσπονδιών. Επιπλέον στα κριτήρια αναζήτησης μπορούν να καθοριστούν τα επιθυμητά επίπεδα φήμης της IoT συσκευής/πόρου που υποστηρίζονται στο symbIoTe.

Πίνακας 2: Κριτήρια αναζήτησης για πόρους (L2) που ανήκουν σε ομοσπονδίες, με το symbIoTeAPI..

#	Κριτήριο αναζήτησης	Τύπος δεδομένων	Περιγραφή
1	name	List<String>	Τα ονόματα των ομόσπονδων πόρων.
2	description	List<String>	Περιγραφές των ομόσπονδων πόρων που τους έδωσε ο πάροχος κατά την εγγραφή τους..
3	id	List<String>	Τα αναγνωριστικά των ομόσπονδων πόρων μέσα στην ομοσπονδία.
4	federationId	List<String>	Τα αναγνωριστικά των ομοσπονδιών.
5	observes_property	List<String>	Οι παρατηρήσεις των ομόσπονδων πόρων, μετρικές όπως η υγρασία (humidity) και η θερμοκρασία (temperature).
6	resource_type	String	Τύπος των ομόσπονδων πόρων (π.χ. http://www.symbiote-h2020.eu/ontology/core#StationarySensor)
7	location_name	List<String>	Τοποθεσίες των ομόσπονδων πόρων (π.χ. Europe/Athens).
8	location_lat	Double	Γεωγραφικό μήκος της τοποθεσίας των πόρων.
9	location_long	Double	Γεωγραφικό πλάτος της τοποθεσίας των πόρων.
10	max_distance	Integer	Μέγιστη απόσταση (σε μέτρα) από την τοποθεσία των πόρων.
11	resource_trust	Double	*απενεργοποιημένο στο IoTFeds
12	adaptive_trust	Double	*απενεργοποιημένο στο IoTFeds

13	sort	String	Σειρά ταξινόμησης των ομόσπονδων πόρων με το αναγνωριστικό τους. («ASC» για αύξουσα σειρά και «DESC» για φθίνουσα σειρά)

Στα πλαίσια του έργου IoTFeds, οι παραπάνω μηχανισμοί αξιοποιούνται για την υποστήριξη (α) της αναζήτησης από έναν πάροχο δεδομένων των εγγεγραμμένων IoT συσκευών του στην πλατφόρμα IoTFeds με στόχο τον διαμοιρασμό τους στις επιθυμητές ομοσπονδίες (L1 Resources) και (β) της αναζήτησης ομόσπονδων IoT πόρων από μέλος της ομοσπονδίας για τη δημιουργία προϊόντος με τις επιθυμητές πηγές δεδομένων στην εκάστοτε ομόσπονδη αγορά (L2 resources). Για το σκοπό αυτό, οι υπάρχουσες διεπαφές του symbIoTe αξιοποιήθηκαν για την υλοποίηση αντίστοιχων διεπαφών στο στοιχείο λογισμικού symbIoTeAPI οι οποίες ενσωματώνουν επιπλέον επικοινωνία με τις διεπαφές του BaaS για τον έλεγχο και ανάκτηση πληροφορίας από το on-chain σύστημα. Τέλος, οι διεπαφές του symbIoTeAPI αξιοποιούνται από το στοιχείο λογισμικού του marketplace (την πύλη αγοράς) που αναπτύχθηκε στα πλαίσια του έργου για την αλληλεπίδραση των τελικών χρηστών του IoTFeds με το σύστημα για πρόσβαση στις παρεχόμενες υπηρεσίες αγοράς. Τα κριτήρια αναζήτησης που ενσωματώνει η υπηρεσία Marketplace είναι τα ίδια πεδία που υποστηρίζει το symbIoTeAPI θέλοντας να δώσει στον χρήστη της υπηρεσίας όλες τις δυνατότητες αναζήτησης. Τα κριτήρια παρουσιάστηκαν παραπάνω (Πίνακας 1 και Πίνακας 2).

Τα σημεία πρόσβασης (endpoints) που παρέχονται από το στοιχείο λογισμικού symbIoTeAPI μέσω REST-API για την αναζήτηση IoT πόρων παρουσιάζονται στον Πίνακας 3.

Πίνακας 3: Διεπαφές symbIoTeAPI για την αναζήτηση IoT πόρων.

#	Interface	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	searchresource	marketplace	symbIoTeAPI	POST	symbioteapi/resources/searchL1	{"String", "String", "String", "String"}	(List<CloudResource Object>,Message)	Αναζήτηση IoT πόρων που ικανοποιούν τα κριτήρια.
2	REST	searchResourceL2	marketplace	symbIoTeAPI	POST	symbioteapi/resources/search/l2	{"String", "String", "String", "String"}	(List<CloudResource Object>,Message)	Αναζήτηση ομόσπονδων πόρων που ικανοποιούν τα κριτήρια.
3	REST	SparqlQuery	marketplace	symbIoTeAPI	POST	symbioteapi/resources/sparql?name=string	{"String", "String", "String", "String"}	(List<CloudResource Object>,Message)	Αναζήτηση IoT πόρων με SparqlQuery.

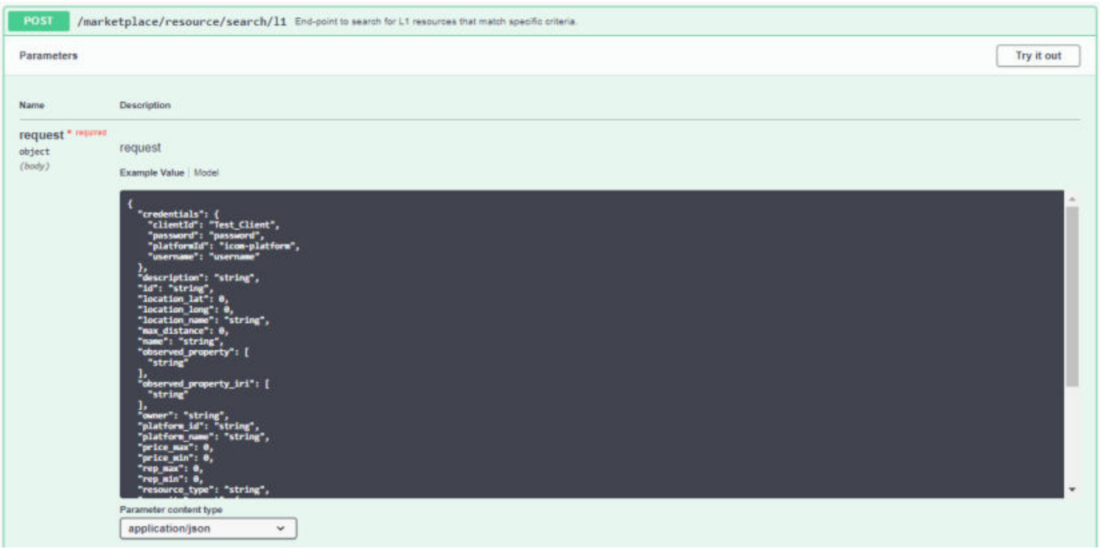
Τα σημεία πρόσβασης (endpoints) που παρέχονται από το στοιχείο λογισμικού marketplace μέσω REST-API για την αναζήτηση IoT πόρων παρουσιάζονται στον επόμενο πίνακα.

Πίνακας 4: Διεπαφές marketplaceAPI για την αναζήτηση IoT πόρων.

#	Interface	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	searchresource	IoT data consumer	marketplace	POST	/marketplace/resources/search	{"String", "String", "String", "String"}	(List<Cloud Resource Object>,Message)	Αναζήτηση IoT πόρων που ικανοποιούν τα κριτήρια.
2	REST	searchResourceL2	IoT data consumer	marketplace	POST	/marketplace /resources /search/l2	{"String", "String", "String", "String"}	(List<Cloud Resource Object>,Message)	Αναζήτηση ομόσπονδων πόρων που ικανοποιούν τα κριτήρια.
3	REST	SparqlQuery	IoT data consumer	marketplace	POST	marketplace /resources /sparql?name=string	{"String", "String", "String", "String"}	(List<Cloud Resource Object>,Message)	Αναζήτηση IoT πόρων με SparqlQuery.

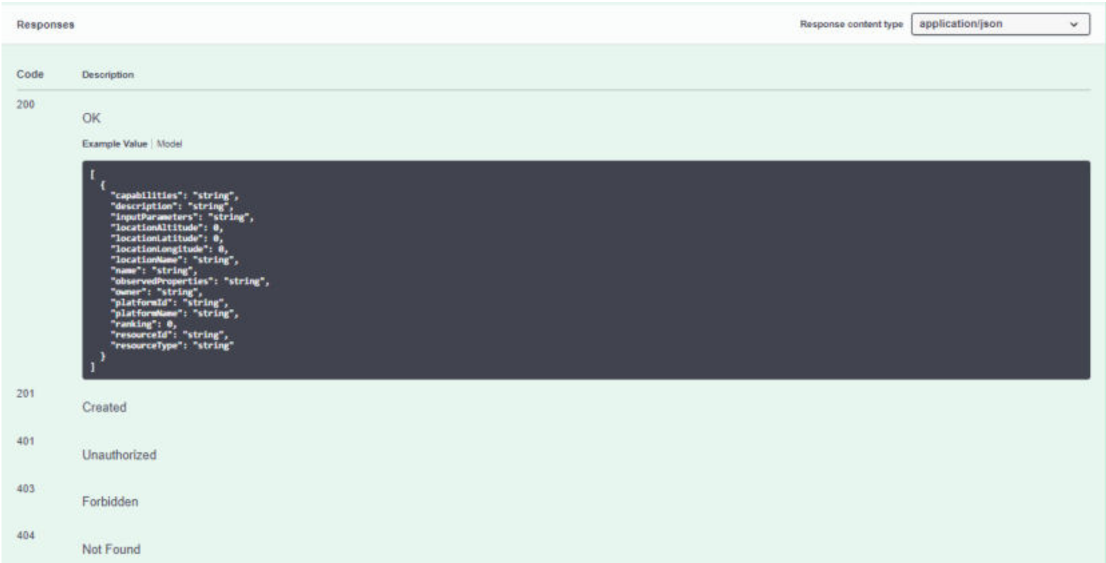
3.1.1 Αναζήτηση Πόρων Διαθέσιμων προς Τρίτους

Ένας χρήστης του IoTFeds μπορεί να αναζητήσει τις συσκευές που έχουν καταχωρηθεί στο σύστημα μέσω του παρακάτω endpoint, καθορίζοντας κριτήρια όπως εύρος τιμής και φήμης, τοποθεσία, χαρακτηριστικά, περιγραφή, τον τύπο της συσκευής κ.ά.:



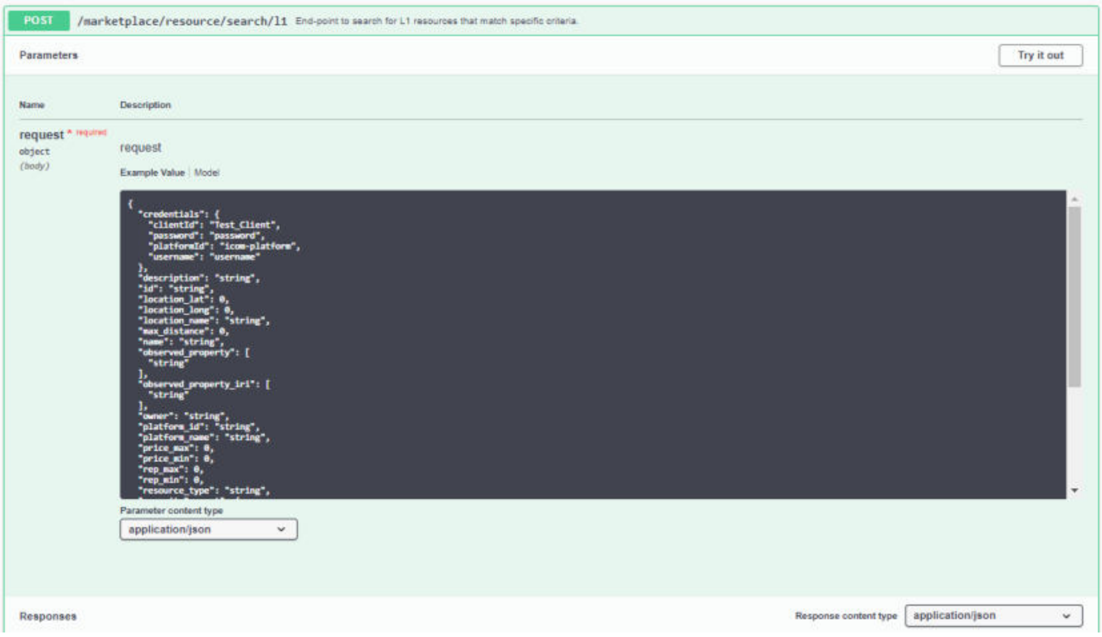
Εικόνα 6: Marketplace endpoint για αναζήτηση καταχωρημένων πηγών δεδομένων στο IoTFeds σύστημα.

Ο χρήστης ενημερώνεται με τη λίστα των πηγών δεδομένων με βάση τα κριτήρια αναζήτησης ή με αντίστοιχο μήνυμα λάθους.



Εικόνα 7:Απάντηση αναζήτησης με τη λίστα των διαθέσιμων IoT πόρων.

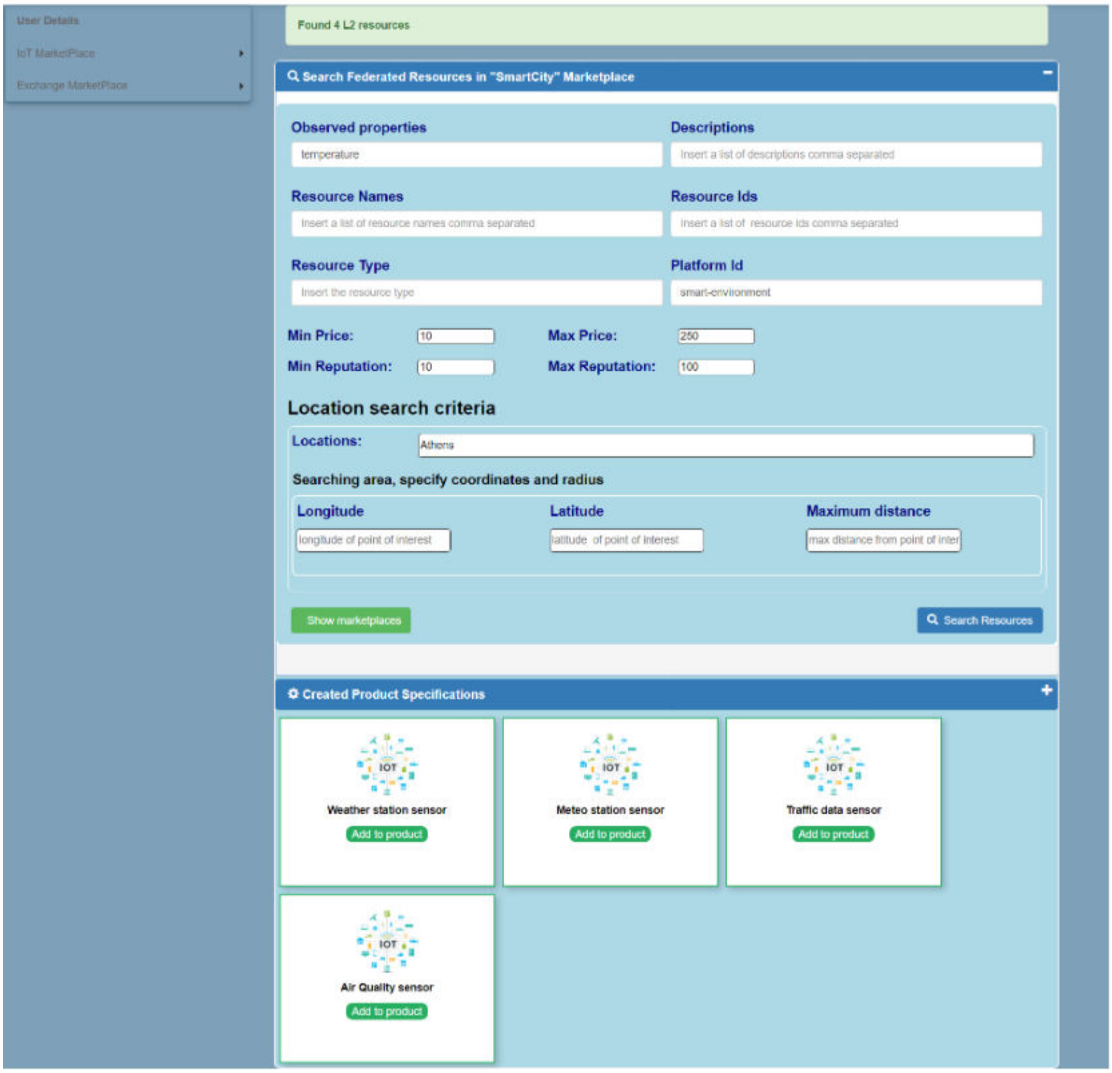
Η παραπάνω διεπαφή καλεί το αντίστοιχο endpoint του symbIoTeAPI (Εικόνα 8) για αναζήτηση στο υποσύστημα του symbIoTe τα αποτελέσματα από τα οποία προωθούνται στην αντίστοιχη διεπαφή του BaaS για φιλτράρισμα με τα επιπλέον κριτήρια όπως τιμή και φήμη. Όπως φαίνεται στην παρακάτω εικόνα, η αναζήτηση πόρων στο symbIoTeAPI που αναπτύχθηκε στα πλαίσια του έργου γίνεται από το endpoint <symbiotecore-url>/symbioteapi/resources/search το οποίο δέχεται τα κριτήρια αναζήτησης του symbIoTe όπως location, id, description, ενώ απαιτούνται τα διαπιστευτήρια του χρήστη για την επαλήθευση των δικαιωμάτων αναζήτησης και το φιλτράρισμα των IoT πόρων.



Εικόνα 8: symbIoTe-API endpoint για την αναζήτηση καταχωρημένων IoT πόρων.

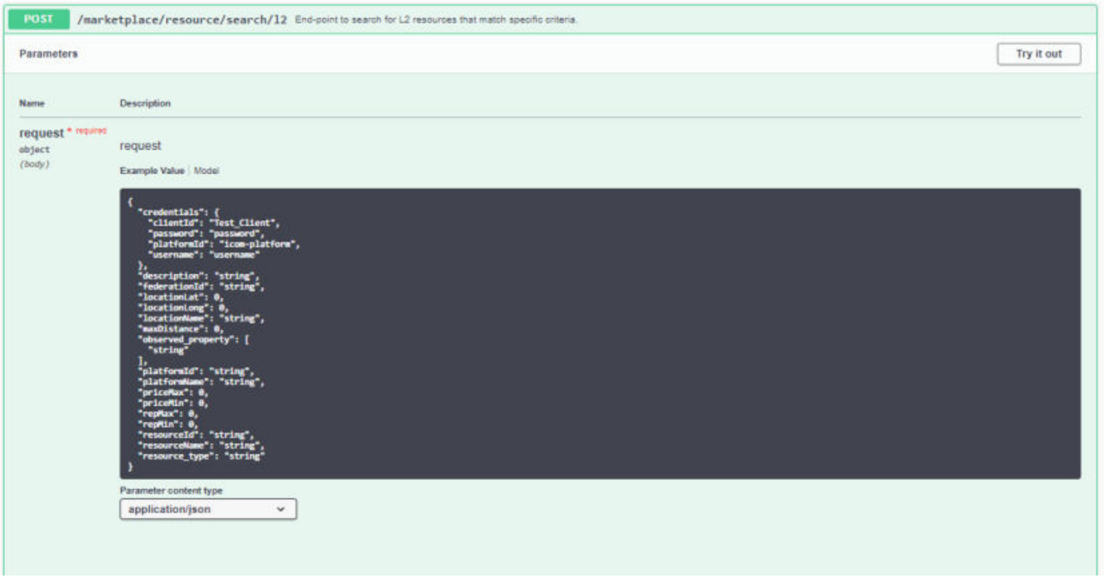
3.1.2 Αναζήτηση Ομόσπονδων Πόρων (L2 Resources)

Όπως φαίνεται στην παρακάτω εικόνα, ένα ομόσπονδο μέλος μπορεί να κάνει αναζήτηση από την γραφική διεπαφή χρήστη στην πύλη αγοράς (marketplace) για ομόσπονδες πηγές δεδομένων. Με την αναζήτηση αυτή μπορεί να ανακαλύψει πηγές δεδομένων που τον ενδιαφέρουν και τα χαρακτηριστικά τους (όπως η τιμή τους στην ομοσπονδία) για τη σύνθεση ενός προϊόντος στην επισκεπτόμενη ομόσπονδη αγορά.



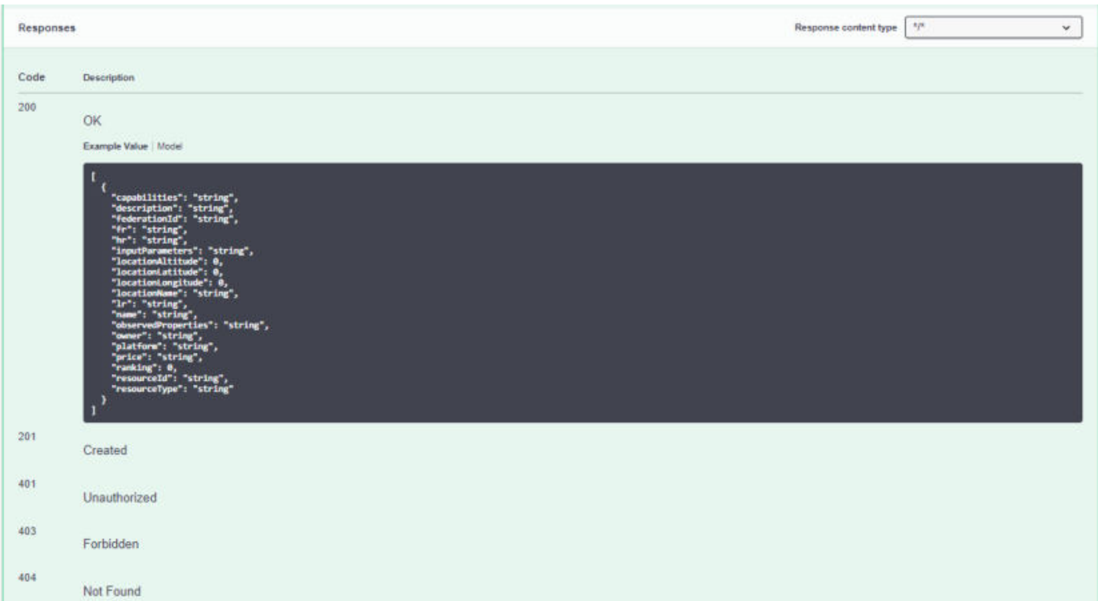
Εικόνα 9: Αναζήτηση πηγών δεδομένων σε μία ομόσπονδη αγορά.

Το ερώτημα με τα κριτήρια στη φόρμα που συμπλήρωσε ο χρήστης προωθούνται στην παρακάτω διεπαφή το οποίο διαχειρίζεται ερωτήματα από την πύλη αγοράς προς το σύστημα.



Εικόνα 10:Marketplace endpoint για αναζήτηση ομόσπονδων πηγών δεδομένων.

Επιστρέφεται η λίστα με τις πηγές δεδομένων και τα χαρακτηριστικά τους σε περίπτωση επιτυχίας ή διαφορετικά αντίστοιχο μήνυμα λάθους.



Εικόνα 11: Απάντηση αναζήτησης ομόσπονδων πηγών δεδομένων.

Το ερώτημα με τα κριτήρια αναζήτησης προωθείται στο symbIoTeAPI το οποίο λαμβάνει τη λίστα των διαθέσιμων IoT πόρων από το symbIoTe. Στην συνέχεια γίνεται ερώτημα στο BaaS για περαιτέρω φιλτράρισμα και ταξινόμηση με βάση τα υπόλοιπα κριτήρια αναζήτησης όπως το εύρος τιμής και φήμης. Τα αποτελέσματα των δύο ερωτημάτων, στο symbiote και στο Baas, συνδυάζονται ώστε να επιστραφεί μια ολοκληρωμένη εικόνα για την IoT συσκευή/πόρο.

3.2 Μηχανισμοί Κατανεμημένης Αναζήτησης στο on-chain Σύστημα (BaaS)

Η κατανεμημένη αναζήτηση στο BaaS λαμβάνει χώρα εξ’ ορισμού, καθώς το blockchain, αποτελεί ένα αποκεντρωμένο σύστημα, που αποτελείται από ένα πλήθος κόμβων κατανεμημένοι σε διαφορετικούς διακομιστές (servers). Όταν πραγματοποιείται ένα ερώτημα για την ανακάλυψη IoT πόρων, η αναζήτηση συμβαίνει παράλληλα σε όλους τους κόμβους. Ο κόμβος που είναι ενεργός και πιο «γρήγορος» είναι αυτός που επιστρέφει τα αποτελέσματα της αναζήτησης. Ο αλγόριθμος για το consensus που χρησιμοποιείται στο Hyperledger Fabric (HLF) εξασφαλίζει ότι όλοι οι κόμβοι ανά πάσα στιγμή «βλέπουν» τα ίδια δεδομένα, διασφαλίζοντας έτσι την ακεραιότητα των δεδομένων.

Όταν τα πρώτα κριτήρια αναζήτησης στο off-chain σύστημα έχουν εφαρμοστεί και έχει γίνει η αντίστοιχη αναζήτηση από το symbIoTe, μια λίστα από προϊόντα περνάει ως είσοδος στο BaaS. Είτε υπάρχουν επιπλέον κριτήρια αναζήτησης σχετικά με την φήμη ή/και την τιμή των προϊόντων, είτε όχι, τα προϊόντα που έχουν εξαχθεί ως αποτελέσματα της πρώτης αναζήτησης από το component του symbIoTe, ανασύρονται από το blockchain, ελέγχοντας έτσι την εγκυρότητα τους και κυρίως ότι αυτά υπάρχουν και δεν έχουν εισαχθεί κα επιλεγεί προϊόντα από κακόβουλους χρήστες. Σε αυτό ακριβώς το σημείο γίνεται η κατανεμημένη αναζήτηση στο blockchain. Στη συνέχεια, όπου χρειάζεται, εφαρμόζονται τα κριτήρια της φήμης ή/και της τιμής, φιλτράροντας τα προϊόντα και επιστρέφονται μόνο αυτά που τα ικανοποιούν. Ένας αντίστοιχος μηχανισμός πραγματοποιεί την κατανεμημένη αναζήτηση για τους ομόσπονδους πόρους, με κριτήριο αναζήτησης τη φήμη τους (καθώς οι ομόσπονδοι πόροι δεν διαθέτουν κάποια τιμή), όπως παρουσιάζεται αναλυτικά στο διάγραμμα ακολουθίας στην Εικόνα 14. Τα αποτελέσματα αυτής της αναζήτησης περνούν στη συνέχεια στο μηχανισμό της διαφήμισης πόρων, που περιγράφεται στο επόμενο Κεφάλαιο 4.

Για την υλοποίηση της κατανεμημένης αναζήτησης μέσω της πλατφόρμας IoTFeds, το υποσύστημα BaaS «εκθέτει» συγκεκριμένα σημεία πρόσβασης (endpoints) μέσω REST-API και περιγράφονται παρακάτω (Πίνακας 5). Τα συγκεκριμένα endpoints περιγράφουν τη λειτουργία της αναζήτησης στο BaaS για τους ομόσπονδους πόρους.

Πίνακας 5: Endpoint που περιγράφουν τη λειτουργία της αναζήτησης πόρων στο BaaS.

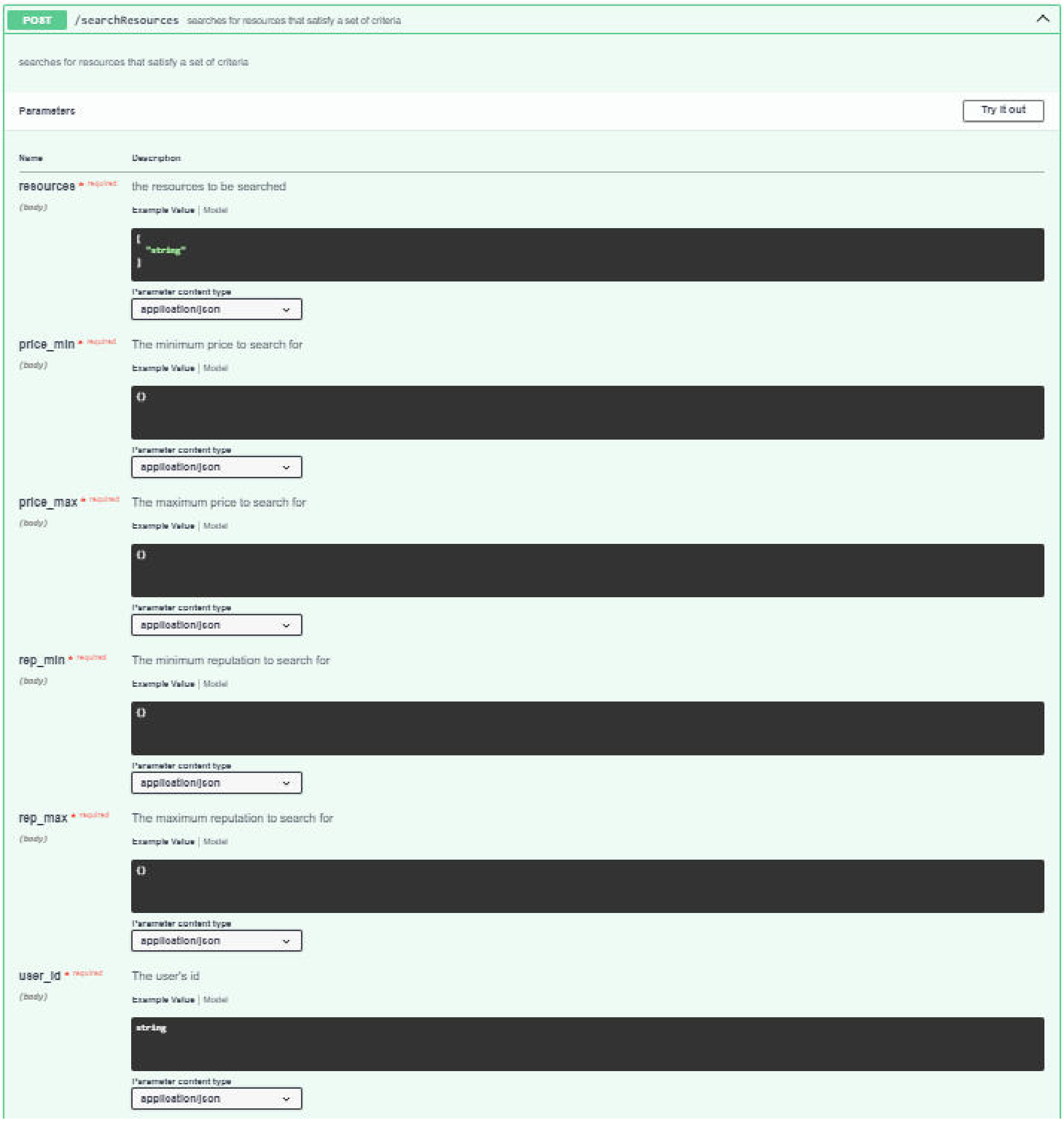
#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	searchResources	Marketplace API	BaaS	POST	/baas/products /search_resources	(Array[String], Integer, Integer, Integer, Integer, String)	(Object, Message)	Αναζήτηση IoT πόρων που ικανοποιούν τα κριτήρια.
2	REST	getResource	Marketplace API	BaaS	GET	/baas/products /get_resource_info	-	(Object, Message)	Πρόσβαση σε πληροφορίες ενός πόρου.
3	REST	getAllResources	Marketplace API	BaaS	GET	/baas/products /get_all_resource_info	-	(Object, Message)	Πρόσβαση σε πληροφορίες όλων των πόρων.
4	REST	getFederatedResources	Marketplace API	BaaS	POST	/baas/products /get_federated_resources	(String, String, String, String, Integer, String, String, String,	(Object, Message)	Πρόσβαση σε πληροφορίες όλων των πόρων μιας ομοσπονδίας.

							String, String)		

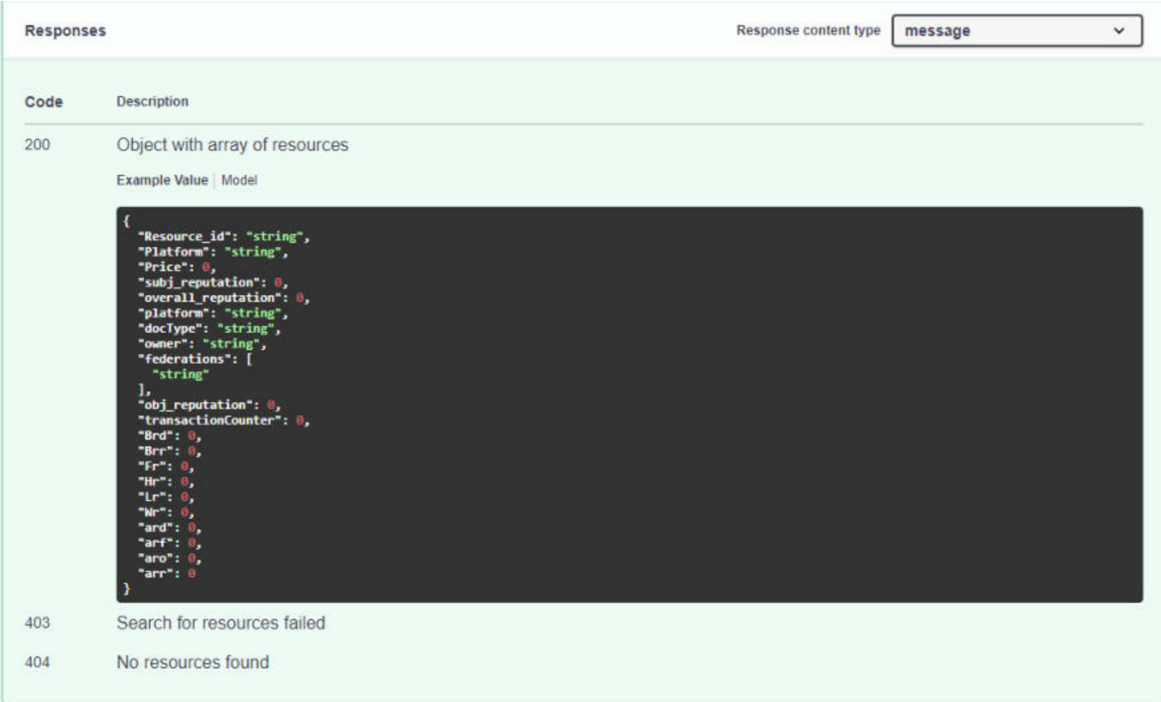
3.2.1 Αναζήτηση Ομόσπονδων Πόρων IoT

Η κατανεμημένη αναζήτηση ομόσπονδων πόρων αφορά την αναζήτησή τους με βάση το κριτήριο της φήμης τους και στη συνέχεια διαφημίζονται με βάση τον αλγόριθμο διαφήμισης που περιγράφεται στο επόμενο Κεφάλαιο 4, όπως περιγράφεται αναλυτικά στο διάγραμμα ακολουθίας στην Εικόνα 14.

Ο συγκεκριμένος αλγόριθμος δέχεται σαν είσοδο μια λίστα από ομόσπονδους πόρους, που έχουν προκύψει από μια πρώτη αναζήτηση μέσα από το symbIoTe (με βάση τα κριτήρια που υποστηρίζονται από αυτό), τα όρια της φήμης στα οποία πρέπει να βρίσκονται οι πόροι και το username του χρήστη που πραγματοποιεί την αναζήτηση. Στην περίπτωση που δεν έχει οριστεί ένα από τα δύο όρια της φήμης, αυτό παίρνει μια τιμή που είναι αδύνατον να πάρει η φήμη ενός πόρου. Για παράδειγμα, εφόσον η τιμή της φήμης για έναν πόρο κυμαίνεται από 0 έως και 1, και λείπει το άνω όριο, τότε η τιμή που θα πάρει ως είσοδο το BaaS μπορεί να είναι 2. Στις επόμενες εικόνες φαίνονται οι παράμετροι που δέχεται ως είσοδο η υπηρεσία αναζήτησης ομόσπονδων πόρων (Εικόνα 12) και επιστρέφει ένα αντικείμενο με τους ομόσπονδους πόρους που ικανοποιούν τα κριτήρια αναζήτησης (τιμή και φήμη του πόρου) (Εικόνα 13).



Εικόνα 12: Παράμετροι του endpoint για την αναζήτηση ομόσπονδων πόρων στο BaaS.



Εικόνα 13: Αντικείμενο που επιστρέφεται και περιλαμβάνει πίνακα με τους ομόσπονδους πόρους.

4 Διαφήμιση Ομόσπονδων Πόρων IoT

Στόχος του συγκεκριμένου κεφαλαίου του παραδοτέου είναι η παρουσίαση του τρόπου αλληλεπίδρασης του συστήματος φήμης και εμπιστοσύνης της IoTFeds πλατφόρμας με το μηχανισμό διαφήμισης που υλοποιείται στο υποσύστημα BaaS. Οι μηχανισμοί φήμης και εμπιστοσύνης, καθώς και ο τρόπος υπολογισμού του αντικειμενικού βαθμού των πιλοτικών εφαρμογών και του υποκειμενικού βαθμού των προϊόντων, θα αναλυθούν εκτενέστερα στο επόμενο παραδοτέο Π2.3 – «Αναφορά Μηχανισμών Φήμης και Εμπιστοσύνης».

4.1 Αλληλεπίδραση Φήμης και Εμπιστοσύνης με Διαφήμιση Ομόσπονδων Πόρων

Στις αρχές του Διαδικτύου, ο καθορισμός μιας πιθανής κακόβουλης συμπεριφοράς μιας οντότητας δεν θεωρούνταν πρόβλημα, καθώς η κοινότητα του Διαδικτύου αποτελούνταν από ομάδες και χρήστες με κοινούς στόχους και ισχυρή μεταξύ τους εμπιστοσύνη. Οι κακόβουλες συμπεριφορές εμφανίστηκαν αφού η συγκεκριμένη τεχνολογία έγινε διαθέσιμη και για το ευρύ κοινό και άρχισε να χρησιμοποιείται για εμπορικούς σκοπούς. Συνεπώς, μπορεί το Διαδίκτυο να προσφέρει νέες ευκαιρίες και ευκολία στις αλληλεπιδράσεις με εντελώς άγνωστα άτομα, οι οποίες μπορεί να είναι ενημερωτικές και προσοδοφόρες, ωστόσο μπορεί να ενέχουν και κάποιο ρίσκο. Για το σκοπό αυτό, τα σύγχρονα συστήματα διαχείρισης και επεξεργασίας δεδομένων περιλαμβάνουν κατάλληλους μηχανισμούς φήμης και εμπιστοσύνης που καθιστούν δυνατή την προστασία των δεδομένων στο Διαδίκτυο.

Πιο συγκεκριμένα, η εμπιστοσύνη αποτελεί μια σχέση αλληλεπίδρασης μεταξύ δύο μερών, του εκχωρητή εμπιστοσύνης (trustor) και του αποδέκτη εμπιστοσύνης (trustee) (Jøsang, Trust and reputation systems, 2007), ο οποίος μπορεί να είναι μια οποιαδήποτε οντότητα, όπως κάποιο άτομο, ένας οργανισμός ή φυσική οντότητα, ακόμα και μια αφηρημένη έννοια όπως πληροφορίες ή ένα κρυπτογραφικό κλειδί (Jøsang, The right type of trust for distributed systems, 1996). Μια σχέση εμπιστοσύνης ισχύει για ένα συγκεκριμένο σκοπό ή τομέα δράσης, όπως ενδεικτικά ένα «έμπιστο» κρυπτογραφικό κλειδί ή η παροχή «αξιόπιστων πληροφοριών» σε ένα λήμμα στη σελίδα της Wikipedia, ενώ αμοιβαία εμπιστοσύνη υφίσταται όταν και τα δύο μέρη εμπιστεύονται το ένα το άλλο με τον ίδιο σκοπό, γεγονός που είναι εφικτό μόνο όταν και τα δύο μέρη αποτελούν φυσικές οντότητες.

Παράλληλα, οι υπηρεσίες του Διαδικτύου λειτουργούν σε πολύ μεγάλη κλίμακα, επιτρέποντας σχεδόν ανώνυμες αλληλεπιδράσεις. Ωστόσο, η φήμη στις συγκεκριμένες περιπτώσεις παίζει ιδιαίτερα σημαντικό ρόλο. Ένα σύστημα φήμης είναι ικανό να συλλέγει, να διανέμει και να συγκεντρώνει κριτικές (feedback) σχετικά με προηγούμενες συμπεριφορές των συμμετεχόντων σε αυτό. Καθώς οι συμμετέχοντες γνωρίζονται ελάχιστα ή και καθόλου μεταξύ τους, στόχος των συγκεκριμένων συστημάτων είναι η υποβοήθηση των συμμετεχόντων ώστε να μπορέσουν να αποφασίσουν ποιον να εμπιστευτούν, η ενθάρρυνση της αξιόπιστης συμπεριφοράς και η αποτροπή της συμμετοχής όσων είναι ανειδίκευτοι ή αναξιόπιστοι σε αυτά (Resnick, Kuwabara, Zeckhauser, & Friedman, 2000).

Οι εφαρμογές αγορών δεδομένων απαιτούν κατάλληλα συστήματα αξιολόγησης της ποιότητας των παρεχόμενων προϊόντων και υπηρεσιών, καθώς επίσης και των παρόχων αυτών. Υπάρχει μεγάλη ποικιλία συστημάτων αξιολόγησης που εφαρμόζονται στις σύγχρονες αγορές δεδομένων και περιλαμβάνουν είτε κλιμακωτές (π.χ. από το 1 έως το 5), είτε δυαδικές βαθμολογίες (π.χ. «μου αρέσει»/«δε μου αρέσει»). Στα πλαίσια του έργου IoTFeds, το προτεινόμενο σύστημα διαφήμισης είναι άρρηκτα συνδεδεμένο με τη φήμη του εκάστοτε IoT πόρου. Όπως σε διάφορες περιπτώσεις εφαρμογής συστημάτων φήμης για αγορές δεδομένων, έτσι και στην IoTFeds πλατφόρμα, περιλαμβάνονται δύο οντότητες, η οντότητα που προσφέρει μια αξιολόγηση (reviewer), ο οποίος είναι ο καταναλωτής, και αυτή που δέχεται μια αξιολόγηση (reviewee), ο οποίος είναι ο πάροχος των δεδομένων.

Για τις ανάγκες του έργου IoTFeds ορίζονται δύο τύποι μετρικών που χρησιμοποιούνται για την αξιολόγηση/βαθμολόγηση των πόρων και των παρόχων δεδομένων και διακρίνονται σε αντικειμενικές και υποκειμενικές μετρικές, ο τρόπος υπολογισμού και χρήση των οποίων αναλύεται εκτενώς στο επόμενο παραδοτέο Π2.3 – «Αναφορά Μηχανισμών Φήμης και Εμπιστοσύνης». Κάθε πιλοτική εφαρμογή που είναι εγγεγραμμένη στην IoTFeds πλατφόρμα προσφέρει ένα σύνολο από μετρικές αξιολόγησης της ποιότητας της παρεχόμενης υπηρεσίας (QoS), οι οποίες περιλαμβάνουν μετρικές όπως η καθυστέρηση, το throughput, η διαθεσιμότητα, ο χρόνος απόκρισης του συστήματος ή συνδυασμό αυτών. Στη συνέχεια, γίνεται υπολογισμός του αντικειμενικού βαθμού κάθε εφαρμογής βάσει των παρεχόμενων αυτών μετρικών περιοδικά.

Από την άλλη πλευρά, οι υποκειμενικές μετρικές σχετίζονται με κάθε τύπο υπηρεσίας και αντιστοιχίζονται σε ένα προφίλ ποιότητας εμπειρίας (QoE) του καταναλωτή για κάθε πόρο που περιλαμβάνεται στην IoTFeds πλατφόρμα και περιλαμβάνουν μετρικές όπως η ευχρηστία, η σχέση ποιότητας-τιμής, η πληρότητα κ.λπ. Σε αντίθεση, επομένως, με τις αντικειμενικές μετρικές που σχετίζονται με τη λειτουργία της κάθε πιλοτικής εφαρμογής της πλατφόρμας ξεχωριστά, οι υποκειμενικές αφορούν την αξιολόγηση της εμπειρίας του καταναλωτή μετά την αγορά κάποιου πόρου. Ως αποτέλεσμα, ο υποκειμενικός βαθμός υπολογίζεται για κάθε μία αξιολόγηση πόρου που κατατίθεται στην πλατφόρμα από έναν καταναλωτή. Οι αξιολογήσεις αυτές, στη συνέχεια, συγκεντρώνονται στο υποσύστημα BaaS, από όπου υπολογίζεται η βαθμολογία της φήμης κάθε πόρου (reputation score). Ως αποτέλεσμα, κάθε IoT πόρος που περιλαμβάνεται στην αγορά της IoTFeds πλατφόρμας διαθέτει μια βαθμολογία φήμης, η οποία λειτουργεί ως μια ένδειξη αξιοπιστίας του συγκεκριμένου πόρου, και μπορεί μελλοντικά να χρησιμοποιηθεί ως παράγοντας επιλογής ή απόρριψης ενός συγκεκριμένου πόρου και από άλλους καταναλωτές.

4.2 Μηχανισμός Διαφήμισης Ομόσπονδων Πόρων στην IoTFeds Πλατφόρμα

Στον πίνακα που ακολουθεί (Πίνακας 6) παρουσιάζεται ο ψευδοκώδικας του αλγορίθμου ταξινόμησης πόρων IoT που δημιουργήθηκε για το BaaS. Πιο συγκεκριμένα, ο αλγόριθμος δέχεται ως είσοδο έναν πίνακα με objects που περιλαμβάνει το ID του κάθε πόρου και την αντίστοιχη φήμη του ($\{id, rep\_score\}$) και εξάγει ένα δεύτερο object που περιλαμβάνει τους ταξινομημένους πόρους. Τα δύο αυτά objects περιλαμβάνονται στις λίστες $resourceList$ και $sortedResourceList$, αντίστοιχα.

Όσον αφορά τη ροή του αλγορίθμου, αρχικά, γίνεται διαχωρισμός των IoT πόρων από τη βαθμολογία φήμης τους σε δύο ξεχωριστές λίστες, $items$ και $weights$, αντίστοιχα, οι οποίες θα πρέπει να έχουν το ίδιο μέγεθος. Στη συνέχεια, για όλα τα στοιχεία της λίστας αθροίζονται τα βάρη όλων των πόρων που υπάρχουν στη λίστα τη δεδομένη στιγμή ($cumulativeWeights[]$), αθροίζεται το μέγιστο συνολικό βάρος ($maxCumulativeWeight$) των βαρών της λίστας και γίνεται ταξινόμηση όλων των πόρων βάσει του βάρους τους ($rep\_score/maxCumulativeWeight$). Σημειώνεται πως σε κάθε επανάληψη, το αθροιστικό βάρος αλλάζει καθώς από την αρχική λίστα αφαιρείται κάθε φορά ο πόρος με το μεγαλύτερο βάρος και εισάγεται με τη σειρά στη νέα λίστα $sortedResourceList$. Τέλος, γίνεται υπολογισμός της μεταβλητής $randomNumber$, η οποία συγκρίνεται με το αθροιστικό βάρος του κάθε πόρου. Σε περίπτωση που το βάρος του πόρου είναι μεγαλύτερο ή ίσο από τη μεταβλητή $randomNumber$, ο αλγόριθμος αφαιρεί τον συγκεκριμένο πόρο από την αρχική λίστα και τον περνάει στη νέα λίστα $sortedResourceList$. Η διαδικασία αυτή επαναλαμβάνεται μέχρι να περαστεί και ο τελευταίος εναπομείναν πόρος της αρχικής λίστας.

Ο αλγόριθμος τελικά επιστρέφει το object με τον πίνακα που περιέχει τους ταξινομημένους πόρους της αρχικής λίστας, όπως αυτή έχει προκύψει από την αναζήτηση του BaaS.

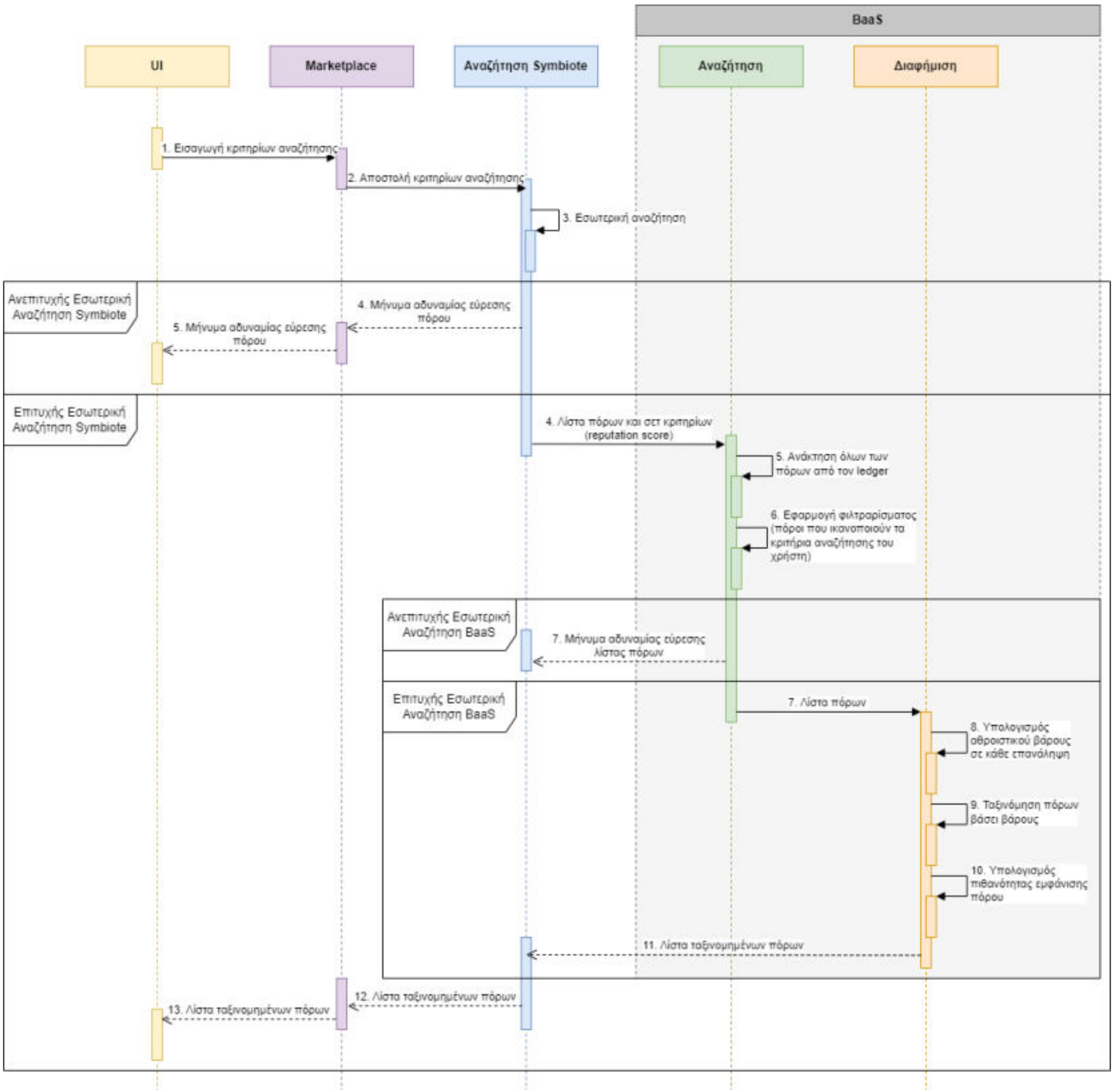
Πίνακας 6: Ψευδοκώδικας για τον αλγόριθμο διαφήμισης πόρων IoT του BaaS.

$resourceList[]$:	$List\ of\ resources\ with\ their\ reputation\ scores$
$random\_factor$:	$Generation\ of\ random\ results$
$maxCumulativeWeight$:	$Maximum\ cumulative\ weight\ of\ the\ resources\ in\ the\ resourceList$
$sortedResourceList[]$:	$List\ of\ sorted\ resources$

```
function weightedRandom(items, weights)
        if items.length != weights.length
                throw error "Resources and weights must be of the same size"

        if items.length == 0:
                return

        cumulativeWeights = [];
        for i in range(0, len(weights)):
                cumulativeWeights[i] = weights[i] + (cumulativeWeights[i − 1] || 0)

        maxCumulativeWeight = cumulativeWeights[cumulativeWeights.length − 1]

        sortedResources = items.sort((a, b) =>
        b.rep_score/maxCumulativeWeight – a.rep_score/maxCumulativeWeight)

        randomNumber = maxCumulativeWeight ∗ Math.random() ∗ random_factor

        for itemIndex in range(0, len(sortedResources)):
                if cumulativeWeights[itemIndex] >= randomNumber:
                        sortedResourceList.push(items[itemIndex].id)
                        products.splice(itemIndex, 1)
                        weights.splice(itemIndex, 1)
                        weightedRandom(items, weights)

sortedResourceList = []
random_factor = 1/3
weightedRandom(resourceList, resourceList.map(resource => resource.rep_score))
```

4.3 Ακολουθία Αναζήτησης και Διαφήμισης Ομόσπονδων Πόρων IoT

Στο διάγραμμα ακολουθίας στην Εικόνα 14 περιγράφεται η συνολική ροή των επιμέρους διαδικασιών που παρουσιάστηκαν αναλυτικά στα Κεφάλαια 3 και 4, από την εισαγωγή των κριτηρίων αναζήτησης των IoT πόρων από το χρήστη στο UI, μέχρι την τελική επιστροφή των ταξινομημένων αποτελεσμάτων στο symbIoTe.



Εικόνα 14: Διάγραμμα ακολουθίας για την αναζήτηση και τη διαφήμιση των πόρων IoT.

Πιο συγκεκριμένα, τα βήματα που παρουσιάζονται στο διάγραμμα ακολουθίας στην Εικόνα 14 για τους μηχανισμούς αναζήτησης και διαφήμισης πόρων IoT του BaaS έχουν ως εξής:

1. Εισαγωγή των κριτηρίων αναζήτησης πόρων από το UI στο marketplace.
2. Αποστολή των κριτηρίων αναζήτησης πόρων από το marketplace στο marketplace backend (αναζήτηση symbIoTe).
3. Εσωτερική αναζήτηση στο symbIoTe για τους συγκεκριμένους πόρους.
4. Σε περίπτωση που οι συγκεκριμένοι πόροι δεν μπορούν να βρεθούν από το symbIoTe, επιστρέφεται στο marketplace μήνυμα αδυναμίας εύρεσης του συγκεκριμένου πόρου.
5. Το ίδιο μήνυμα επιστρέφεται από το marketplace στο UI για εμφάνιση στο χρήστη.

Σε αντίθετη περίπτωση, όπου η εύρεση του συγκεκριμένου πόρου από το symbIoTe είναι επιτυχής, η διαδικασία συνεχίζει ως εξής:

4. Αποστολή της λίστας των πόρων IoT και του σετ των κριτηρίων (βαθμολογία φήμης) από το symbIoTe στο BaaS.
5. Ανάκτηση από το BaaS όλων των πόρων από τον ledger.
6. Εφαρμογή κατάλληλου φιλτραρίσματος στη λίστα για την εύρεση των πόρων που ικανοποιούν τα κριτήρια αναζήτησης που ορίστηκαν από το χρήστη.

7. Σε περίπτωση αδυναμίας εύρεσης της λίστας των πόρων που ικανοποιούν τα κριτήρια αναζήτησης του χρήστη στον ledger, επιστρέφεται μήνυμα αδυναμίας εύρεσης της λίστας των πόρων από τη μονάδα αναζήτησης του BaaS στο symbIoTe.

Εναλλακτικά, σε περίπτωση εύρεσης της λίστας των πόρων από τον ledger που ικανοποιούν τα κριτήρια αναζήτησης που ορίστηκαν από το χρήστη, η διαδικασία της αναζήτησης και της διαφήμισης τερματίζει ως εξής:

7. Αποστολή της λίστας των επιλεγμένων πόρων στη μονάδα της διαφήμισης του BaaS.
8. Υπολογισμός σε κάθε επανάληψη του αθροιστικού βάρους των πόρων που βρίσκονται στη λίστα προς ταξινόμηση.
9. Ταξινόμηση των πόρων της λίστας βάσει του βάρους τους (βαθμολογία φήμης/αθροιστικό βάρος).
10. Υπολογισμός της πιθανότητας εμφάνισης κάθε πόρου της λίστας, σύμφωνα με τον τύπο που παρουσιάζεται στον ψευδοκώδικα του αλγορίθμου ταξινόμησης (Πίνακας 6).
11. Αποστολή από το BaaS στο symbIoTe της λίστας των ταξινομημένων πόρων για εμφάνιση στο χρήστη.
12. Αποστολή από το symbIoTe στο marketplace της λίστας των ταξινομημένων πόρων για εμφάνιση στο χρήστη.
13. Εμφάνιση της λίστας των ταξινομημένων πόρων στο χρήστη μέσω του UI.

5 Σύνθεση Προϊόντων στην IoTFeds Πλατφόρμα

Τα προϊόντα στην IoTFeds πλατφόρμα αποτελούν μια από τις βασικές οντότητες, καθώς σε αυτές στηρίζεται ένα μεγάλο μέρος των λειτουργιών της, όπως για παράδειγμα η δυνατότητα αγοράς τους μέσα από το Marketplace. Ένα προϊόν αποτελείται από έναν αριθμό ομόσπονδων πόρων που συνδυάζονται για να παρέχουν στους χρήστες ένα σύνολο από δεδομένα που προέρχονται από πληθώρα IoT πόρων. Η σύνθεση ενός προϊόντος λαμβάνει χώρα στο marketplace, ωστόσο είναι απαραίτητη η καταγραφή και η αποθήκευσή του στο blockchain μέσω του BaaS για τη διαχείριση των συναλλαγών, την τιμολόγηση κ.α. Παρακάτω περιγράφεται η λειτουργία της σύνθεσης και δημιουργίας ενός προϊόντος.

5.1 Σύνθεση Προϊόντος στο off-chain Σύστημα (Marketplace)

Η σύνθεση ενός προϊόντος είναι δυνατή μέσα από μία ομοσπονδιακή αγορά από ένα μέλος της ομοσπονδίας. Το προϊόν που δημιουργείται μπορεί επιπλέον να καταχωρηθεί και στην καθολική αγορά για χρήση από τρίτους (αγορά από οποιοδήποτε IoTFeds μέλος). Ένας πάροχος δεδομένων μπορεί να καταχωρήσει στην IoTFeds πλατφόρμα οποιοδήποτε IoT πόρο (πηγή δεδομένων) επιθυμεί και να επιλέξει τις ομοσπονδίες στις οποίες θα διαμοιράσει καθεμία πηγή δεδομένων όπως περιγράφηκε στις προηγούμενες ενότητες. Ο παρακάτω πίνακας συνοψίζει τα σημεία πρόσβασης (endpoints) που παρέχονται από τα στοιχεία λογισμικού marketplace μέσω REST-API (Πίνακας 7). Οι διεπαφές περιγράφονται με περισσότερη λεπτομέρεια στις παραγράφους που ακολουθούν. Η υλοποίησή τους περιλαμβάνει την επικοινωνία με τα αντίστοιχα endpoints του BaaS για την καταγραφή ή έλεγχο της αντίστοιχης πληροφορίας στο on-chain σύστημα που περιγράφονται σε επόμενη ενότητα.

Πίνακας 7: Διεπαφές marketplace για τη σύνθεση προϊόντων.

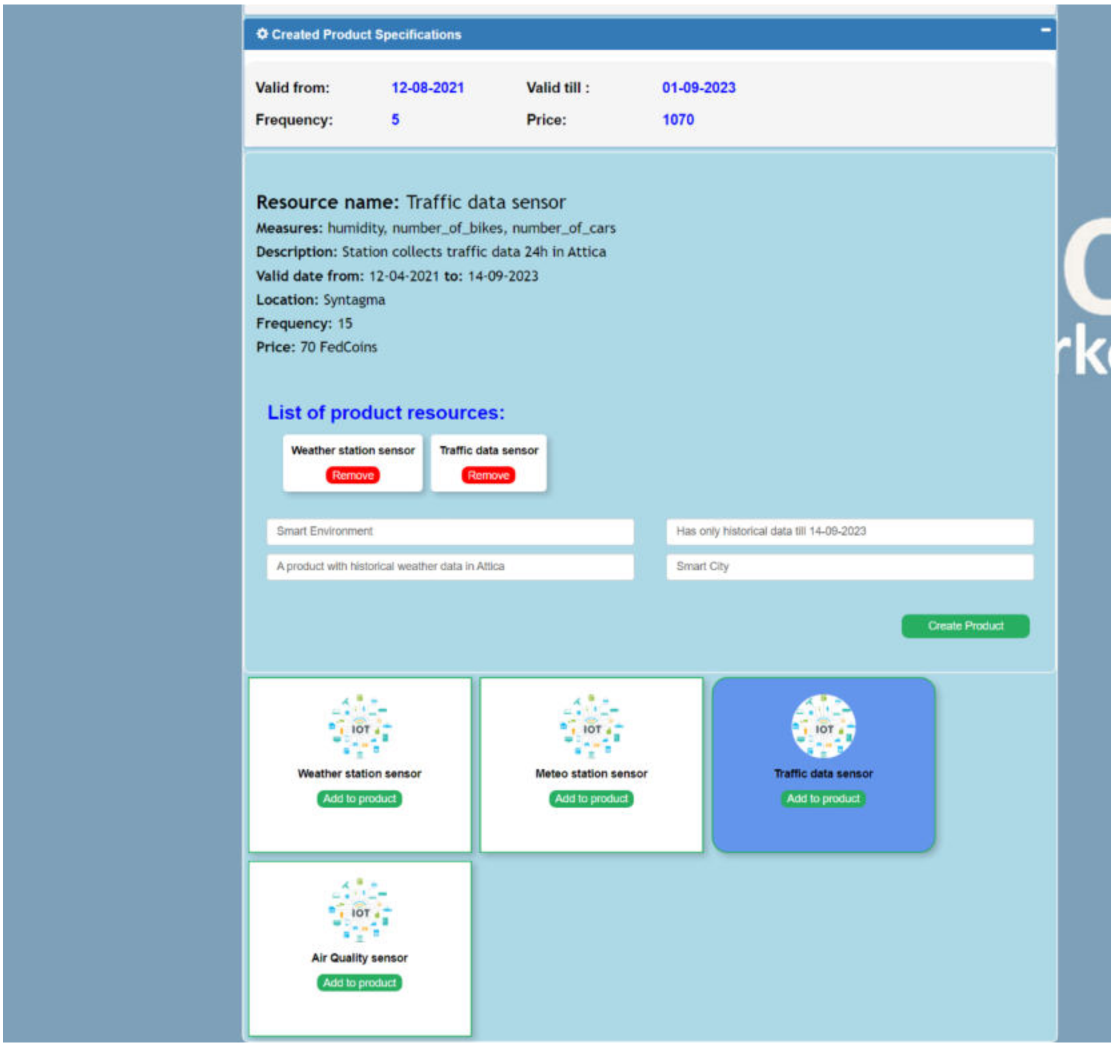
#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	createProdut	IoTFeds	fed member marketplace	POST	/marketplace/product	String productCreateDto	Message	Αίτηση δημιουργίας προϊόντος εντός της ομοσπονδιακής αγοράς (και προώθησή του στην καθολική αγορά)
2	REST	deleteProduct	IoTFeds	fed member marketplace	DELETE	/marketplace/product/{id}	String productCreateDto	Message	Αίτηση διαγραφής προϊόντος από το σύστημα

5.1.1 Σύνθεση προϊόντος σε ομοσπονδιακή αγορά και προώθησή του στην καθολική αγορά

Ο χρήστης μπορεί να συνθέσει ένα προϊόν σε μία ομόσπονδη αγορά μέσω της γραφικής διεπαφής αγοράς όπως φαίνεται στην παρακάτω εικόνα:

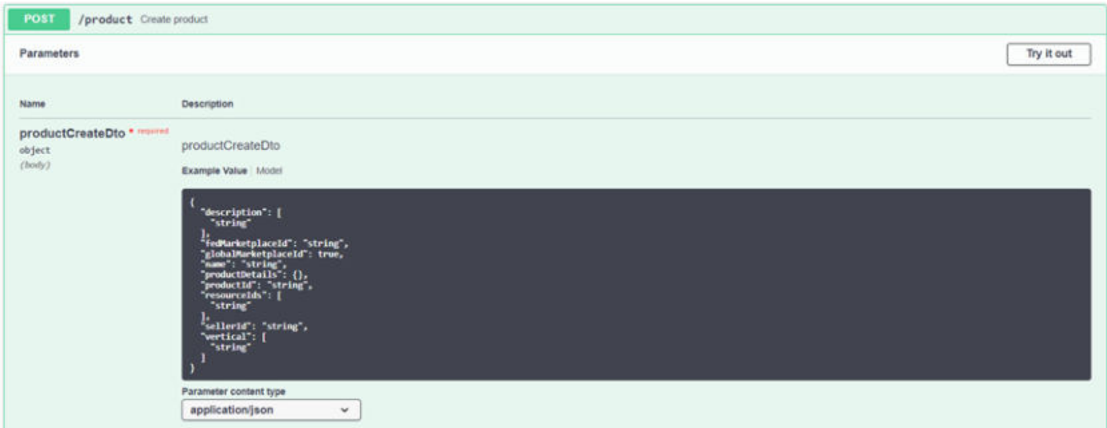
Εικόνα 15: Επιλογή για σύνθεση προϊόντος.

Ο χρήστης επιλέγει από τις πηγές δεδομένων (πραγματοποιώντας την αναζήτηση που περιγράφεται στην Εικόνα 9 στο Κεφάλαιο 3) της επισκεπτόμενης ομόσπονδης αγοράς εκείνες που θέλει να συμπεριλάβει στο προϊόν (“add to product”) προς δημιουργία και συμπληρώνει τα χαρακτηριστικά του προϊόντος όπως φαίνεται στην παρακάτω εικόνα:



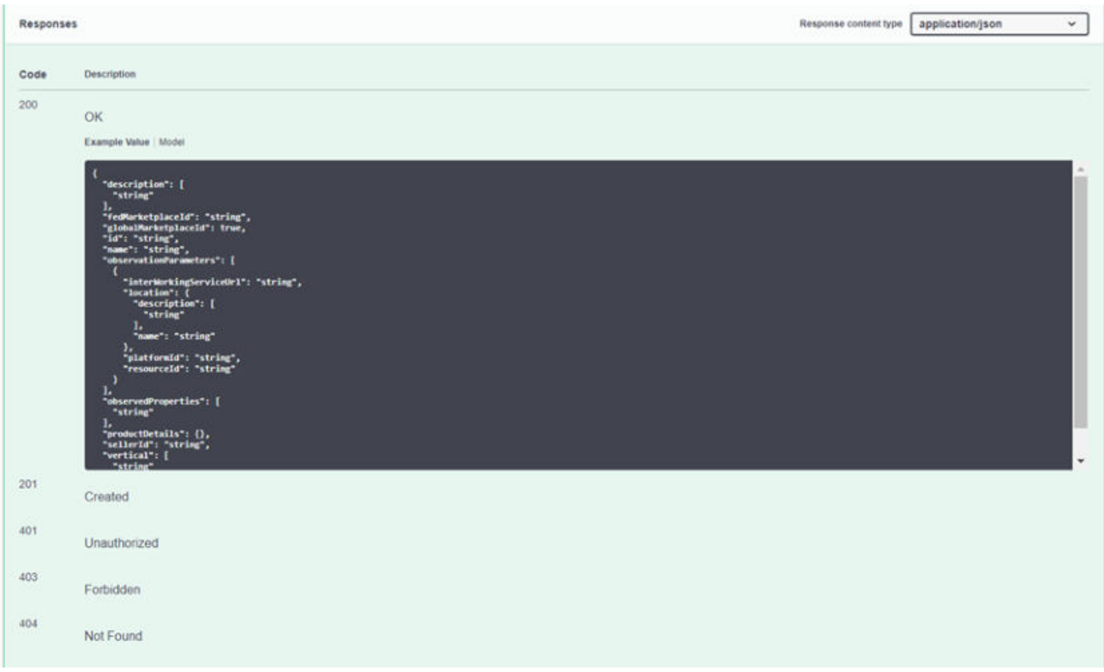
Εικόνα 16: Επιλογή χαρακτηριστικών προϊόντος.

Το ερώτημα για τη δημιουργία ενός προϊόντος προωθείται στη διεπαφή που περιγράφεται στην Εικόνα 17. Η διεπαφή δέχεται ως είσοδο το όνομα (name) και την περιγραφή (description) του προϊόντος, το αναγνωριστικό της ομόσπονδης αγοράς στην οποία ανήκει (fedMarketplaceId). Επιπλέον, ο δημιουργός του προϊόντος (sellerId) καθορίζει αν το προϊόν θα διατεθεί στην καθολική αγορά (globalMarketplaceId). Τέλος, το πεδίο vertical αφορά την ένταξη του προϊόντος σε μια κατηγορία ενδιαφέροντος. Άλλες λεπτομέρειες του προϊόντος μπορούν να περιγραφούν στο πεδίο productDetails. Η καταχώρηση του προϊόντος περιλαμβάνει και την ενημέρωση στο BaaS σύστημα όπως περιγράφεται στην ενότητα 5.2. Η διεπαφή που περιγράφηκε καλείται κατά την διαδικασία σύνθεσης προϊόντος στη γραφική διεπαφή χρήστη της ομόσπονδης αγοράς. Η διεπαφή αυτή ενσωματώνει την επικοινωνία με το αντίστοιχο endpoint του BaaS που περιγράφεται στην ενότητα 5.2. Κατά τη διαδικασία σύνθεσης του προϊόντος πραγματοποιείται επιπλέον από το BaaS έλεγχος των κανόνων ομοσπονδίας σχετικά με την προώθηση του προϊόντος στην καθολική αγορά (με βάση το product visibility που αναλύεται στο Π3.2).



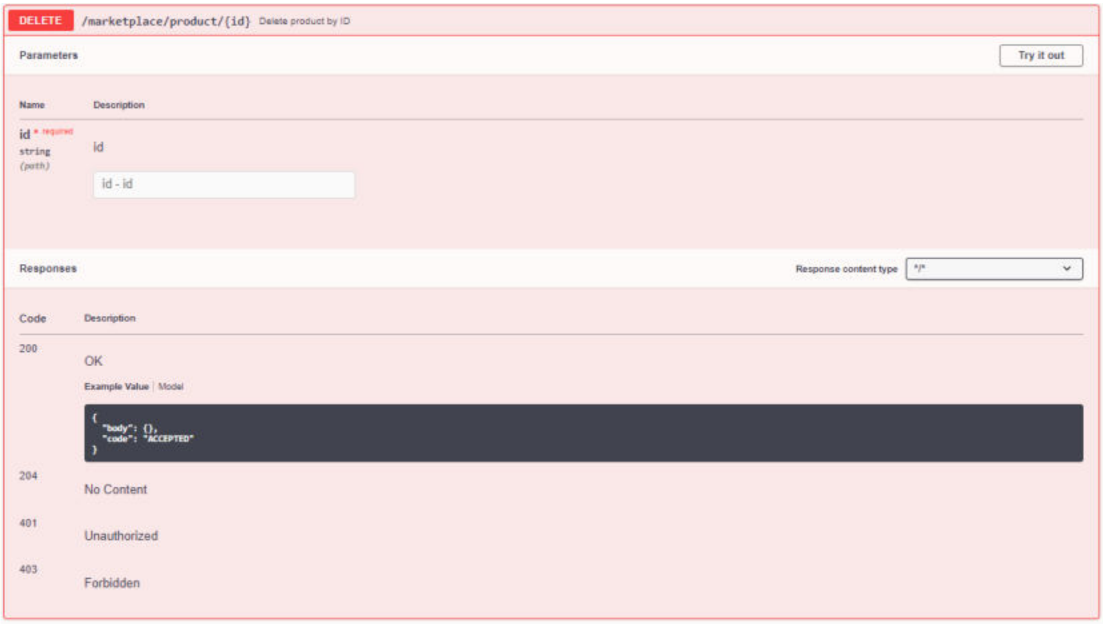
Εικόνα 17: Σύνθεση προϊόντος.

Το αίτημα επιστρέφει τα στοιχεία της καταχώρησης και αντίστοιχο μήνυμα επιτυχίας/αποτυχίας όπως φαίνεται στην Εικόνα 18.



Εικόνα 18:Απάντηση αιτήματος σύνθεσης προϊόντος στο marketplace.

Ένα προϊόν μπορεί επιπλέον να αφαιρεθεί από τον δημιουργό του από μία ομόσπονδη αγορά επιλέγοντας το κουμπί ("Delete") στη λίστα των διαθέσιμων προϊόντων. Το ερώτημα προωθείται στο παρακάτω endpoint με παράμετρο το αναγνωριστικό του προϊόντος:



Εικόνα 19:Διαγραφή προϊόντος από το IoTFeds σύστημα.

Η παραπάνω διεπαφή ενσωματώνει την απαραίτητη επικοινωνία με το BaaS το οποίο επιπλέον ελέγχει αν το προϊόν συνδέεται με κάποιο έγκυρο κουπόνι ώστε να επιτραπεί η διαγραφή του μόνο σε περίπτωση που το προϊόν δεν χρησιμοποιείται από κάποιον χρήστη.

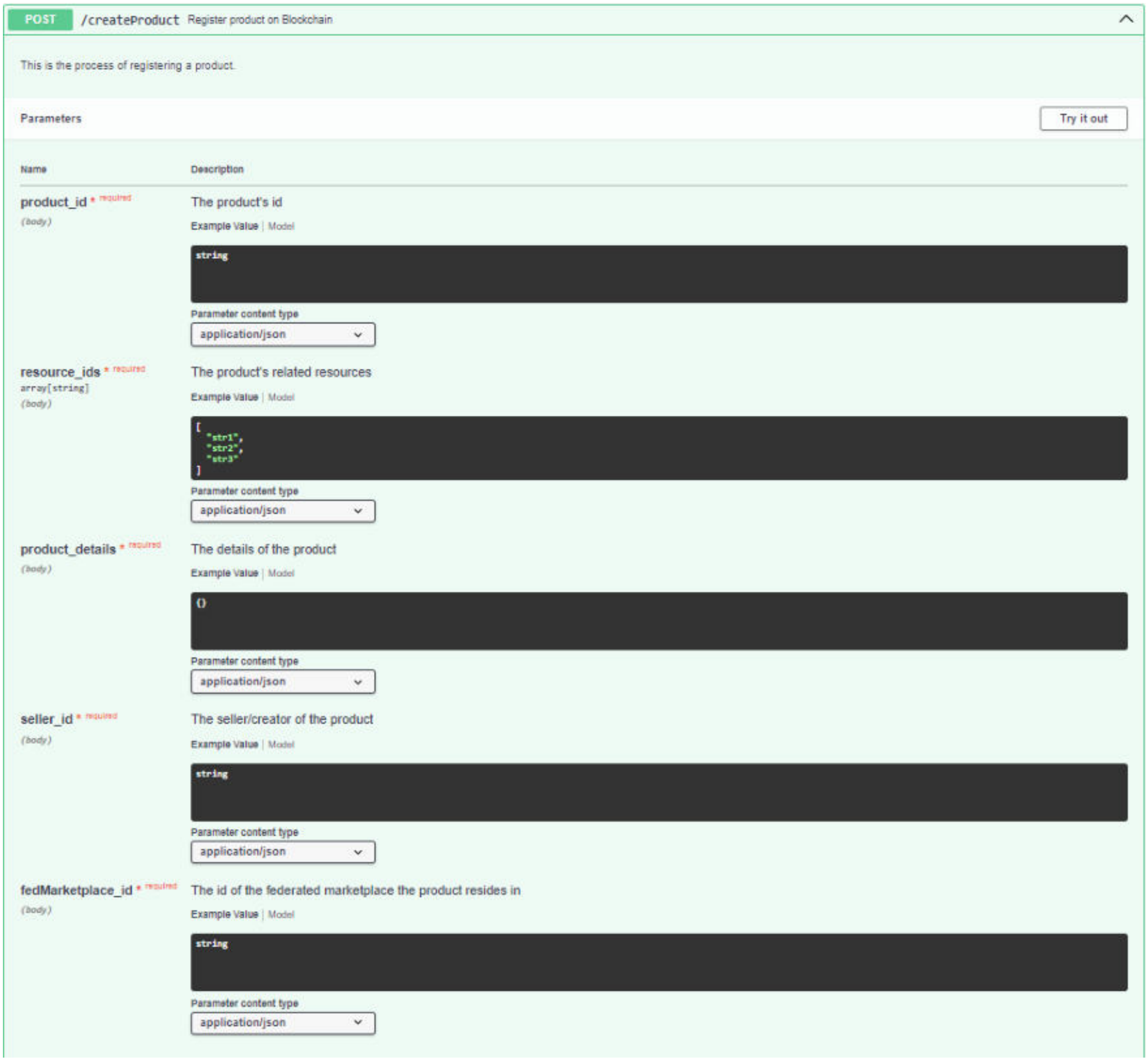
5.2 Καταχώρηση προϊόντος στο on-chain σύστημα (BaaS)

Από τη μεριά του BaaS, η δημιουργία ενός προϊόντος ξεκινά αμέσως μετά τη στιγμή που ο χρήστης έχει ορίσει όλα τα απαραίτητα στοιχεία του, όπως για παράδειγμα από ποιους ομόσπονδους πόρους θα αποτελείται, διάφορες λεπτομέρειες σχετικά με το προϊόν, όπως το είδος του, η τιμή αγοράς του και το αν διατίθεται μόνο σε κάποια ομοσπονδιακή αγορά ή και στην καθολική αγορά. Για την υλοποίηση αυτής της λειτουργίας έχει δημιουργεί η αντίστοιχη υπηρεσία που αντιστοιχεί σε ένα endpoint (Πίνακας 8).

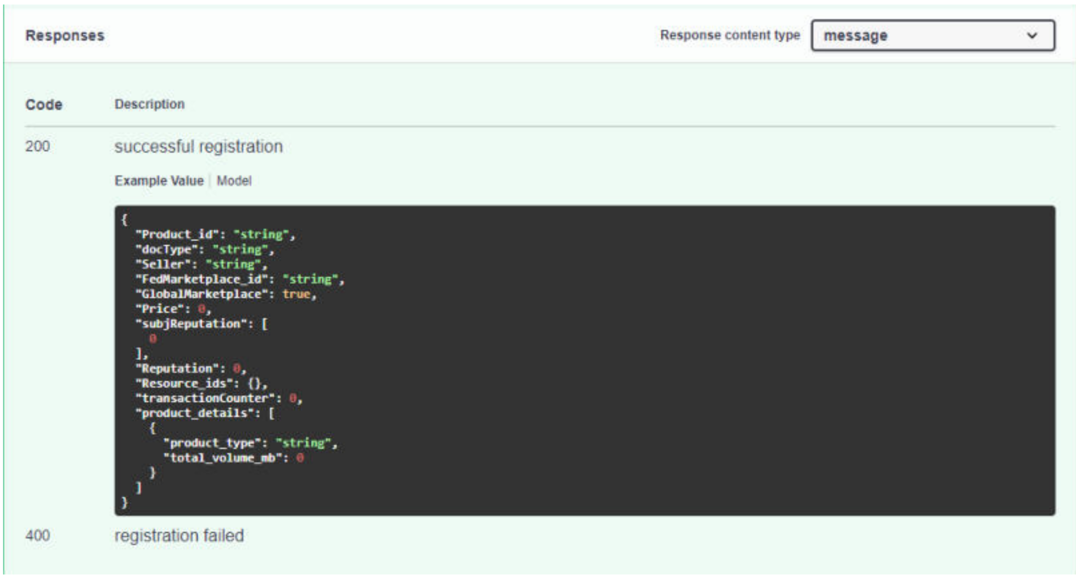
Πίνακας 8: Endpoint που περιγράφουν τη λειτουργία της σύνθεσης προϊόντος στο BaaS.

#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	createProduct	marketplace API	BaaS	POST	/baas/products /create_product	(String, Array[String], Object, String, String,)	(Object, Message)	Αίτηση δημιουργίας ενός προϊόντος στο blockchain

Η δημιουργία ενός προϊόντος στο BaaS δέχεται ως είσοδο το αναγνωριστικό του προϊόντος, την τιμή του, μια λίστα με τους πόρους που το αποτελούν, ένα αντικείμενο που μπορεί να περιέχει πληροφορίες σχετικές με το προϊόν, το username του χρήστη που έχει δημιουργήσει το προϊόν και συνεπώς τον πωλητή του, το αναγνωριστικό της ομοσπονδιακής αγοράς, όπως φαίνεται στην Εικόνα 20. Εφόσον η καταγραφή του προϊόντος στο blockchain είναι επιτυχής επιστρέφει το αντικείμενο που περιγράφει το καινούριο προϊόν, ενώ σε αντίθετη περίπτωση επιστρέφει ένα μήνυμα αποτυχίας, όπως φαίνεται στις παρακάτω εικόνες (Εικόνα 21).



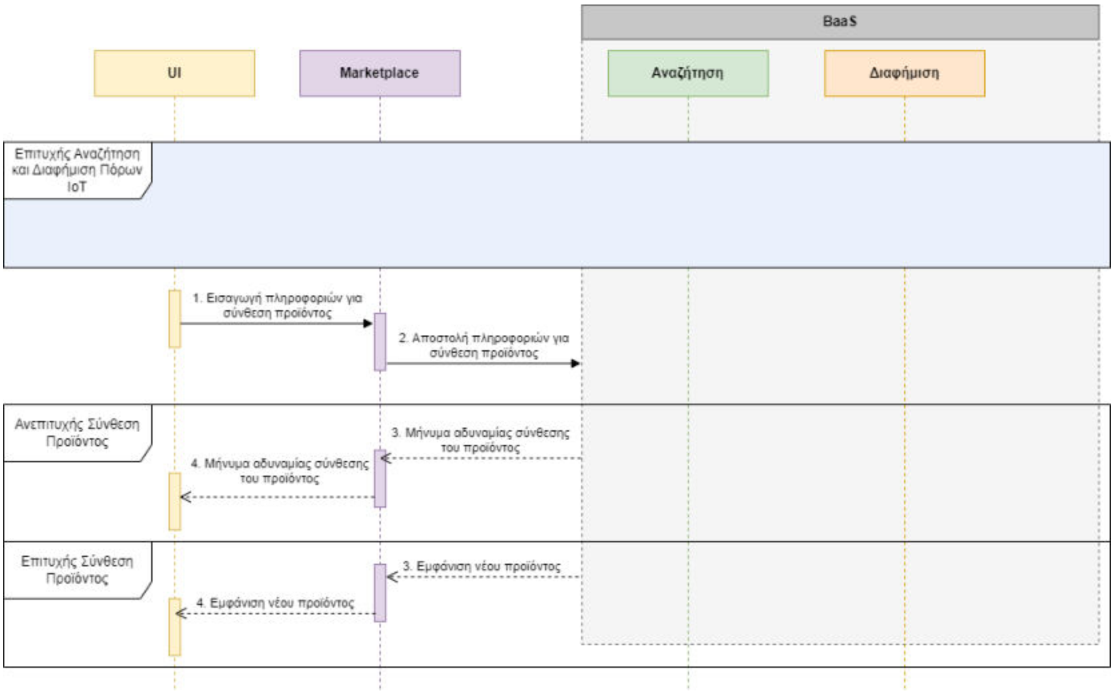
Εικόνα 20: Παράμετροι του endpoint για τη δημιουργία ενός προϊόντος στο BaaS.



Εικόνα 21: Αντικείμενο που επιστρέφεται και περιγράφει το νέο προϊόν.

5.3 Ακολουθία Σύνθεσης Προϊόντων

Στο διάγραμμα ακολουθίας στην Εικόνα 22 περιγράφεται η συνολική ροή της διαδικασίας σύνθεσης ενός προϊόντος στην IoTFeds πλατφόρμα, όπως αυτή έπεται των διαδικασιών αναζήτησης και διαφήμισης πόρων IoT που παρουσιάστηκαν στα προηγούμενα Κεφάλαια 3 και 4.



Εικόνα 22: Διάγραμμα ακολουθίας για τη σύνθεση προϊόντος.

Η λεπτομερής περιγραφή της διαδικασίας σύνθεσης ενός προϊόντος στην IoTFeds πλατφόρμα, όπως αυτή παρουσιάζεται στο διάγραμμα ροής στην Εικόνα 22, προϋποθέτει την αναζήτηση και την επιτυχή επιστροφή των IoT πόρων από το BaaS πίσω στο χρήστη. Στη συνέχεια, ο χρήστης έχει πλέον τη δυνατότητα να συνθέσει ένα προϊόν ως εξής:

1. Εισαγωγή στο marketplace των απαραίτητων πληροφοριών για τη σύνθεση του προϊόντος.
2. Αποστολή των πληροφοριών αυτών από το marketplace backend στο BaaS.
3. Σε περίπτωση ανεπιτυχούς σύνθεσης του προϊόντος, επιστρέφεται από το BaaS στο marketplace backend μήνυμα αδυναμίας σύνθεσης του προϊόντος.
4. Και τέλος, το ίδιο μήνυμα επιστρέφεται από το marketplace στο UI για ενημέρωση του χρήστη.

Αντίθετα, σε περίπτωση που η σύνθεση του προϊόντος από το BaaS είναι επιτυχής, η διαδικασία της σύνθεσης τερματίζει ως εξής:

3. Εμφάνιση του νέου προϊόντος από το BaaS στο marketplace backend.
4. Αποστολή του νέου προϊόντος από το marketplace στο UI για εμφάνιση στο χρήστη.

6 Ανακάλυψη Προϊόντων στην IoTFeds Πλατφόρμα

Σε συνδυασμό με τους μηχανισμούς ανακάλυψης ομόσπονδων πόρων IoT, η IoTFeds πλατφόρμα παρέχει τη δυνατότητα στους χρήστες να αναζητήσουν επίσης και προϊόντα, δηλαδή ένα σύνολο ομόσπονδων πόρων που έχουν «συσκευαστεί» μαζί (bundled), προσφέροντας στους χρήστες τη δυνατότητα να παίρνουν δεδομένα από πολλές πηγές την ίδια στιγμή. Η αναζήτηση των προϊόντων μπορεί να πραγματοποιηθεί με αντίστοιχους μηχανισμούς βάσει μιας πληθώρας κριτηρίων, συμπεριλαμβανομένης της τοποθεσίας, του τύπου δεδομένων, της τιμής των προϊόντων, καθώς και της φήμης τους.

Στις ενότητες που ακολουθούν περιγράφονται αναλυτικά οι μηχανισμοί αναζήτησης προϊόντων που παρέχονται από την IoTFeds πλατφόρμα, τόσο από το marketplace, όσο και από το BaaS.

6.1 Μηχανισμοί και Κριτήρια Αναζήτησης στο off-chain Σύστημα

Το στοιχείο λογισμικού αγοράς (marketplace) παρέχει τη δυνατότητα σε έναν χρήστη του συστήματος να αναζητήσει επιθυμητά προϊόντα στην επισκεπτόμενη αγορά. Τα συγκεκριμένα σημεία πρόσβασης (endpoints) παρέχονται από το στοιχείο λογισμικού symbIoTeAPI μέσω REST-API όπως περιγράφονται παρακάτω (Πίνακας 9).

Πίνακας 9: Διεπαφές marketplace για την αναζήτηση IoT πόρων.

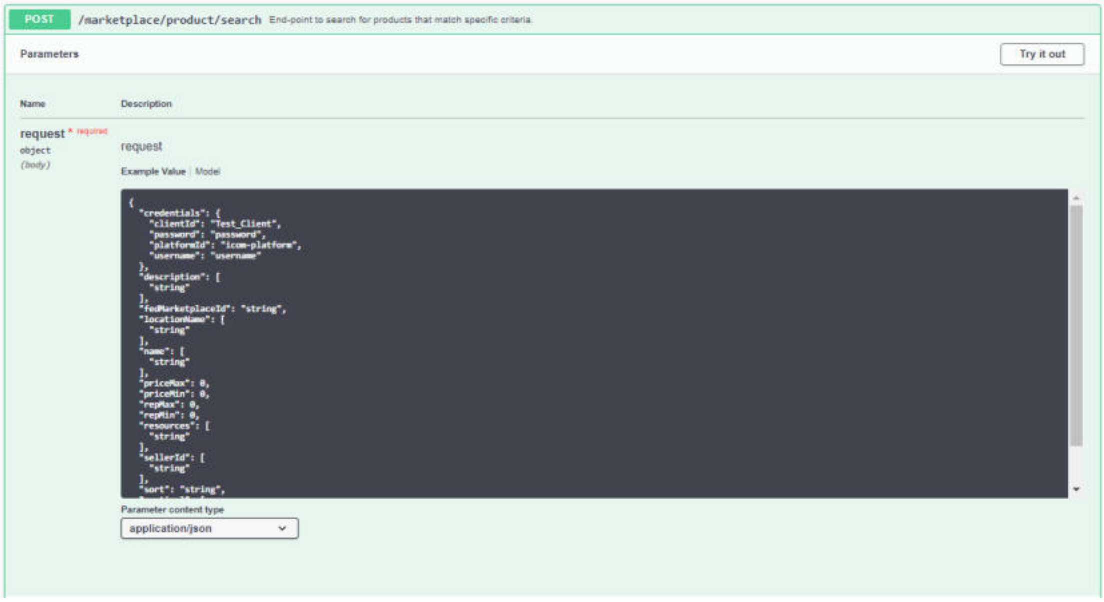
#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
4	REST	searchProducts	IoTFeds member	symbIoTeAPI	POST	Product/search	credentialsObject, List<String>	List<productCreateDto>	Αίτηση αναζήτησης προϊόντων εντός της αγοράς βάσει ικανοποίησης ενός συνόλου κριτηρίων

6.1.1 Αναζήτηση Προϊόντων

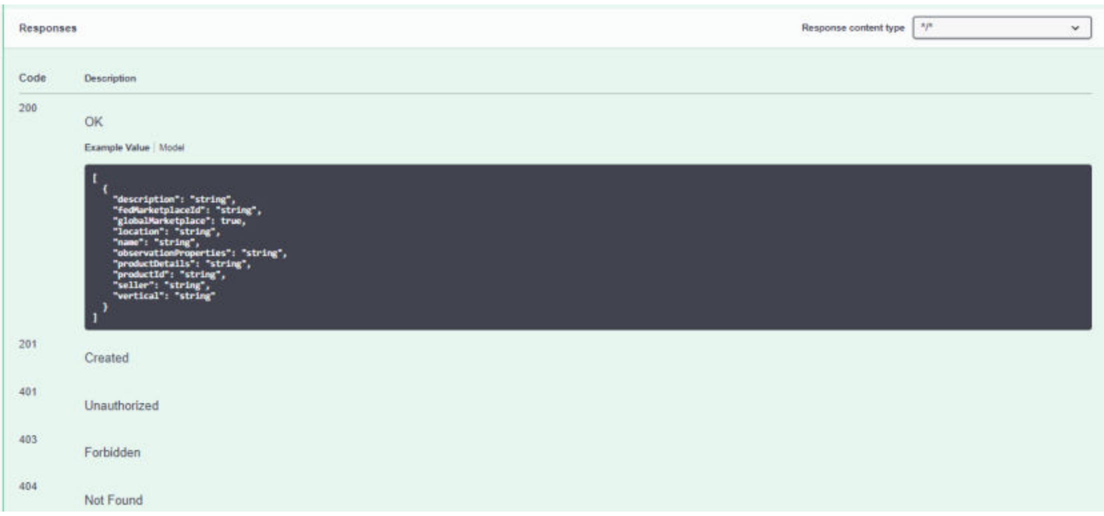
Η αναζήτηση προϊόντων από έναν χρήστη γίνεται μέσω της γραφικής διεπαφής της πύλης αγοράς όπως φαίνεται στην παρακάτω εικόνα:

Εικόνα 23:Αναζήτηση διαθέσιμων προϊόντων στην επισκεπτόμενη αγορά.

Ανάλογα με τον τύπο της αγοράς στην οποία γίνεται η αναζήτηση, το backend στοιχείο λογισμικού του marketplace επιτρέπει την αναζήτηση προϊόντων στην επισκεπτόμενη (καθολική ή ομόσπονδη) αγορά, όπως φαίνεται στο παρακάτω endpoint. Οι παράμετροι περιλαμβάνουν τα κριτήρια που υποστηρίζονται, το όνομα των προϊόντων, τα χαρακτηριστικά των πηγών δεδομένων, την περιοχή, την τοποθεσία, περιγραφή (εύρος τιμής και φήμης). Στις παραμέτρους καθορίζεται επιπλέον το αναγνωριστικό της αγοράς (fedID) – global στην περίπτωση της καθολικής αγοράς. Επιστρέφεται η λίστα με τα προϊόντα που καλύπτουν τα κριτήρια αναζήτησης ή μήνυμα λάθους (Εικόνα 25).



Εικόνα 24: Αναζήτηση προϊόντος στο Marketplace.



Εικόνα 25: Απάντηση αναζήτησης προϊόντων στο marketplace.

6.2 Μηχανισμοί Αναζήτησης Προϊόντων στο BaaS

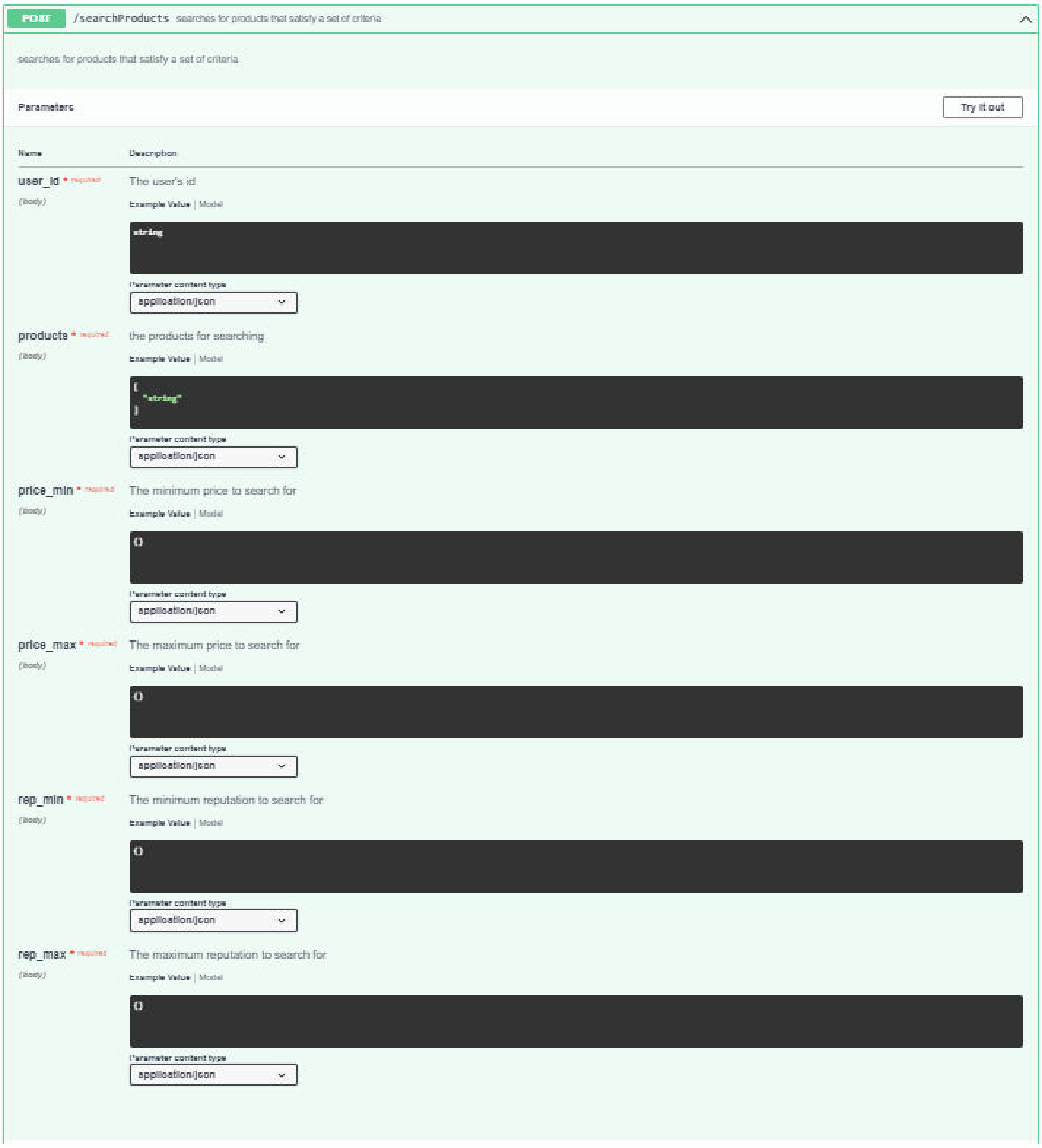
Η συγκεκριμένη ενότητα αφορά την αναζήτηση προϊόντων στο BaaS με βάση τα κριτήρια της τιμής κα της φήμης τους, ενώ στη συνέχεια αυτά ταξινομούνται και διαφημίζονται με βάση τον αλγόριθμό που περιγράφεται στο Κεφάλαιο 7.

Ο συγκεκριμένος αλγόριθμος δέχεται ως είσοδο μια λίστα από προϊόντα, τα οποία έχουν προέλθει από την πρώτη αναζήτηση από το component του symbIoTe, τις μέγιστες και ελάχιστες τιμές των κριτηρίων αναζήτησης και το αναγνωριστικό του χρήστη που κάνει την αναζήτηση. Πιο συγκεκριμένα δέχεται τα όρια της τιμής του προϊόντος και τα όρια της φήμης του (Πίνακας 10).

Πίνακας 10: Endpoint που περιγράφουν τη λειτουργία της αναζήτησης προϊόντων στο BaaS.

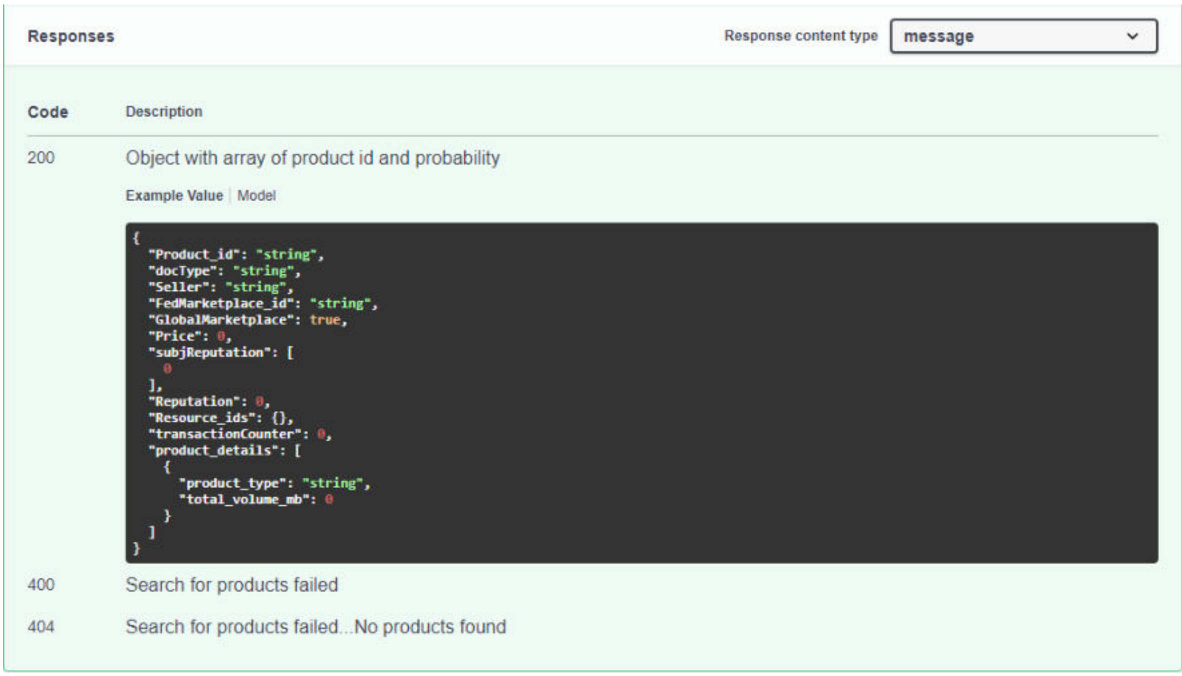
#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	search Products	marketplace API	BaaS	POST	/baas/products /search_products	(Array[String], Integer, Integer, Integer,Integer, String)	(Object, Message)	Αίτηση αναζήτησης προϊόντων βάσει ικανοποίησης ενός συνόλου κριτηρίων

Για πιο εύκολη αναζήτηση, στην περίπτωση που κάποιο από αυτά τα όρια δεν έχει οριστεί από τον χρήστη, η τιμή του όταν η παράμετρος αυτή εισέρχεται στο BaaS έχει μια τιμή, την οποία είναι αδύνατο να πάρει αυτή παράμετρος. Για παράδειγμα, αν το κάτω όριο της τιμής ενός προϊόντος δεν έχει οριστεί, για το BaaS, έχει μια αρνητική τιμή (π.χ. -1). Αντίστοιχα, και για τις μέγιστες τιμές, όπου λαμβάνουν πολύ μεγάλες, μη ρεαλιστικές τιμές, για παράδειγμα η μέγιστη τιμή της φήμης όταν αυτή δεν έχει οριστεί, μπορεί να είναι μια τιμή μεγαλύτερη από τη μονάδα (όπου μονάδα είναι η μέγιστη τιμή φήμης που μπορεί να πάρει ένα προϊόν. Στην Εικόνα 26, φαίνονται οι παράμετροι που δέχεται ως είσοδο η υπηρεσία της αναζήτησης, και επιστρέφει ένα object που περιέχει έναν πίνακα με τα προϊόντα που έχουν προκύψει μετά από την αναζήτηση και την διαφήμιση βάσει των κριτηρίων αυτών (φήμη και τιμή προϊόντος) (Εικόνα 26).



Εικόνα 26: Παράμετροι του endpoint για την αναζήτηση προϊόντων στο BaaS.

Το αντικείμενο που επιστρέφεται περιλαμβάνει τον μονοδιάστατο πίνακα που περιέχει τα objects των προϊόντων και παρουσιάζεται στην Εικόνα 27. Στην περίπτωση που κανένα προϊόν δεν ικανοποιεί τα κριτήρια αναζήτησης, επιστρέφεται ένα μήνυμα λάθους που ενημερώνει τον χρήστη (Εικόνα 27).



Εικόνα 27: Αντικείμενο που επιστρέφεται και περιλαμβάνει πίνακα με τα προϊόντα.

7 Διαφήμιση Προϊόντων στην IoTFeds Πλατφόρμα

Όπως περιγράφηκε και σε προηγούμενη ενότητα σχετικά με την αλληλεπίδραση φήμης και εμπιστοσύνης κατά τη διαφήμιση ομόσπονδων πόρων IoT στην IoTFeds πλατφόρμα (ενότητα 4.1), το προτεινόμενο σύστημα διαφήμισης είναι άρρηκτα συνδεδεμένο με τη φήμη του εκάστοτε IoT προϊόντος. Όπως σε διάφορες περιπτώσεις εφαρμογής συστημάτων φήμης για αγορές δεδομένων, έτσι και στην IoTFeds πλατφόρμα, περιλαμβάνονται δύο οντότητες, η οντότητα που προσφέρει μια αξιολόγηση (reviewer), ο οποίος είναι ο καταναλωτής, και αυτή που δέχεται μια αξιολόγηση (reviewee), ο οποίος είναι ο πάροχος των δεδομένων.

Όπως προαναφέρθηκε, στα πλαίσια του έργου IoTFeds ορίζονται δύο τύποι μετρικών για την αξιολόγηση/βαθμολόγηση των IoT πόρων, οι υποκειμενικές μετρικές και οι αντικειμενικές μετρικές. Οι ίδιες ακριβώς μετρικές χρησιμοποιούνται και για την αξιολόγηση των προϊόντων που κατατίθενται στην πλατφόρμα από έναν καταναλωτή. Στη συνέχεια, όπως και στην περίπτωση των IoT πόρων, οι αξιολογήσεις αυτές συγκεντρώνονται στο υποσύστημα BaaS, από όπου υπολογίζεται η βαθμολογία της φήμης κάθε προϊόντος, η οποία μπορεί να αποτελέσει καταλυτικό παράγοντα για την επιλογή ή την απόρριψη ενός συγκεκριμένου προϊόντος από τους καταναλωτές.

Στο συγκεκριμένο κεφάλαιο περιλαμβάνεται αναλυτική περιγραφή του προτεινόμενου αλγορίθμου ταξινόμησης για τη διαφήμιση των προϊόντων στην πλατφόρμα, ο οποίος εκμεταλλεύεται τη φήμη του κάθε προϊόντος για την κατάταξή του στη λίστα των αποτελεσμάτων που θα εμφανίζονται στο χρήστη μετά την αναζήτηση.

7.1 Μηχανισμός Διαφήμισης Προϊόντων στην IoTFeds Πλατφόρμα

Στον πίνακα που ακολουθεί (Πίνακας 11) παρουσιάζεται ο ψευδοκώδικας του αλγορίθμου ταξινόμησης προϊόντων που δημιουργήθηκε για το BaaS. Πιο συγκεκριμένα, ο αλγόριθμος δέχεται ως είσοδο έναν πίνακα με objects που περιλαμβάνει το ID του προϊόντος και την αντίστοιχη φήμη του ($\{id, rep\_score\}$) και εξάγει ένα δεύτερο object που περιλαμβάνει τα ταξινομημένα προϊόντα. Τα δύο αυτά objects περιλαμβάνονται στις λίστες $productList$ και $sortedProductList$, αντίστοιχα.

Όσον αφορά τη ροή του αλγορίθμου, αρχικά, γίνεται διαχωρισμός των προϊόντων από τη βαθμολογία φήμης τους σε δύο ξεχωριστές λίστες, $items$ και $weights$, αντίστοιχα, οι οποίες θα πρέπει να έχουν το ίδιο μέγεθος. Στη συνέχεια, για όλα τα στοιχεία της λίστας αθροίζονται τα βάρη όλων των προϊόντων που υπάρχουν στη λίστα τη δεδομένη στιγμή ($cumulativeWeights[]$), αθροίζεται το μέγιστο συνολικό βάρος ($maxCumulativeWeight$) των βαρών της λίστας και γίνεται ταξινόμηση όλων των προϊόντων βάσει του βάρους τους ($rep\_score/maxCumulativeWeight$). Σημειώνεται πως σε κάθε επανάληψη, το αθροιστικό βάρος αλλάζει καθώς από την αρχική λίστα αφαιρείται κάθε φορά το προϊόν με το μεγαλύτερο βάρος και εισάγεται με τη σειρά στη νέα λίστα $sortedProductList$. Τέλος, γίνεται υπολογισμός της μεταβλητής $randomNumber$, η οποία συγκρίνεται με το αθροιστικό βάρος του κάθε προϊόντος. Σε περίπτωση που το βάρος του προϊόντος είναι μεγαλύτερο ή ίσο από τη μεταβλητή $randomNumber$, ο αλγόριθμος αφαιρεί το συγκεκριμένο προϊόν από την αρχική λίστα και το περνάει στη νέα λίστα $sortedProductList$. Η διαδικασία αυτή επαναλαμβάνεται μέχρι να περαστεί και το τελευταίο εναπομείναν προϊόν αρχικής λίστας.

Ο αλγόριθμος τελικά επιστρέφει το object με τον πίνακα που περιέχει τα ταξινομημένα προϊόντα της αρχικής λίστας, όπως αυτή έχει προκύψει από την αναζήτηση του BaaS.

Πίνακας 11: Ψευδοκώδικας για τον αλγόριθμο διαφήμισης προϊόντων του BaaS.

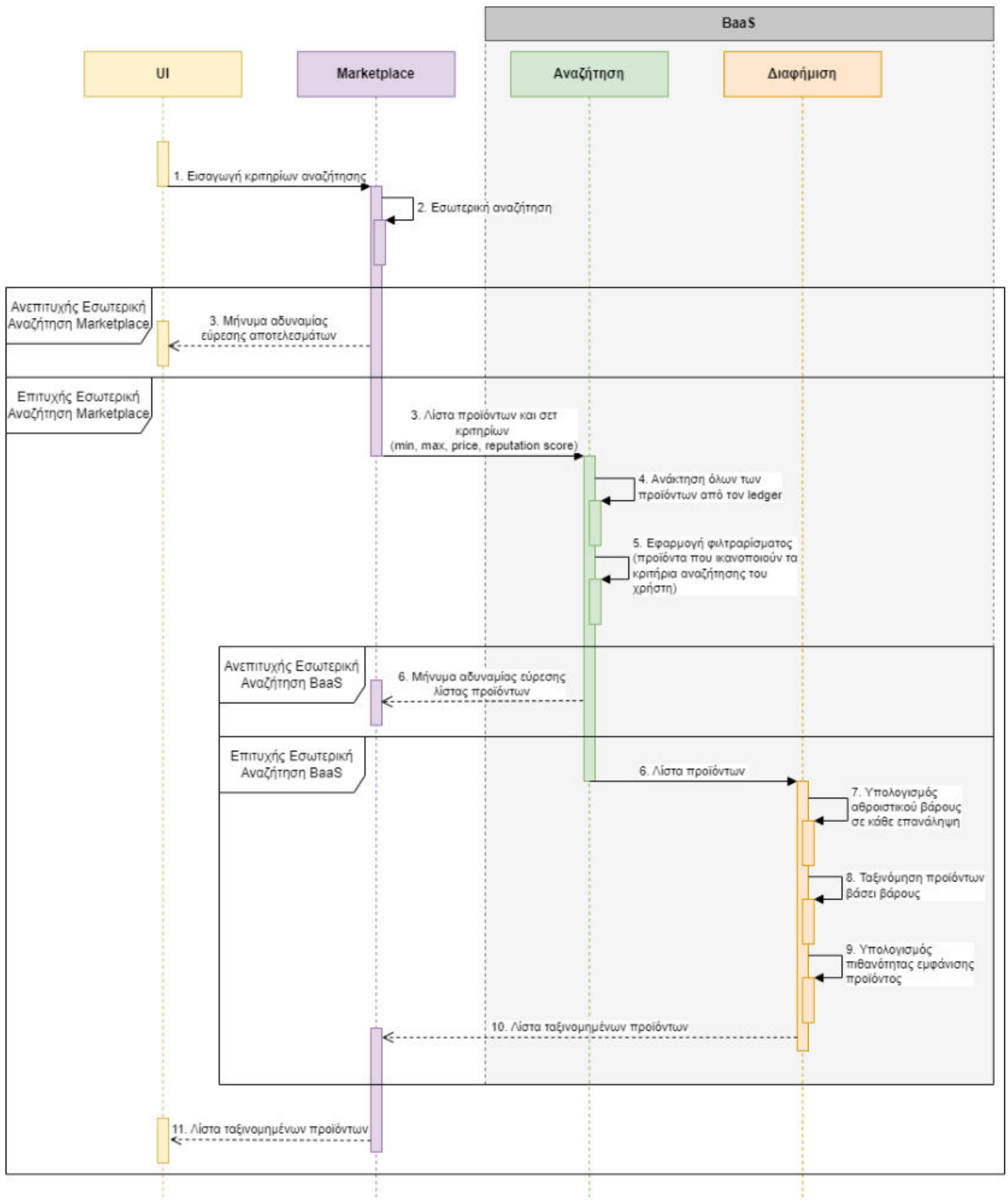
$productList[]$:	$List\ of\ products\ with\ their\ reputation\ scores$
$random\_factor$:	$Generation\ of\ random\ results$

$maxCumulativeWeight$: $Maximum\ cumulative\ weight\ of\ the\ products\ in\ the\ productList$
$sortedProductList[]$: $List\ of\ sorted\ products$

```
function weightedRandom(items, weights)
        if items.length != weights.length
                throw error "Products and weights must be of the same size"

        if items.length == 0:
                return

        cumulativeWeights = [];
        for i in range(0, len(weights)):
                cumulativeWeights[i] = weights[i] + (cumulativeWeights[i − 1] || 0)

        maxCumulativeWeight = cumulativeWeights[cumulativeWeights.length − 1]

        sortedProducts = items.sort((a, b) =>
        b.rep_score/maxCumulativeWeight – a.rep_score/maxCumulativeWeight)

        randomNumber = maxCumulativeWeight * Math.random() * random_factor

        for itemIndex in range(0, len(sortedProducts)):
                if cumulativeWeights[itemIndex] >= randomNumber:
                        sortedProductList.push(items[itemIndex].id)
                        products.splice(itemIndex, 1)
                        weights.splice(itemIndex, 1)
                        weightedRandom(items, weights)

sortedProductList = []
random_factor = 1/3
weightedRandom(productList, productList.map(product => product.rep_score))
```

7.2 *Ακολουθία Αναζήτησης και Διαφήμισης* Προϊόντων

Στο διάγραμμα ακολουθίας στην Εικόνα 28 περιγράφεται η συνολική ροή των επιμέρους διαδικασιών που παρουσιάστηκαν αναλυτικά στα Κεφάλαια 6 και 7, από την εισαγωγή των κριτηρίων αναζήτησης προϊόντων του χρήστη στη γραφική διεπαφή χρήστη της αγοράς (marketplace), μέχρι την τελική επιστροφή των ταξινομημένων αποτελεσμάτων πίσω σε αυτό.



Εικόνα 28: Διάγραμμα ακολουθίας για την αναζήτηση και τη διαφήμιση των προϊόντων.

Πιο συγκεκριμένα, τα βήματα που παρουσιάζονται στο διάγραμμα ακολουθίας στην Εικόνα 28 για τους μηχανισμούς αναζήτησης και διαφήμισης των προϊόντων του BaaS έχουν ως εξής:

1. Εισαγωγή των κριτηρίων αναζήτησης του χρήστη από την γραφική διεπαφή της αγοράς στο marketplace backend.
2. Εσωτερική αναζήτηση των προϊόντων στο marketplace που πληρούν τα κριτήρια που έχουν οριστεί από το χρήστη κατά την εισαγωγή τους στο UI.
3. Το marketplace backend επιστρέφει στο UI μήνυμα αδυναμίας εύρεσης προϊόντων που να αντιστοιχούν στα κριτήρια αναζήτησης που έχουν εισαχθεί από το χρήστη.

Εναλλακτικά, σε περίπτωση αντιστοίχισης των κριτηρίων αναζήτησης του χρήστη σε συγκεκριμένα αποτελέσματα, η διαδικασία της αναζήτησης συνεχίζει ως εξής:

3. Αποστολή της λίστας των προϊόντων που πληρούν τα κριτήρια του χρήστη, καθώς και του συνόλου των κριτηρίων που εισήχθησαν κατά την αναζήτηση στο BaaS.
4. Ανάκτηση από το BaaS όλων των προϊόντων που βρίσκονται καταχωρημένα στον ledger.
5. Εφαρμογή κατάλληλου φιλτραρίσματος στη λίστα των προϊόντων για την εύρεση των προϊόντων που ικανοποιούν τα κριτήρια αναζήτησης που ορίστηκαν από το χρήστη.
6. Σε περίπτωση αδυναμίας εύρεσης της λίστας των προϊόντων που ικανοποιούν τα κριτήρια αναζήτησης του χρήστη στον ledger, επιστρέφεται μήνυμα αδυναμίας εύρεσης της λίστας των προϊόντων από τη μονάδα αναζήτησης του BaaS στο marketplace.

Εναλλακτικά, σε περίπτωση εύρεσης της λίστας των προϊόντων από τον ledger που ικανοποιούν τα κριτήρια αναζήτησης που ορίστηκαν από το χρήστη, η διαδικασία της αναζήτησης και της διαφήμισης τερματίζει ως εξής:

6. Αποστολή της λίστας των επιλεγμένων προϊόντων στη μονάδα της διαφήμισης του BaaS.
7. Υπολογισμός σε κάθε επανάληψη του αθροιστικού βάρους των προϊόντων που βρίσκονται στη λίστα προς ταξινόμηση.
8. Ταξινόμηση των προϊόντων της λίστας βάσει του βάρους τους (βαθμολογία φήμης/αθροιστικό βάρος).
9. Υπολογισμός της πιθανότητας εμφάνισης κάθε προϊόντος της λίστας σύμφωνα με τον τύπο που παρουσιάζεται στον ψευδοκώδικα του αλγορίθμου ταξινόμησης (Πίνακας 11). Ο αλγόριθμος τελικά επιστρέφει το object με τον πίνακα που περιέχει τα ταξινομημένα προϊόντα της αρχικής λίστας, όπως αυτή έχει προκύψει από την αναζήτηση του BaaS.
10. Αποστολή στο marketplace της λίστας των ταξινομημένων προϊόντων για εμφάνιση στο χρήστη.
11. Εμφάνιση της λίστας των ταξινομημένων προϊόντων στο χρήστη μέσω της γραφικής διεπαφής χρήστη της επισκεπτόμενης αγοράς.

8 Ασφαλής Πρόσβαση και Διαχείριση Δεδομένων IoT

Η ασφαλής πρόσβαση και διαχείριση IoT δεδομένων στα πλαίσια του IoTFeds, είναι μια από τις πιο σημαντικές λειτουργίες, καθώς κρίνεται απαραίτητος ο έλεγχος για το αν και μέχρι πότε μπορεί κάποιος χρήστης να προσπελάσει IoT πόρους. Ο έλεγχος αυτός λαμβάνει χώρα σε δύο επίπεδα, με το πρώτο να αφορά τους ήδη υπάρχοντες μηχανισμούς του symbIoTe, ενώ το δεύτερο επίπεδο αφορά το δίκτυο blockchain και τους καινούριους μηχανισμούς που έχουν αναπτυχθεί για αυτό το σκοπό, έτσι ώστε ο συνδυασμός των δύο επιπέδων να προσφέρει ένα υψηλό επίπεδο ασφάλειας.

Στο IoTFeds διακρίνουμε δύο οντότητες στις οποίες απαιτείται ο έλεγχος για ασφαλή πρόσβαση και διαχείριση των δεδομένων, τις πηγές δεδομένων IoT, που είναι υπεύθυνες για τη λήψη μετρήσεων και παραγωγή των δεδομένων, και τα προϊόντα (products), τα οποία όπως έχει ήδη αναφερθεί αποτελούν μια νέα οντότητα στο IoTFeds. Το symbIoTe παρέχει μηχανισμούς ABAC για τον έλεγχο πρόσβασης ενός χρήστη σε κάποια πηγή δεδομένων, μέσα από τον ορισμό ενός συνόλου πολιτικών που καλύπτουν μια πληθώρα περιπτώσεων. Ωστόσο, προέκυψε η ανάγκη για την ύπαρξη κάποιας μεθόδου για την ασφαλή και εξουσιοδοτημένη πρόσβαση στα προϊόντα του IoTFeds. Καθώς υπάρχουν δύο είδη αγορών, η αγορά στα πλαίσια μιας ομοσπονδίας (federated marketplace) και μια γενική αγορά (global marketplace), θα πρέπει σε κάθε είδος αγοράς να υπάρχουν τα προϊόντα που έχουν οριστεί για κάθε μία από αυτές, ώστε να μην μπορεί κάποιος να έχει πρόσβαση σε προϊόντα που δεν ανήκουν στις ομοσπονδιακές αγορές που συμμετέχει. Επιπλέον, δημιουργήθηκε στο blockchain ένας μηχανισμός ελέγχου πρόσβασης βασισμένος στην κατοχή «κουπονιών» πρόσβασης από τον χρήστη (access tokens) και τα οποία εκφράζουν την ικανότητα του χρήστη να προσπελάσει τα προϊόντα που έχει αγοράσει. Τα access tokens μπορούν να θεωρηθούν ως ένα είδος ABAC ελέγχου, καθώς κάθε χρήστης μπορεί να θεωρηθεί πως έχει ως χαρακτηριστικό του τα συγκεκριμένα tokens που αντιστοιχούν στα προϊόντα που έχει στην κατοχή του.

Στις ενότητες που ακολουθούν αναλύονται ξεχωριστά οι προαναφερθέντες μηχανισμοί.

8.1 Μηχανισμοί Ασφαλούς Πρόσβασης στο off-chain Σύστημα

Στην ενότητα αυτή αρχικά περιγράφεται ο μηχανισμός ελέγχου πρόσβασης του symbIoTe στο οποίο βασίζεται η πρόσβαση στα δεδομένα των πηγών δεδομένων. Στη συνέχεια περιγράφονται οι διεπαφές που υλοποιήθηκαν στα πλαίσια του έργου και ενσωματώνουν την επικοινωνία με το BaaS.

Ο μηχανισμός ασφαλείας στο symbIoTe βασίζεται στον έλεγχο πρόσβασης με βάση τα χαρακτηριστικά (Attribute Based Access Control – ABAC). Στη μεθοδολογία ABAC, ως χαρακτηριστικό (attribute) ορίζεται μια συγκεκριμένη ιδιότητα, ρόλος ή άδεια που σχετίζεται με μια οντότητα στο σύστημα και εκχωρείται μετά από μια διαδικασία ελέγχου ταυτότητας από τον διαχειριστή του συστήματος. Η πρόσβαση σε πόρους ελέγχεται μέσω των πολιτικών ελέγχου πρόσβασης. Η πολιτική πρόσβασης ορίζει ένα συγκεκριμένο συνδυασμό χαρακτηριστικών που απαιτούνται για την παραχώρηση πρόσβασης σε έναν IoT πόρο και εκχωρείται σε κάθε πόρο από τον κάτοχό του. Επομένως, μια εφαρμογή ενός καταναλωτή δεδομένων μπορεί να λάβει πρόσβαση σε έναν IoT πόρο μόνο εφόσον διαθέτει ένα σύνολο χαρακτηριστικών που ταιριάζουν με την προκαθορισμένη, από τον κάτοχο του πόρου, πολιτική πρόσβασης.

Πιο συγκεκριμένα στο symbIoTe:

- Τα «χαρακτηριστικά» αποθηκεύονται σε διακριτικά πρόσβασης (access tokens) και δημιουργούνται από τις αντίστοιχες μικρο-υπηρεσίες (microservices) αυθεντικοποίησης και εξουσιοδότησης (Authentication Authorization Manager -

AAM) κάθε συμμορφούμενης με το symbIoTe, IoT πλατφόρμας. Τα διακριτικά πρόσβασης είναι συνεπώς ψηφιακά αντικείμενα που περιέχουν μία λίστα στοιχείων που σχετίζονται με τον μηχανισμό ασφαλείας που χρησιμοποιείται στα πλαίσια του symbIoTe, τα χαρακτηριστικά που παραχωρούνται στον κάτοχο του διακριτικού, και χρησιμοποιούνται για σκοπούς ελέγχου ταυτότητας και εξουσιοδότησης.
- Κάθε διακριτικό εξασφαλίζει την αυθεντικότητα των «χαρακτηριστικών» που περιέχει.
- Τα «χαρακτηριστικά» μπορούν να τροποποιηθούν όσον αφορά την πρόσβαση σε μια απομακρυσμένη IoT πλατφόρμα.
- Οι πολιτικές πρόσβασης ελέγχονται από την μικρο-υπηρεσία που είναι υπεύθυνη για την διαχείριση της πρόσβασης στα δεδομένα των IoT πόρων (Resource Access Proxy - RAP).

Η μέθοδος ABAC έχει σαν στόχο την επίλυση του προβλήματος της αυθεντικοποίησης (authorization) ενός πελάτη (client) απέναντι σε δράσεις που αφορούν ένα αντικείμενο. Στο σύστημα symbIoTe το αντικείμενο είναι ένας IoT πόρος/συσκευή και οι δράσεις είναι:

- Αλλαγή κατάστασης (status)
- Εντολή προς τη συσκευή (μετακίνηση, άνοιγμα, κλείσιμο)
- Λήψη μετρήσεων (get observation)
- Αναζήτηση

Στο σύστημα symbIoTe οι δράσεις ομαδοποιούνται σε δύο κατηγορίες:

- Προσπέλαση (access) του IoT πόρου/συσκευής που περιέχει τις τρεις πρώτες δράσεις (αλλαγή κατάστασης, εντολή προς την συσκευή και λήψη μετρήσεων).
- Αναζήτηση πόρων.

Ο ιδιοκτήτης του IoT πόρου επιδρώντας σε αυτές τις κατηγορίες δράσεων του IoT πόρου, έχει την δυνατότητα να επηρεάσει την διαδικασία αυθεντικοποίησης των διαπιστευμένων (athenticated) χρηστών.

Με αυτόν τον τρόπο, δεν είναι υποχρεωμένος ο ίδιος ή ο διαχειριστής του συστήματος να αλλάξει ή να εμπλουτίσει τις ιδιότητες ενός ρόλου χρηστών σύμφωνα με παραδοσιακά συστήματα ασφαλείας χρηστών.

Με σκοπό να επιδράσει ο ιδιοκτήτης του IoT πόρου σε μια κατηγορία δράσεων πρέπει να ενημερώσει την πληροφορία του IoT πόρου (μεταδεδομένα), έτσι ώστε να περιλαμβάνει τα χαρακτηριστικά που πρέπει να έχει ο πελάτης (client) ο οποίος θα εξετασθεί με σκοπό την αυθεντικοποίηση του.

Απαραίτητο λοιπόν είναι (για την επιτυχή ολοκλήρωση του μηχανισμού ABAC) κατά την διαδικασία της ταυτοποίησης του client, το security token το οποίο εκδίδεται, να περιλαμβάνει τα χαρακτηριστικά του client.

Ακόμη, για να είναι ολοκληρωμένος ο μηχανισμός ABAC από άκρη σε άκρη, πρέπει ο ιδιοκτήτης του IoT πόρου να γνωρίζει την πλήρη λίστα των χαρακτηριστικών που ενσωματώνονται αυτόματα στο security token, έτσι ώστε να επιλέξει μεταξύ αυτών, τα κατάλληλα για τον έλεγχο της αυθεντικοποίησης χρήσης.

Ένα παράδειγμα του ABAC μηχανισμού του symbIoTe όπου επιτρέπεται η πρόσβαση σε έναν πόρο μίας πλατφόρμας fed_h σε μία συγκεκριμένη ομοσπονδία fed_id από χρήστες που ανήκουν σε πλατφόρμες που εμπλέκονται στην ομοσπονδία φαίνεται παρακάτω Στο παράδειγμα αυτό, οι χρήστες με έγκυρο εσωτερικό διακριτικό, όπως υποδεικνύεται από το πεδίο req_loc ή αλλιώς requireAllLocalTokens, από οποιοδήποτε μέλος της ομοσπονδίας (UiTOP, Zastel) μπορούν να έχουν πρόσβαση με βάση τους κανόνες τα ομοσπονδίας:

```
{
   "policyType":"SFTAP",
   "requiredClaims":{
     "fed_id":"fedSmartCity",
     "fed_h":"UiTOP",
     "fed_s" : "2",
     "req_loc" : "false",
     "fed_m_1" : "Zastel",
     "fed_m_2" : "UiTOP"
   }
```

}, ενώ η παρακάτω πολιτική μπορεί να περιορίσει την πρόσβαση μόνο στον χρήστη marketplace της πλατφόρμας symbIoTe_Core_AAM:

```
{
  "policyType":"SLHTIBAP",
  "requiredClaims":{
   "sub":"marketplace",
   "iss":"SymbIoTe_Core_AAM"
  }
}.
```

Ο μηχανισμός ABAC καθορίζει τα δικαιώματα αναζήτησης και φιλτραρίσματος IoT πόρων που συζητήθηκαν στο Κεφάλαιο 3. Όσον αφορά την πρόσβαση στα δεδομένα πηγών δεδομένων, στα πλαίσια του IoTFeds τα δεδομένα αποκτούνται μέσα από την πρόσβαση σε προϊόντα δεδομένων και συνεπώς σε αγορές προϊόντων η πρόσβαση στα δεδομένα των πηγών δεδομένων γίνεται από το στοιχείο λογισμικού αγοράς. Ο μηχανισμός ασφαλείας του symbIoTe συνδυάζεται με τους μηχανισμούς του BaaS για να διαπιστωθεί αν ένας χρήστης είναι εξουσιοδοτημένος να εκτελέσει συγκεκριμένες ενέργειες στο επίπεδο των προϊόντων. Οι πολιτικές φιλτραρίσματος και πρόσβασης πηγών δεδομένων καθορίζονται κατά την διαδικασία της καταχώρησης τους στο σύστημα.

Στον παρακάτω πίνακα συνοψίζονται οι βασικές διεπαφές στο Marketplace και symbIoTeAPI που εμπλέκονται στην καταχώρηση, διαμοιρασμό, προσπέλαση και διαγραφή IoT πόρων από το σύστημα.

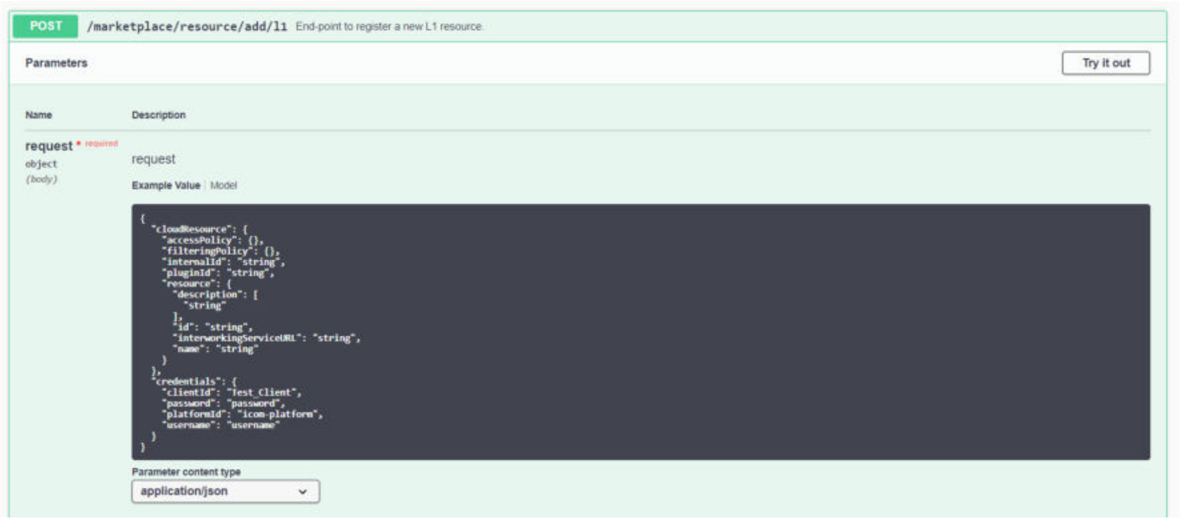
Πίνακας 12: Διεπαφές symbIoTeAPI και marketplaceAPI για εγγραφή και προσπέλαση σε πηγές δεομένων.

#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	addL1resource	marketplace	symbIoTeAPI	POST	/symbioteapi/resources/add/l1	{CloudResource Object, Credentials Object }	(Resource Object, Message)	Εγγραφή IoT πόρου
2	REST	shareResource	marketplace	symbIoTeAPI	POST	/symbioteapi/resources/shareresource	{""Boolean", "string", Credentials Object,"string"	(CloudResource Object, Message)	Διαμοιρασμός πόρου σε ομοσπονδία (federationId).

							}		
3	REST	ushareResource	marketplace	symbIoTeAPI	POST	/symbioteapi/resources/unsharer esource	{"”Boolean”, "string", Credentials Object,"string" }	(CloudResource Object, Message)	Διαγραφή πόρου από ομοσπονδία (federationId).
4	REST	deleteResource	marketplace	symbIoTeAPI	DELETE	/symbioteapi/resources/delete/l1 /{resourceInternalId}	{Credentials Object }	(CloudResource Object, Message)	Διαγραφή πόρου από το σύστημα
5	REST	accessL1	marketplace	symbIoTeAPI	POST	/symbioteapi/ resource/access/ l1/{resource_internalId}?top=Integer&fromDate =string&toDate =string	{ Credentials Object,"string" }	(ObservationMessage)	Προσπέλαση δεδομένων IoT πόρου
6	REST	addL1resource	IoTFeds Fed Member	marketplace	POST	/marketplace /resources/add/l1	{CloudResource Object, Credentials Object }	(Resource Object, Message)	Εγγραφή IoT πόρου στο σύστημα
7	REST	shareResource	IoTFeds Fed Member	marketplace	POST	/marketplace /resources/share resource	{PricngParameters of type <String>, Credentials,"String", ”String> }	(CloudResource Object, Message)	Διαμοιρασμός πόρου σε ομοσπονδία (federationId) στο σύστημα
8	REST	ushareResource	IoTFeds Fed Member	marketplace	POST	/marketplace /resources/unsharereresource	{"”Boolean”, "string", Credentials Object,"string" }	(CloudResource Object, Message)	Διαγραφή πόρου από ομοσπονδία (federationId).
9	REST	deleteResource	IoTFeds Fed Member	marketplace	DELETE	/ marketplace /resources/delete/l1/{resourceInternalId}	{Credentials Object }	(CloudResource Object, Message)	Διαγραφή πόρου από το σύστημα

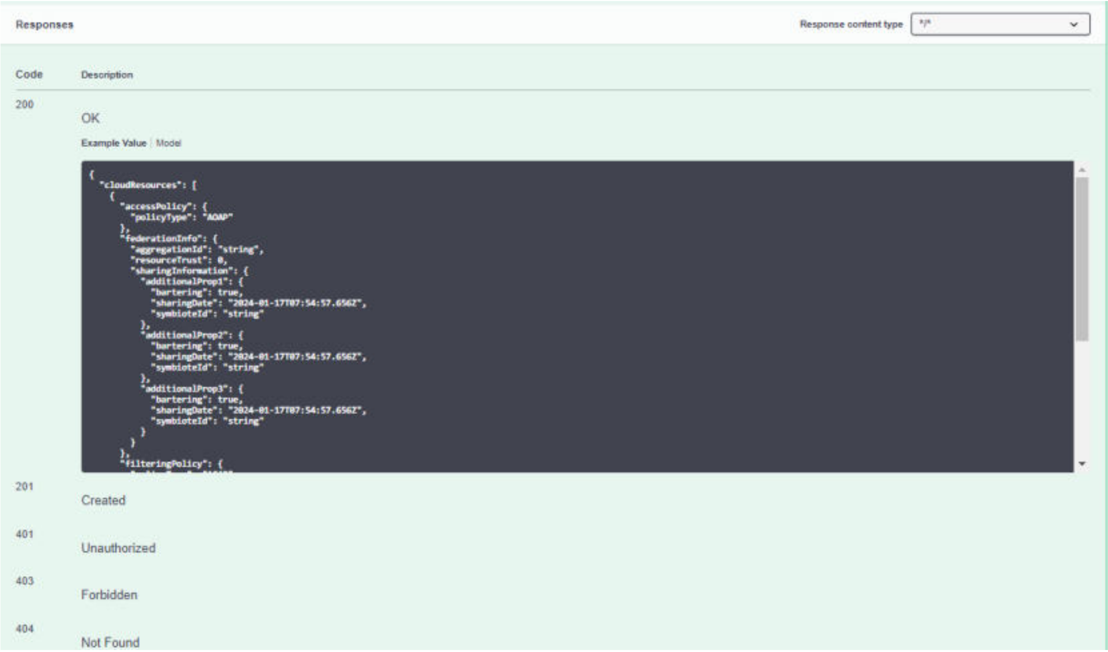
8.1.1 Καταχώρηση IoT πόρου στην IoTFeds πλατφόρμα

Η καταχώρηση ενός IoT πόρου στο σύστημα επιτυγχάνεται χρησιμοποιώντας το παρακάτω endpoint (Εικόνα 29), το οποίο δέχεται ως παραμέτρους τα διαπιστευτήρια του χρήστη, το όνομα και το αναγνωριστικό του (name, id), το url της πλατφόρμας (interworkingServiceURL) στην οποία ανήκει, το plugin id της πλατφόρμας (pluginId), την περιγραφή του (description) και πληροφορίες σχετικά με την τοποθεσία του (location) και τα χαρακτηριστικά του (properties).



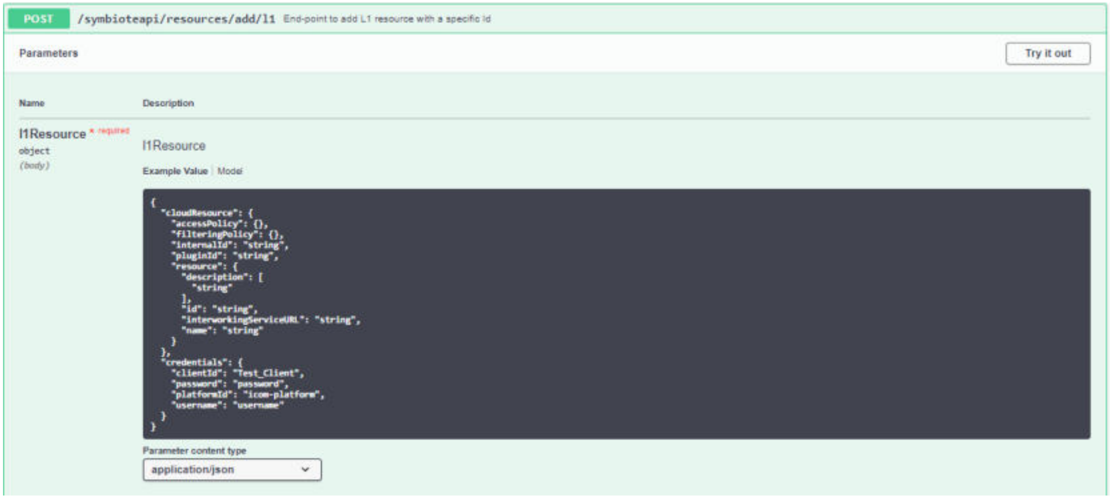
Εικόνα 29: Marketplace endpoint για καταχώρηση πηγής δεδομένων στο IoTFeds σύστημα.

Ο χρήστης ενημερώνεται με τις πληροφορίες της πηγής δεδομένων που καταχωρήθηκε επιτυχώς στο σύστημα ή με αντίστοιχο μήνυμα λάθους, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 30: Απάντηση καταχώρησης πηγής δεδομένων.

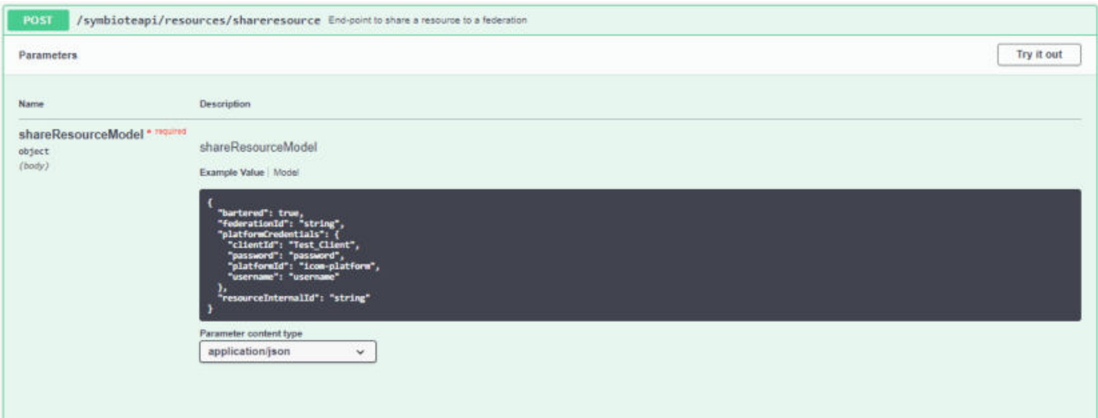
Η παραπάνω διεπαφή ενσωματώνει επικοινωνία με το αντίστοιχο endpoint του symbIoTeAPI (Εικόνα 31) στο οποίο περνάει τα απαραίτητα πεδία για τις πολιτικές πρόσβασης και φιλτραρίσματος στο symbIoTe. Τέλος το symbIoTeAPI ενσωματώνει την επικοινωνία με το BaaS.



Εικόνα 31: symbIoTe endpoint για καταχώρηση πηγής δεδομένων.

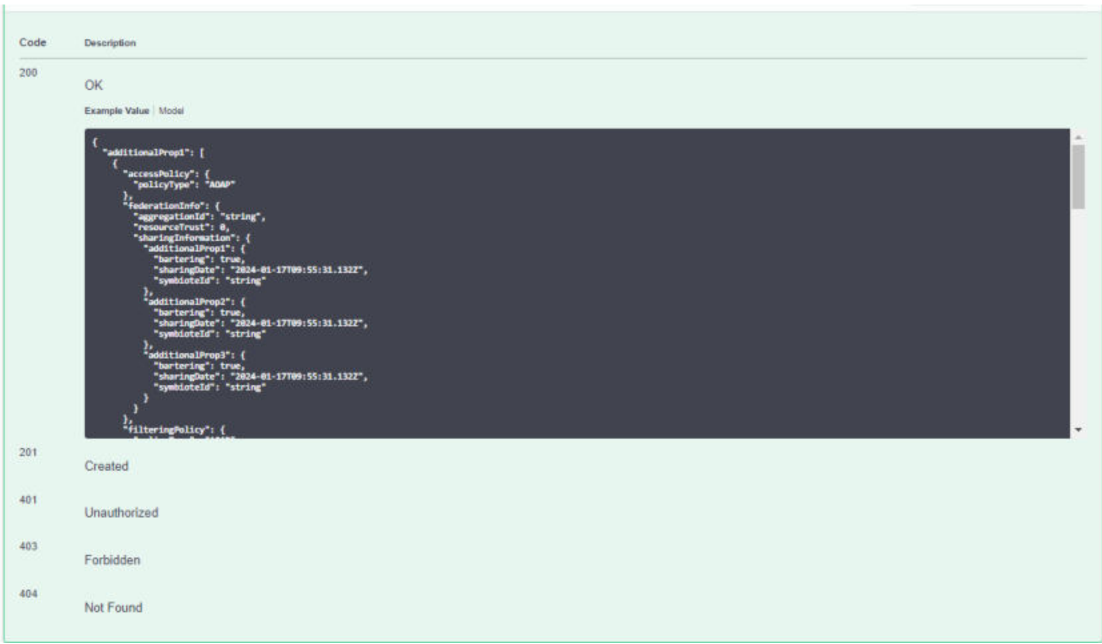
8.1.2 Διαμοιρασμός IoT πόρου σε ομοσπονδία

Οποιοσδήποτε καταχωρημένος IoT πόρος στο σύστημα μπορεί να διαμοιραστεί από τον πάροχο του σε οποιαδήποτε ομοσπονδία συμμετέχει χρησιμοποιώντας το παρακάτω endpoint:



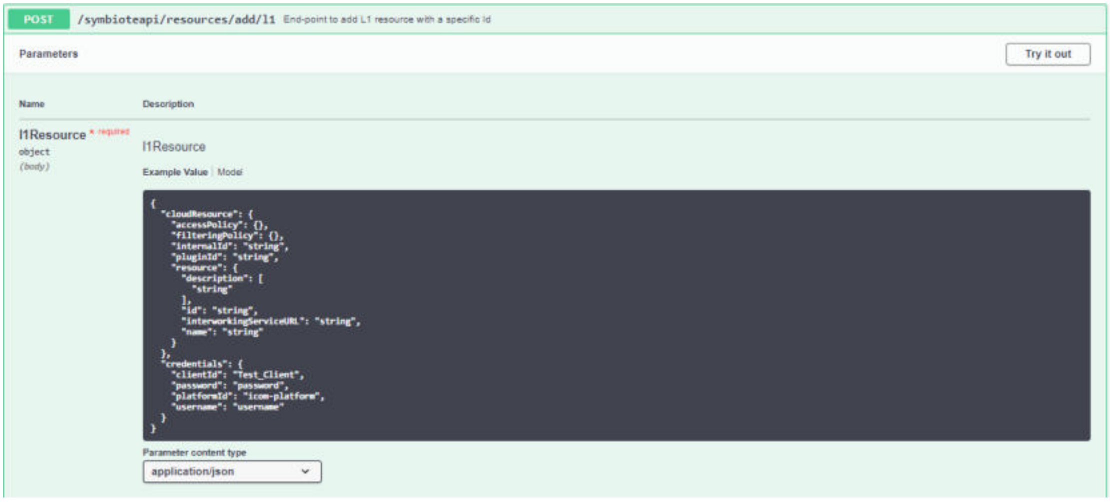
Εικόνα 32: Marketplace endpoint για διαμοιρασμό πηγής δεδομένων σε ομοσπονδία στο IoTFeds σύστημα.

Στις παραμέτρους ο χρήστης καθορίζει το αναγνωριστικό της πηγής δεδομένων, resourceId, το id της ομοσπονδίας, federationId, στην οποία επιθυμεί να το διαμοιράσει και αν ο IoT πόρος είναι bartered (ανάλογα με τον τύπο της ομοσπονδίας), ενώ απαιτούνται τα διαπιστευτήρια του. Ο χρήστης ενημερώνεται με τις πληροφορίες της πηγής δεδομένων που διαμοιράστηκε στην ομοσπονδία ή με αντίστοιχο μήνυμα λάθους, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 33: Απάντηση διαμοιρασμού πηγής δεδομένων.

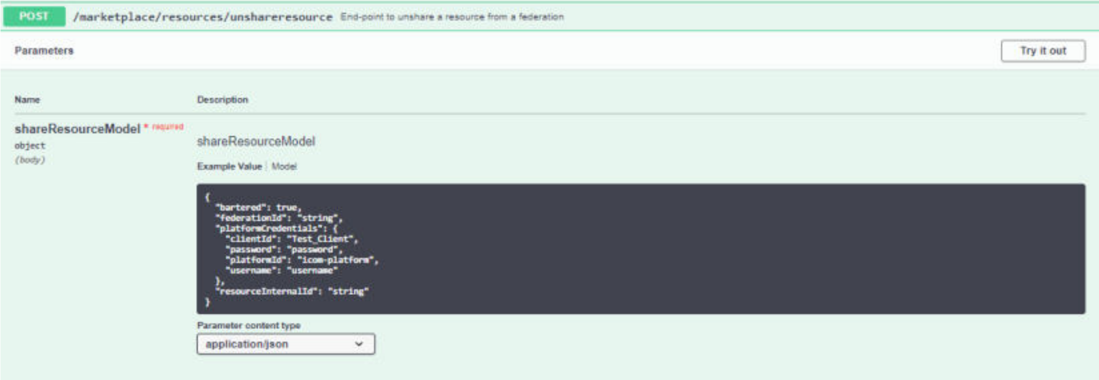
Η διεπαφή αυτή ενσωματώνει επικοινωνία με το αντίστοιχο endpoint του symbIoTeAPI (Εικόνα 31) το οποίο ενημερώνει το symbIoTe εσωτερικά και καταγράφει την απαραίτητη πληροφορία στο BaaS.



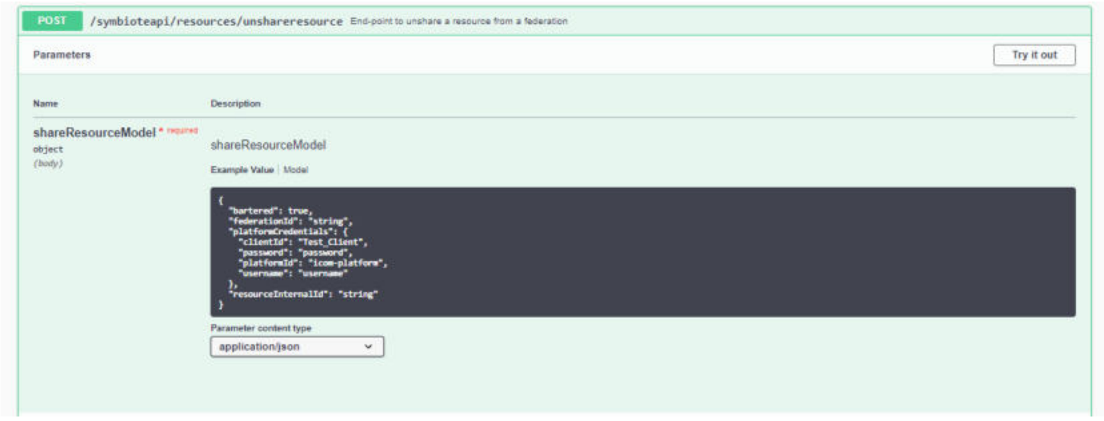
Εικόνα 34: symbIoTeAPI endpoint για διαμοιρασμό πηγής δεδομένων σε ομοσπονδία.

8.1.3 Κατάργηση διαμοιρασμού IoT πόρου από ομοσπονδία

Ο διαμοιρασμός ενός IoT πόρου μπορεί να καταργηθεί από μία ομοσπονδία από τον πάροχο του μέσω της διεπαφής στην Εικόνα 36. Η ενέργεια αυτή επιτρέπεται εφόσον δεν υπάρχει ενεργό κουπόνι πρόσβασης από τρίτους για προϊόν στο οποίο συνεισφέρει δεδομένα ο πόρος αυτός. Ο χρήστης ενημερώνεται με αντίστοιχο μήνυμα επιτυχίας ή αποτυχίας.



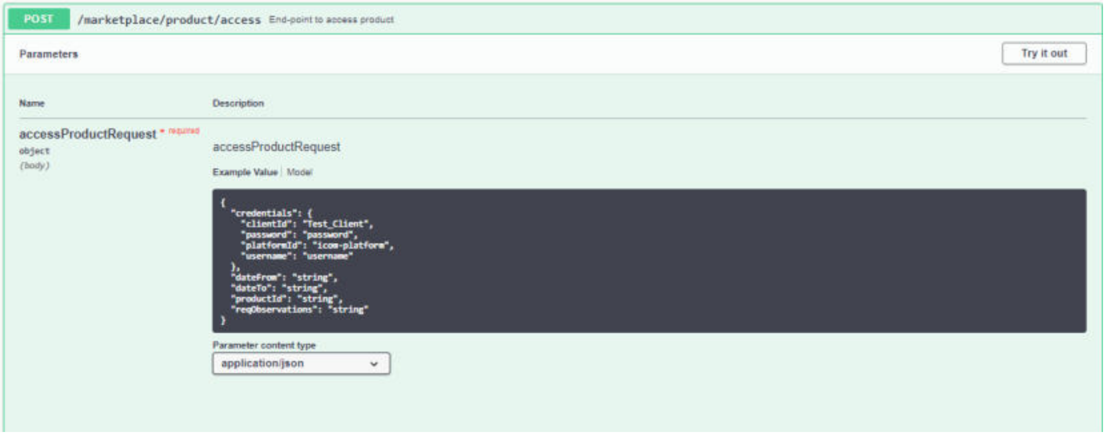
Εικόνα 35:Marketplace endpoint για κατάργηση διαμοιρασμού πηγής δεδομένων από ομοσπονδία



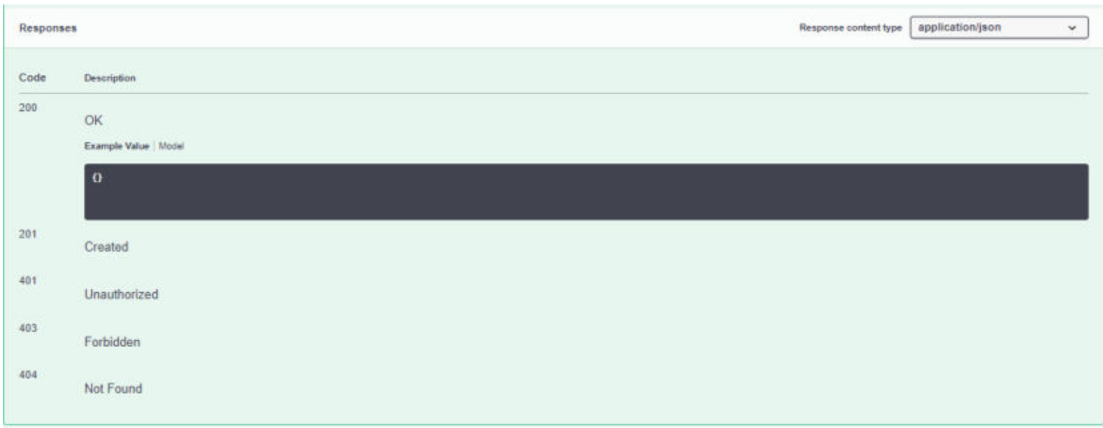
Εικόνα 36: symbIoTeAPI endpoint για κατάργηση διαμοιρασμού πηγής δεδομένων από ομοσπονδία.

8.1.4 Προσπέλαση δεδομένων προϊόντος σε ομοσπονδιακή ή καθολική αγορά

Η προσπέλαση ενός προϊόντος πολλαπλών χρήσεων επιτυγχάνεται χρησιμοποιώντας το παρακάτω endpoint (Εικόνα 37). Στις παράμετρους καθορίζεται το διάστημα των μετρήσεων (για ιστορικά δεδομένα) ή/και ο αριθμός των (πιο πρόσφατων) μετρήσεων που ο χρήστης θέλει να ανακτήσει. Επιστρέφονται οι μετρήσεις ή μήνυμα λάθους (Εικόνα 38). Η διεπαφή ενσωματώνει την επικοινωνία με το BaaS (checkAccess, decreaseToken κλπ) για την ενημέρωση του κουπονιού καθώς και τον έλεγχο για το επιθυμητό αριθμό μετρήσεων, εξασφαλίζοντας ότι ο αριθμός των μετρήσεων που λαμβάνει ο χρήστης δεν ξεπερνά το επιτρεπόμενο όριο με βάση το κουπόνι.

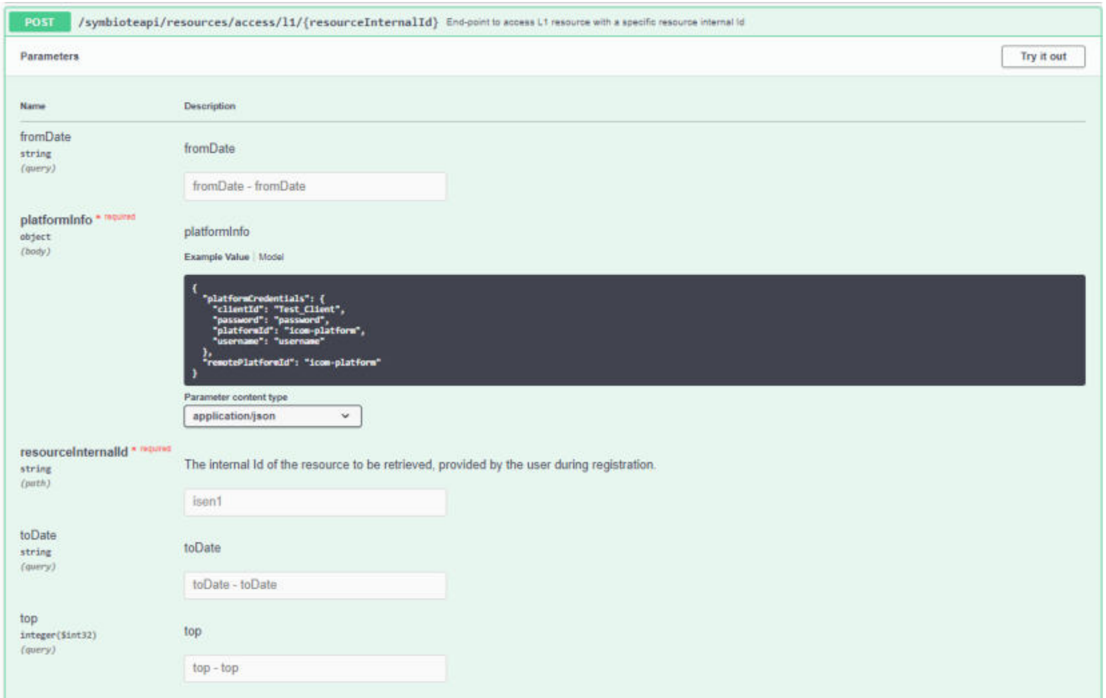


Εικόνα 37: Προσπέλαση δεδομένων στο marketplace.

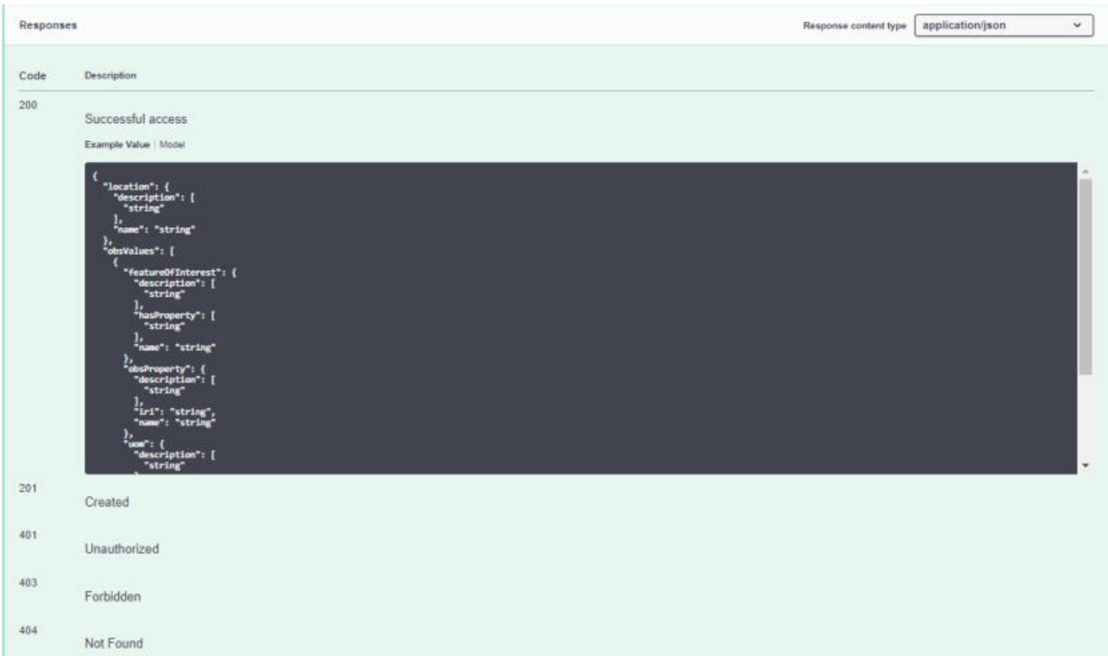


Εικόνα 38:Απάντηση προσπέλασης δεδομένων.

Η παραπάνω διεπαφή ζητάει τις τελευταίες top μετρήσεις στο καθορισμένο χρονικό διάστημα (fromDate, toDate) από κάθε πηγή δεδομένων (με αναγνωριστικό resourceInternalId) του προϊόντος αξιοποιώντας την παρακάτω διεπαφή του symbIoTeAPI (Εικόνα 39). Επιστρέφεται μήνυμα με τις μετρήσεις ή σχετικό μήνυμα λάθους (Εικόνα 40).

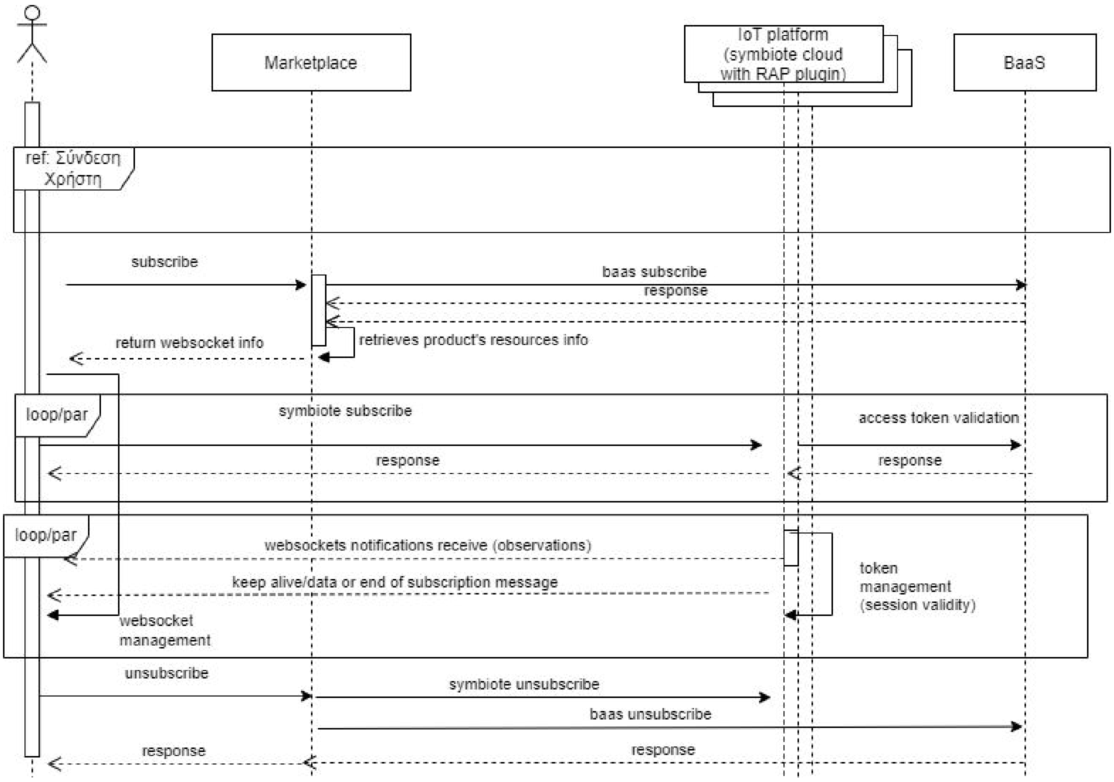


Εικόνα 39: symbIoTeAPI endpoint για πρόσβαση σε δεδομένα πηγής δεδομένων.



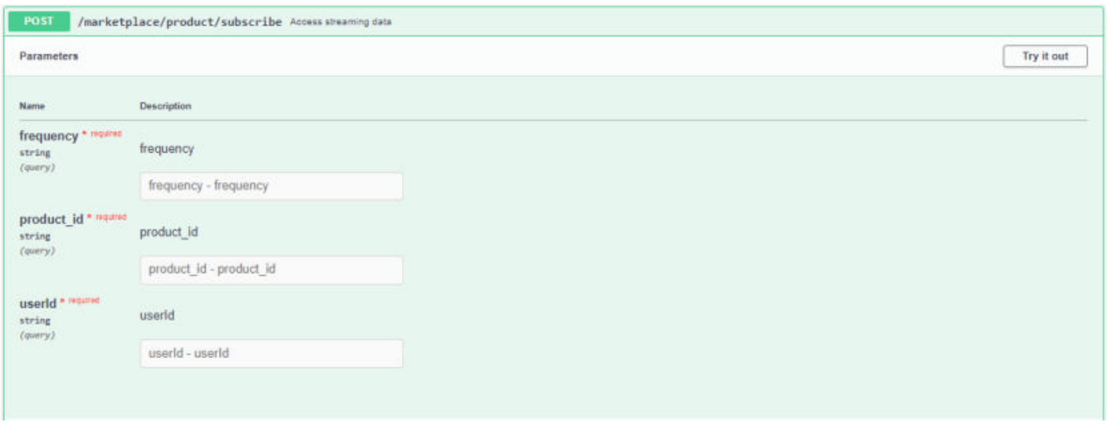
Εικόνα 40:Απάντηση με τις μετρήσεις της πηγής δεδομένων.

Στην περίπτωση streaming προϊόντων, αξιοποιείται ο υπάρχοντας μηχανισμός του symbIoTe ο οποίος επεκτάθηκε για την ενσωμάτωση ελέγχου κουπονιού με το BaaS, όπως φαίνεται στο παρακάτω σχήμα. Ο αντίστοιχος κώδικας με παράδειγμα χρήσης streaming προϊόντος βρίσκεται στο αποθετήριο github του IoTFeds έργου.



Εικόνα 41: Διάγραμμα ροής για streaming προϊόντα.

Πιο συγκεκριμένα, η παρακάτω διεπαφή καλείται από έναν χρήστη για να ανακτήσει τις πληροφορίες σχετικά με την συνδρομή για την διαχείριση των websockets που απαιτούνται. Οι παράμετροι περιλαμβάνουν το αναγνωριστικό του χρήστη, το αναγνωριστικό του προϊόντος που έχει αγοραστεί και την συχνότητα λήψης δεδομένων. Η διεπαφή ενσωματώνει επικοινωνία με το BaaS για τον έλεγχο και ενημέρωση του token.

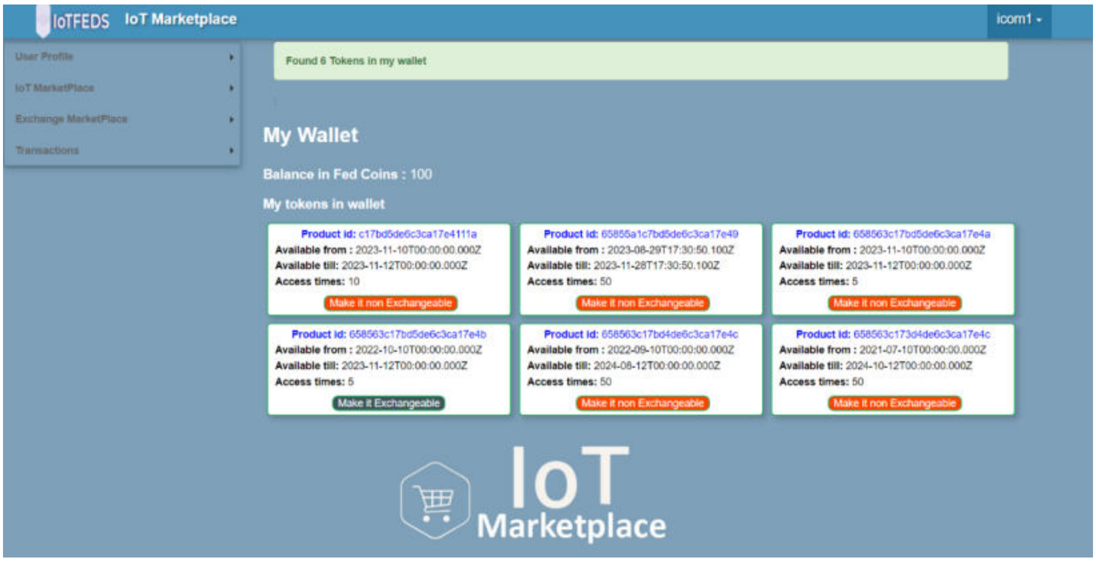


Εικόνα 42: Ενεργοποίηση συνδρομής για προϊόν ροής δεδομένων.

Απαιτείται η διαχείριση των tokens από τη μεριά της κάθε IoT πλατφόρμας που συμμετέχει στο προϊόν καθώς και διαχείριση των websocket sessions για τους IoT πόρους του προϊόντος από τον χρήστη που θέλει να το προσπελάσει. Πιο συγκεκριμένα, ο χρήστης ενημερώνεται με τις πληροφορίες για τον κάθε IoT πόρο του προϊόντος που απαιτούνται για τη διαχείριση του websocket στην απάντηση της παραπάνω διεπαφής. Μετά το άνοιγμα του websocket ο χρήστης χρησιμοποιεί το endpoint του symbIoTe για να στείλει αίτημα subscribe στις εμπλεκόμενες IoT πλατφόρμες ενσωματώνοντας στο αίτημα το token του. Η κάθε IoT πλατφόρμα (RAP plugin) ελέγχει την εγκυρότητα του token με το BaaS και αρχίζει να στέλνει τα δεδομένα στο κανάλι (session) του χρήστη με βάση την καθορισμένη συχνότητα και για όσο διάστημα αναγράφεται στο token. Μετά τη λήξη της συνδρομής ο χρήστης ενημερώνεται με σχετικό μήνυμα και σταματάει να λαμβάνει δεδομένα. Στην περίπτωση λήξης της συνδρομής ή εφόσον ο χρήστης αποφασίσει να λήξει τη συνδρομή νωρίτερα, ο χρήστης ενημερώνει με unsubscribe αίτημα το οποίο προωθείται στις εκάστοτε IoT πλατφόρμες (RAP plugins) και το BaaS. Η ενημέρωση του κουπονιού στο BaaS απαιτείται για την δυνατότητα ανταλλαγής του εφόσον δεν είναι σε χρήση όπως θα περιγραφεί στο Π3.2.

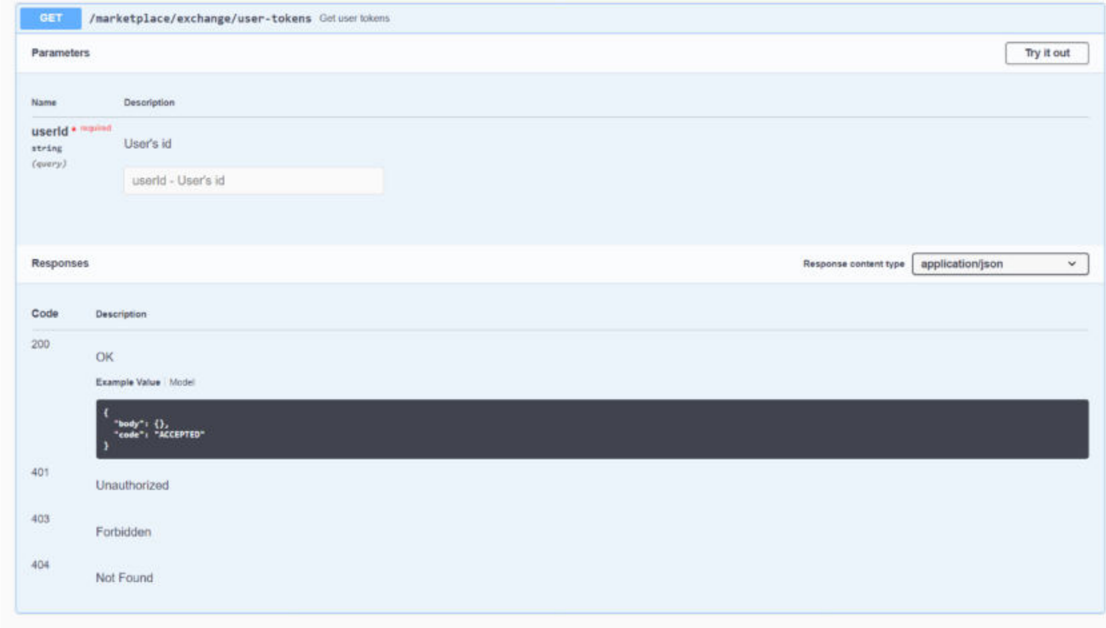
8.1.5 Ενημέρωση προφίλ χρήστη

Ένας χρήστης μπορεί να δει το wallet του (τα έγκυρα κουπόνια για προϊόντα που έχει αγοράσει) μέσα από τη γραφική διεπαφή χρήστη της επισκεπτόμενης αγοράς όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 43: Εμφάνιση του wallet με τα tokens του χρήστη.

Για τη λειτουργικότητα αυτή γίνεται χρήση της παρακάτω διεπαφής που δέχεται ως παράμετρους το αναγνωριστικό του χρήστη (userId), καθώς και προαιρετικά το αναγνωριστικό της αγοράς (MarketplaceId) και το αναγνωριστικό του προϊόντος (productId) στην περίπτωση αναζήτησης για ένα συγκεκριμένο προϊόν. Ο χρήστης ενημερώνεται με τη λίστα των κουπονιών του ή αντίστοιχο μήνυμα λάθους.



Εικόνα 44: Πληροφορίες χρήστη για κουπόνια (wallet) στο Marketplace.

8.2 Μηχανισμοί Ασφαλούς Πρόσβασης στο on-chain σύστημα (BaaS)

Το πρώτο σκέλος της ασφαλούς πρόσβασης στο BaaS αφορά την αντιστοίχιση των προϊόντων στην σωστή αγορά. Ένα προϊόν μπορεί να βρίσκεται σε κάποια ομοσπονδιακή αγορά ή/και στην γενική αγορά. Η ομοσπονδιακή αγορά σχετίζεται με την αντίστοιχη ομοσπονδία μέσω του αναγνωριστικού (id) της ομοσπονδίας. Επομένως, όταν κάποιος χρήστης επιθυμεί να έχει πρόσβαση σε κάποια ομοσπονδιακή αγορά, θα έχει στη διάθεσή του μόνο εκείνα τα προϊόντα που έχουν συσχετιστεί με την συγκεκριμένη ομοσπονδία. Αντίστοιχα, στην γενική αγορά θα έχει στη διάθεσή του μόνο εκείνα που συμμετέχουν σε αυτήν. Ο παραπάνω έλεγχος αποτελεί έναν ABAC μηχανισμό που λαμβάνει υπόψιν του τα χαρακτηριστικά (attributes) του προϊόντος αλλά και χαρακτηριστικά από το περιβάλλον, δηλαδή τα αναγνωριστικά των ομοσπονδιών.

Το δεύτερο κομμάτι της ασφαλούς πρόσβασης στο BaaS αφορά τον έλεγχο για το αν ο χρήστης μπορεί να έχει πρόσβαση σε κάποιο προϊόν και αν ναι, για πόσο καιρό μπορεί να τη διατηρήσει. Αυτή η λειτουργία επιτυγχάνεται με τη δημιουργία ενός access token για κάθε προϊόν που έχει στην κατοχή του ένας χρήστης. Για κάθε χρήστη δημιουργείται ένα «πορτοφόλι» (wallet) στο οποίο αποθηκεύονται τα access tokens. Κάθε φορά που κάποιος χρήστης θέλει να προσπελάσει ένα προϊόν που έχει αγοράσει, ελέγχεται αν διαθέτει το κατάλληλο access token και αν αυτό είναι έγκυρο. Για την υλοποίηση του παραπάνω μηχανισμού, αναπτύχθηκαν οι κατάλληλες συναρτήσεις στα έξυπνα συμβόλαια (smart contracts), αλλά και οι απαραίτητες υπηρεσίες (services).

Στο IoTFeds υπάρχουν δύο είδη προϊόντων, τα προϊόντα ροής δεδομένων (streaming) και τα προϊόντα διακριτών χρήσεων. Για κάθε μία από αυτές τις κατηγορίες, υπάρχει ένας διαφορετικός περιορισμός στο access token, που ελέγχεται για τον έλεγχο πρόσβασης. Στα προϊόντα ροής δεδομένων, ο χρήστης έχει δικαίωμα να χρησιμοποιήσει το προϊόν μέχρι μια συγκεκριμένη ημερομηνία, ενώ στα προϊόντα διακριτών χρήσεων, ο χρήστης μπορεί να τα χρησιμοποιήσει για ένα συγκεκριμένο αριθμό χρήσεων, ή αλλιώς για ένα συγκεκριμένο αριθμό μετρήσεων (observations). Κάθε φορά που ο χρήστης ζητά να πάρει τιμές, κάθε φορά δηλαδή που κάνει χρήση του προϊόντος, ο αριθμός των μετρήσεων που παίρνει αφαιρείται από το διαθέσιμο υπόλοιπό του, έως ότου μηδενιστεί και επομένως τερματιστεί η πρόσβασή του σε αυτό. Είναι σημαντικό να τονιστεί

Το access token περιέχει και άλλες πληροφορίες οι οποίες είναι κοινές για τις δύο κατηγορίες προϊόντων. Αυτές περιλαμβάνουν δύο ημερομηνίες που ορίζουν ένα χρονικό παράθυρο, μέσα στο οποίο οι μετρήσεις που θα λάβει ο χρήστης θεωρούνται έγκυρες. Στην περίπτωση των προϊόντων ροής δεδομένων, αυτό το χρονικό παράθυρο ταυτίζεται με την περίοδο χρήσης. Ακόμη, για τα προϊόντα διακριτών χρήσεων, το access token παραμένει ενεργό για ένα μήνα μετά τη λήξη του χρονικού παραθύρου, ώστε ο χρήστης να μπορέσει να αξιοποιήσει τυχόν εναπομένουσες χρήσεις/μετρήσεις. Οι υπόλοιπες πληροφορίες που περιέχονται στο access token περιλαμβάνουν την συχνότητα του προϊόντος (όπου αυτή εφαρμόζεται), το αναγνωριστικό της αγοράς από την οποία αγοράστηκε, όπως επίσης και πληροφορίες για τον ο χρήστης έχει αξιολογήσει το προϊόν, και αν το έχει ορίσει ως token προς ανταλλαγή.

Επομένως, αμέσως πριν την ολοκλήρωση της αγοράς του προϊόντος, δημιουργείται το wallet του χρήστη, αν αυτή είναι η πρώτη αγορά του, και δημιουργείται το αντίστοιχο access token, ενώ στην περίπτωση που έχει ήδη wallet, απλά δημιουργείται το access token και προστίθεται στο wallet του. Τόσο τα tokens όσο και το wallet αποθηκεύονται on-chain. Πρόκειται στην ουσία για JSON objects, τα οποία έχουν ως attributes τα προϊόντα που έχει στην κατοχή του ο χρήστης και, σε ένα επίπεδο πιο «μέσα» τον χρονικό περιορισμό. Ακόμη, μέσα στο access token περιλαμβάνεται ένα επιπλέον πεδίο το οποίο αναφέρεται στο αν ο χρήστης έχει κάνει κάποιο rating για το συγκεκριμένο προϊόν. Η διαδικασία της αγοράς και κατ' επέκταση η δημιουργία και η αποθήκευση των access tokens γίνεται μέσω των έξυπνων συμβολαίων, οι οποίες γίνονται exposed μέσω συγκεκριμένων services/endpoints σε ένα REST-API.

Έχοντας πραγματοποιήσει επιτυχώς την αγορά ενός προϊόντος, ο χρήστης έχει στην κατοχή του το απαραίτητο access token. Κάθε φορά που επιθυμεί να αποκτήσει πρόσβαση στα δεδομένα που του παρέχει το προϊόν, γίνεται ο απαραίτητος έλεγχος από το BaaS. Το blockchain ψάχνει στον ledger για το wallet του χρήστη. Όταν το βρει, ψάχνει μέσα στο wallet να εντοπίσει το token με την ονομασία του προϊόντος. Αν υπάρχει το συγκεκριμένο token, τότε διαβάζει αυτό το JSON object για να ελέγξει τον περιορισμό.

Αν πρόκειται για προϊόν διακριτών χρήσεων, ελέγχεται αν οι ζητούμενες χρήσεις/μετρήσεις είναι μέσα στο χρονικό παράθυρο και αν επαρκεί το διαθέσιμο υπόλοιπο χρήσεων. Για τα προϊόντα ροής δεδομένων, ελέγχεται αν η δεδομένη χρονική στιγμή χρήσης ανήκει στην επιτρεπόμενη περίοδο χρήσης. Και στις δύο περιπτώσεις ελέγχεται αν το access token έχει τεθεί υπό ανταλλαγή, αλλά και αν είναι ακόμα έγκυρο, αν δηλαδή δεν έχει λήξει. Όταν τα παραπάνω κριτήρια ικανοποιούνται, τότε επιτρέπεται η πρόσβαση στον χρήστη.

Για τα προϊόντα διακριτών χρήσεων, μόλις ο χρήστης λάβει τις ζητούμενες μετρήσεις, το BaaS ενημερώνεται ώστε να γίνει αφαίρεση των χρήσεων από το διαθέσιμο υπόλοιπο. Αν το υπόλοιπο χρήσεων μηδενιστεί, τότε διαγράφεται και το access token. Ωστόσο, στα προϊόντα ροής δεομένων, η λήξη και η διαγραφή του access token από το wallet προγραμματίζεται, να εκτελεστεί μόλις τελειώσει το χρονικό παράθυρο μέσα στο οποίο ο χρήστης λαμβάνει τιμές.

Όσο ο χρήστης έχει στην κατοχή του κάποιο access token για κάποιο προϊόν, δεν μπορεί να το αγοράσει εκ νέου. Θα πρέπει να πρώτα να λήξει το υπάρχον token και μόνο τότε θα μπορεί να το αγοράσει ξανά. Ακόμη, αν προσπαθήσει να αποκτήσει πρόσβαση σε κάποιο προϊόν για το οποίο το token έχει λήξει (και στην ουσία έχει διαγραφεί από το wallet του), δεν θα του επιτραπεί η πρόσβαση. Ο έλεγχος της πρόσβασης γίνεται και πάλι με τη χρήση smart contracts.

Μέσω του BaaS δίνεται στον χρήστη η δυνατότητα να ελέγξει το wallet και τα tokens που έχει διαθέσιμα. Αυτό είναι εφικτό μέσω του αντίστοιχου service που ανασύρει από τον ledger όλο το περιεχόμενο του wallet του χρήστη.

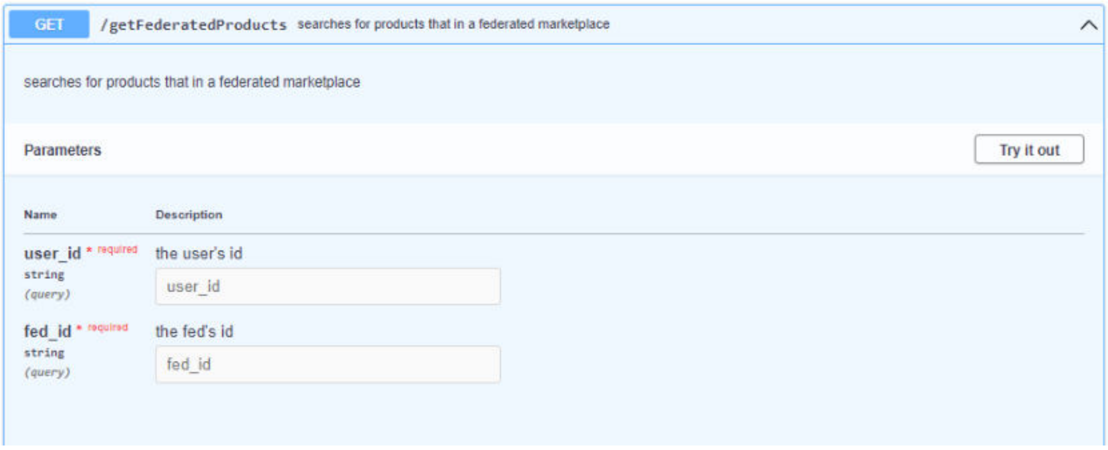
Όλα τα endpoints (services) που εκτελούν τις λειτουργίες που περιεγράφηκαν παραπάνω, συνοψίζονται στον παρακάτω πίνακα (Πίνακας 13).

Πίνακας 13: Endpoints που περιγράφουν τις λειτουργίες για την ασφαλή πρόσβαση του BaaS.

#	Inter-face	Name	Request from	Request to	Method	Endpoint /Queue	Payload	Response	Description
1	REST	getFederatedProducts	marketplace API	BaaS	GET	/baas/products /get_federated_products	(String, String)	(Object, Message)	Αίτηση ανάκτησης προϊόντων από την ομοσπονδιακή αγορά
2	REST	getGlobalProducts	marketplace API	BaaS	GET	/baas/products /get_global_products	(String)	(Object, Message)	Αίτηση ανάκτησης προϊόντων από την καθολική αγορά
3	REST	checkAccess	marketplace API	BaaS	POST	/baas/products /check_access	(String, String, String, String, String)	(Object)	Αίτηση για έλεγχο της πρόσβασης σε ένα προϊόν
4	REST	decreaseAccess	marketplace API	BaaS	POST	/baas/products/decrease_access	(String, String, Integer	(Object)	Αίτηση μείωσης των διαθέσιμων χρόνων πρόσβασης (observations)
5	REST	getUserTokens	marketplace API	BaaS	GET	/baas/products /get_user_tokens	(String)	(Object, Message)	Αίτηση για έλεγχο των access token για ένα χρήστη (από το χρήστη)
6	REST	unsubscribeProduct	marketplace API	BaaS	POST	/baas/products/unsubscribe_product	(String, String)	(Object, Message)	Αίτηση απεγγραφής προϊόντος σε περίπτωση λήξης ή κατάργησης της συνδρομής του χρήστη

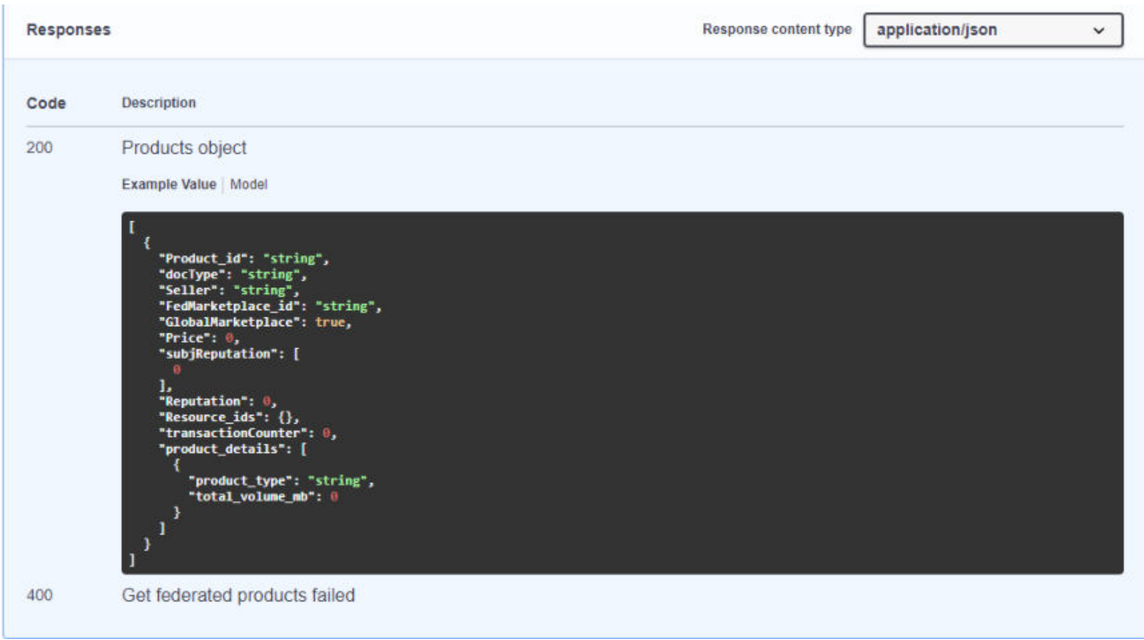
8.2.1 Ανάκτηση Προϊόντων για μια Ομοσπονδιακή Αγορά

Αφορά την ανάκτηση των προϊόντων που ανήκουν σε μια συγκεκριμένη ομοσπονδιακή αγορά. Δέχεται ως είσοδο το αναγνωριστικό (id) του χρήστη και το αναγνωριστικό (id) της ομοσπονδιακής αγοράς και επιστρέφει μήνυμα αποτυχίας, σε περίπτωση σφάλματος, ενώ επιστρέφει έναν πίνακα με τα αντικείμενα των προϊόντων, όπως φαίνεται στην Εικόνα 45. Το συγκεκριμένο endpoint μπορεί να χρησιμοποιηθεί από το symbIoTe/Marketplace ώστε να εμφανίσει όλα τα προϊόντα που είναι συσχετισμένα με κάποια ομοσπονδιακή αγορά.



Εικόνα 45: Παράμετροι του endpoint για την ανάκτηση προϊόντων από ομοσπονδιακή αγορά.

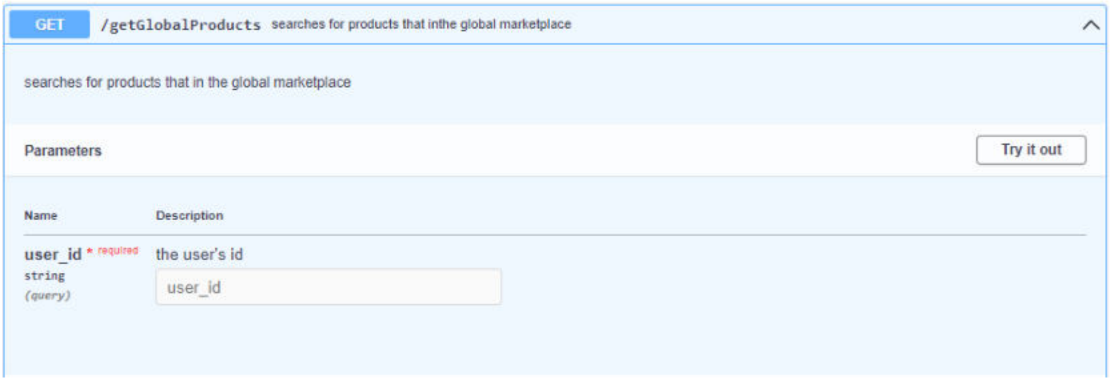
Ο μονοδιάστατος πίνακας που επιστρέφεται από αυτό το endpoint περιλαμβάνει όλα τα προϊόντα (objects) που ανήκουν σε αυτή την αγορά (Εικόνα 46).



Εικόνα 46: Πίνακας με object που επιστρέφεται μετά από επιτυχή ανάκτηση προϊόντων από ομοσπονδιακή αγορά.

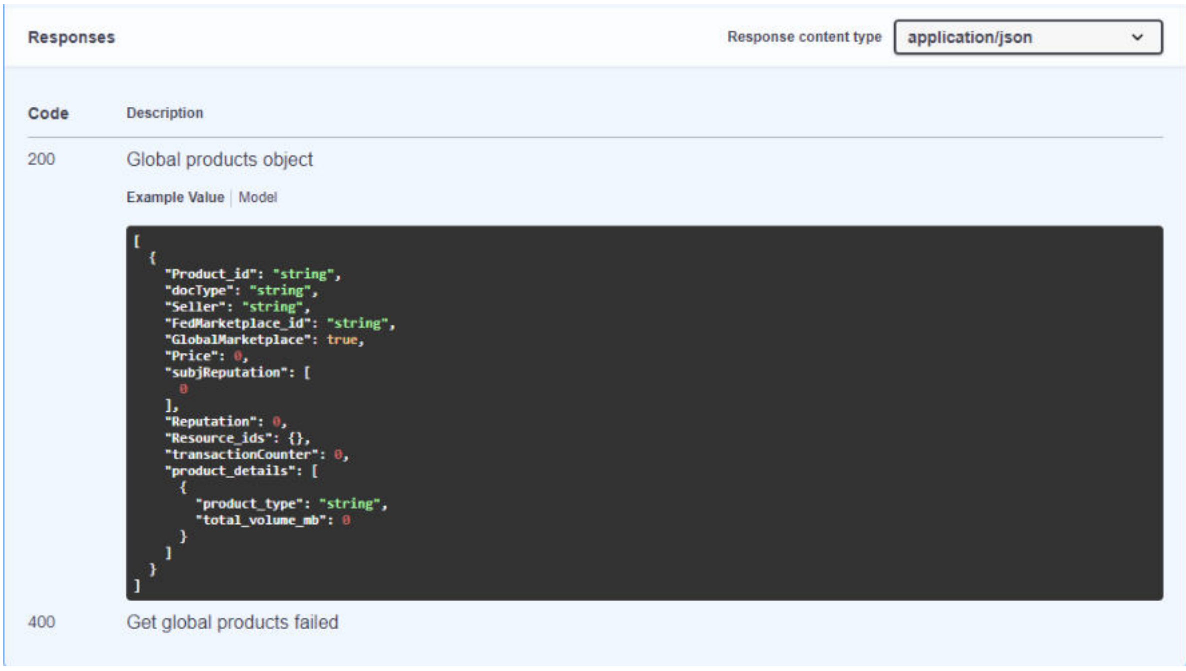
8.2.2 Ανάκτηση Προϊόντων για την Καθολική Αγορά

Αφορά την ανάκτηση των προϊόντων που ανήκουν στην γενική αγορά. Δέχεται ως είσοδο μόνο το αναγνωριστικό (id) του χρήστη και επιστρέφει μήνυμα αποτυχίας, σε περίπτωση σφάλματος, ενώ επιστρέφει έναν πίνακα με τα αντικείμενα των προϊόντων, όπως φαίνεται στην Εικόνα 48.



Εικόνα 47: Παράμετροι του endpoint για την ανάκτηση προϊόντων από την γενική αγορά.

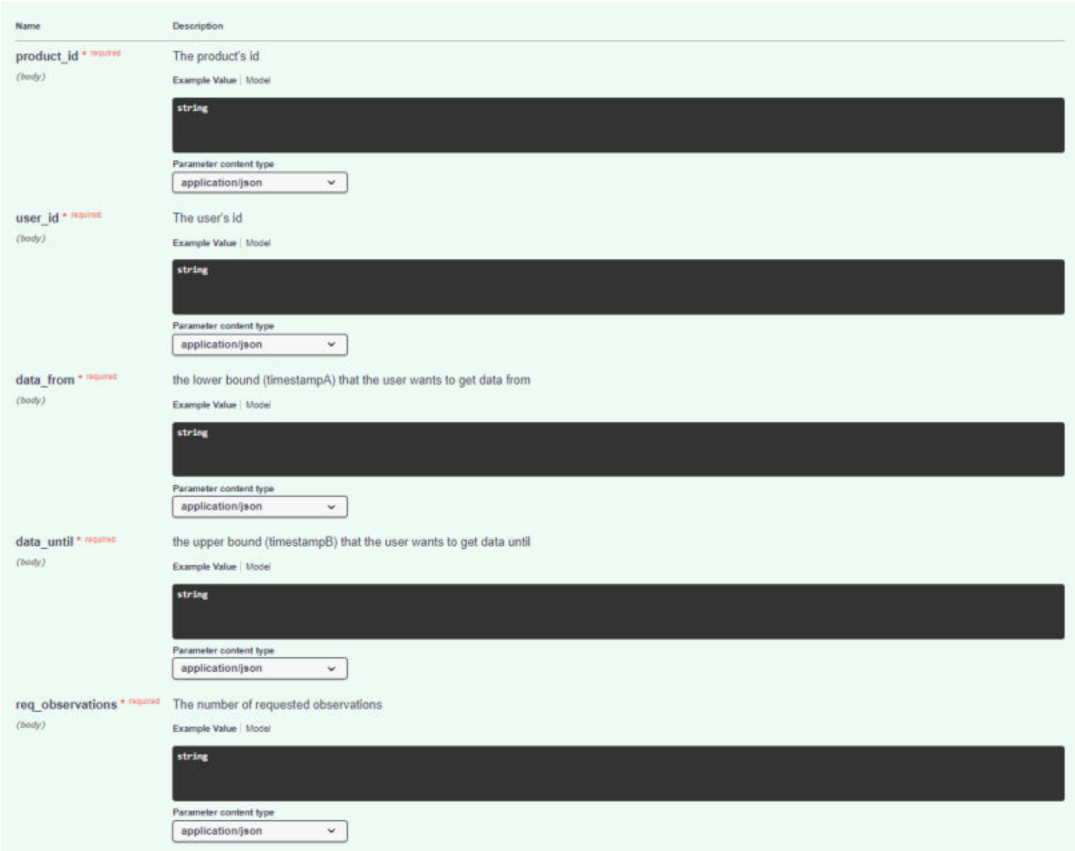
Ο πίνακας που επιστρέφεται από αυτό το endpoint περιλαμβάνει όλα τα προϊόντα (objects) που ανήκουν στην γενική αγορά (Εικόνα 48).



Εικόνα 48: Πίνακας με object που επιστρέφεται μετά από επιτυχή ανάκτηση προϊόντων από την γενική αγορά.

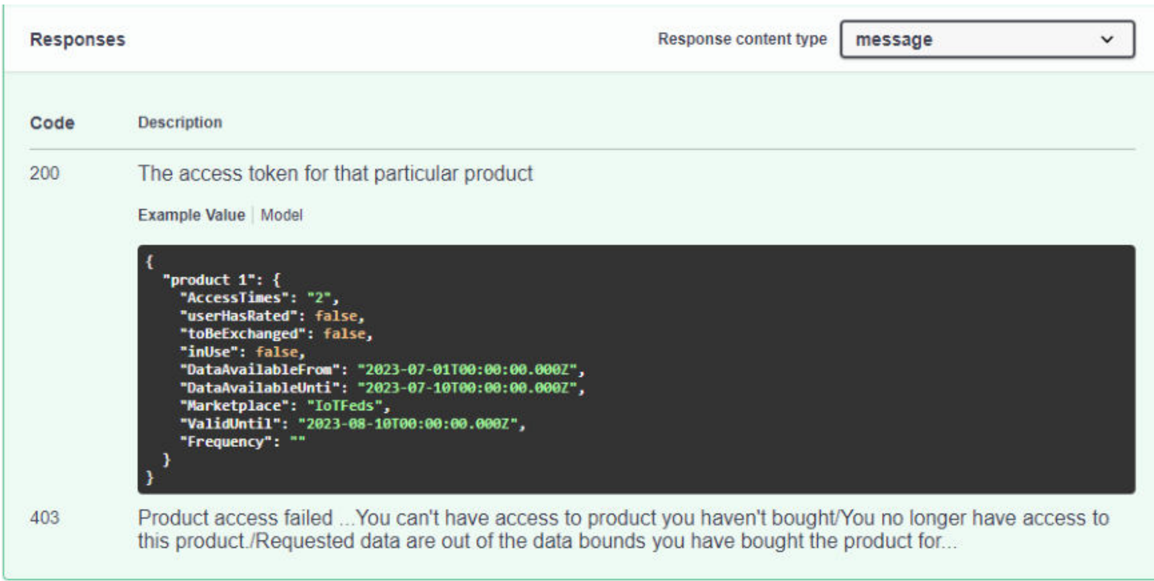
8.2.3 Έλεγχος Πρόσβασης σε ένα Προϊόν

Αφορά τον έλεγχο για την εξουσιοδοτημένη πρόσβαση ενός χρήστη σε ένα συγκεκριμένο προϊόν, μέσα από τον έλεγχο του access token. Δέχεται ως είσοδο το αναγνωριστικό (id) του χρήστη και το αναγνωριστικό (id) του προϊόντος, το κάτω και άνω χρονικό φράγμα μέσα στο οποίο ο χρήστης έχει πρόσβαση στο προϊόν, όπως επίσης και τον ζητούμενο αριθμό μετρήσεων, και επιστρέφει το access token για το συγκεκριμένο προϊόν στην περίπτωση της επιτυχημένης πρόσβασης, ενώ επιστρέφει μήνυμα αποτυχίας όταν ο χρήστης δεν έχει πρόσβαση στο προϊόν, όπως φαίνεται στην Εικόνα 49.



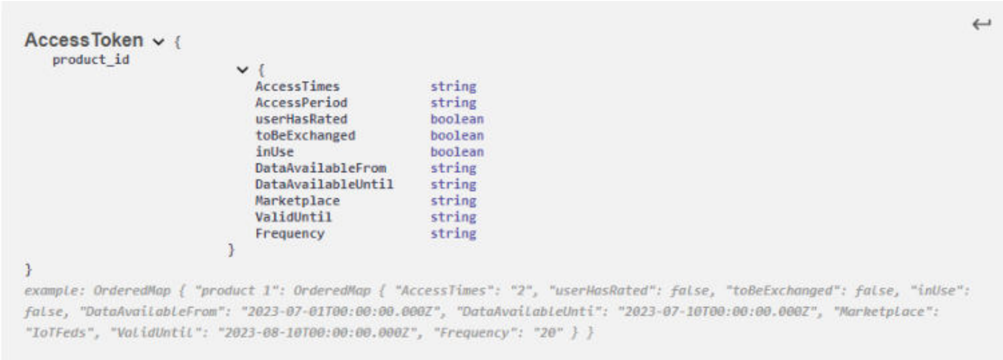
Εικόνα 49: Παράμετροι του endpoint για τον έλεγχο της ασφαλούς πρόσβασης σε ένα προϊόν.

Το αντικείμενο που επιστρέφεται περιλαμβάνει ένα JSON αντικείμενο που περιέχει το access token του χρήστη για το προϊόν (Εικόνα 50).



Εικόνα 50: Αντικείμενο που επιστρέφεται με το access token του προϊόντος.

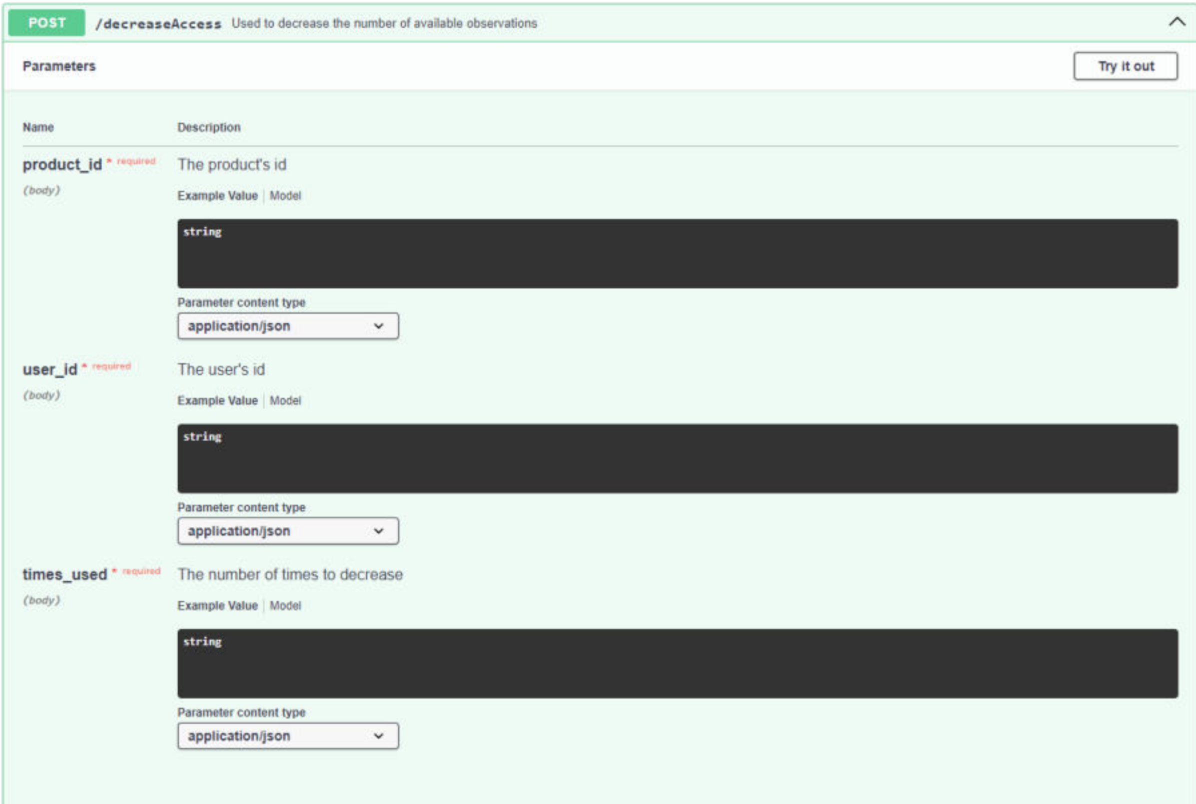
Τέλος, στην Εικόνα 51 παρουσιάζεται το αντικείμενο που περιγράφει τα access tokens που ελέγχονται για την ασφαλή πρόσβαση.



Εικόνα 51: Το αντικείμενο που περιγράφει τα access tokens που ελέγχονται για την ασφαλή πρόσβαση.

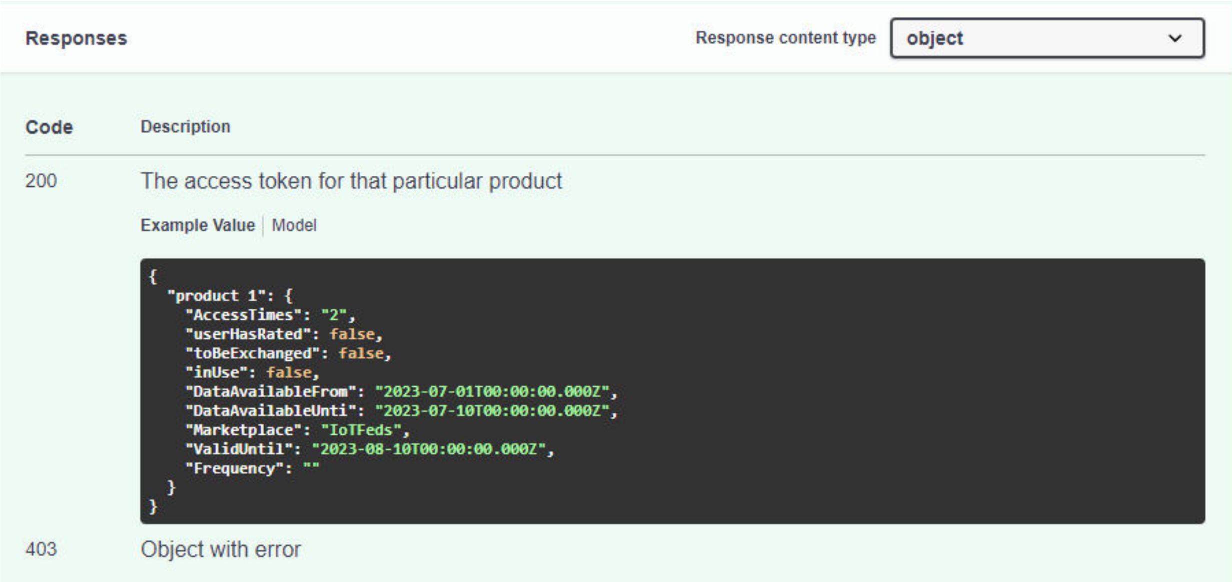
8.2.4 Μείωση διαθέσιμων χρήσεων

Αφού ο χρήστης έχει αποκτήσει πρόσβαση στο προϊόν και καθοριστεί ο τελικός αριθμός χρήσεων που θα του αφαιρεθεί, καλείται το συγκεκριμένο service. Δέχεται ως είσοδο το αναγνωριστικό (id) του προϊόντος, το αναγνωριστικό (id) του χρήστη και τον αριθμό των χρήσεων/μετρήσεων που τελικά θα αφαιρεθούν (Εικόνα 52).



Εικόνα 52: Παράμετροι του endpoint για την αφαίρεση χρήσεων/μετρήσεων.

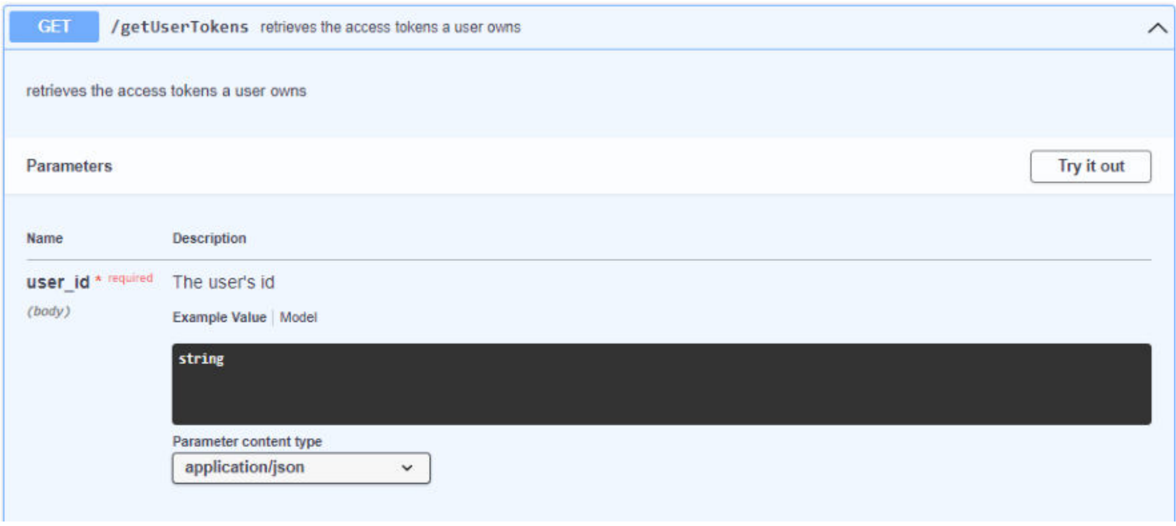
Το αντικείμενο που επιστρέφεται περιλαμβάνει ένα JSON αντικείμενο που περιέχει το access token του χρήστη για το προϊόν, ενημερωμένο με το νέο αριθμό διαθέσιμων χρήσεων/μετρήσεων (Εικόνα 53).



Εικόνα 53: Αντικείμενο που επιστρέφεται με το access token του προϊόντος.

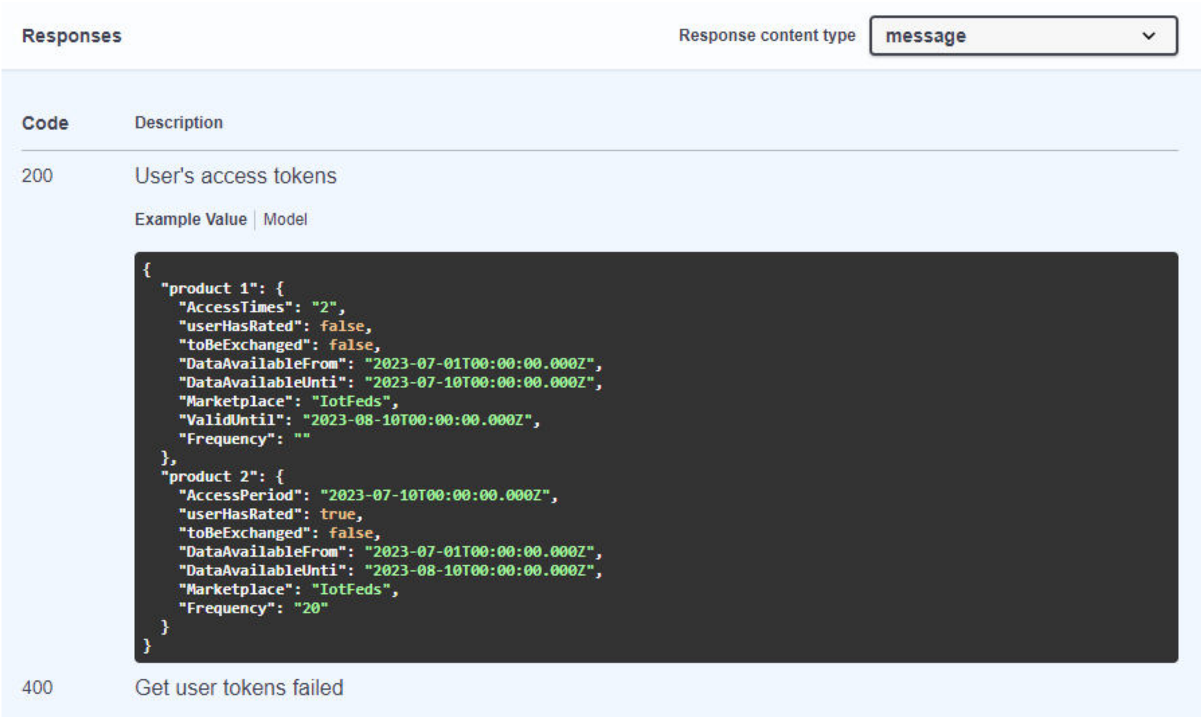
8.2.5 Ανάκτηση πληροφοριών του Wallet ενός Χρήστη

Αφορά τον έλεγχο του wallet ενός χρήστη από τον ίδιο τον χρήστη, ώστε να ελέγξει τα access tokens που έχει στην κατοχή του. Δέχεται ως είσοδο το αναγνωριστικό (id) του χρήστη και επιστρέφει το αντικείμενο του wallet του χρήστη, ενώ σε περίπτωση αποτυχίας επιστρέφει το κατάλληλο μήνυμα, όπως φαίνεται στην Εικόνα 54. Αυτή η ενέργεια μπορεί να χρησιμοποιηθεί από τον χρήστη ώστε να ελέγξει σε ποια προϊόντα έχει ακόμα πρόσβαση και για πόσο καιρό ή τις διαθέσιμες χρήσεις που του απομένουν, αν έχει ψηφίσει (rating) για κάθε προϊόν, ανάμεσα σε άλλες πληροφορίες.



Εικόνα 54: Παράμετροι του endpoint για την ανάκτηση πληροφοριών για το wallet ενός χρήστη.

Το αντικείμενο που επιστρέφεται περιλαμβάνει τα αντικείμενα των access tokens που διαθέτει ο χρήστης (Εικόνα 55).



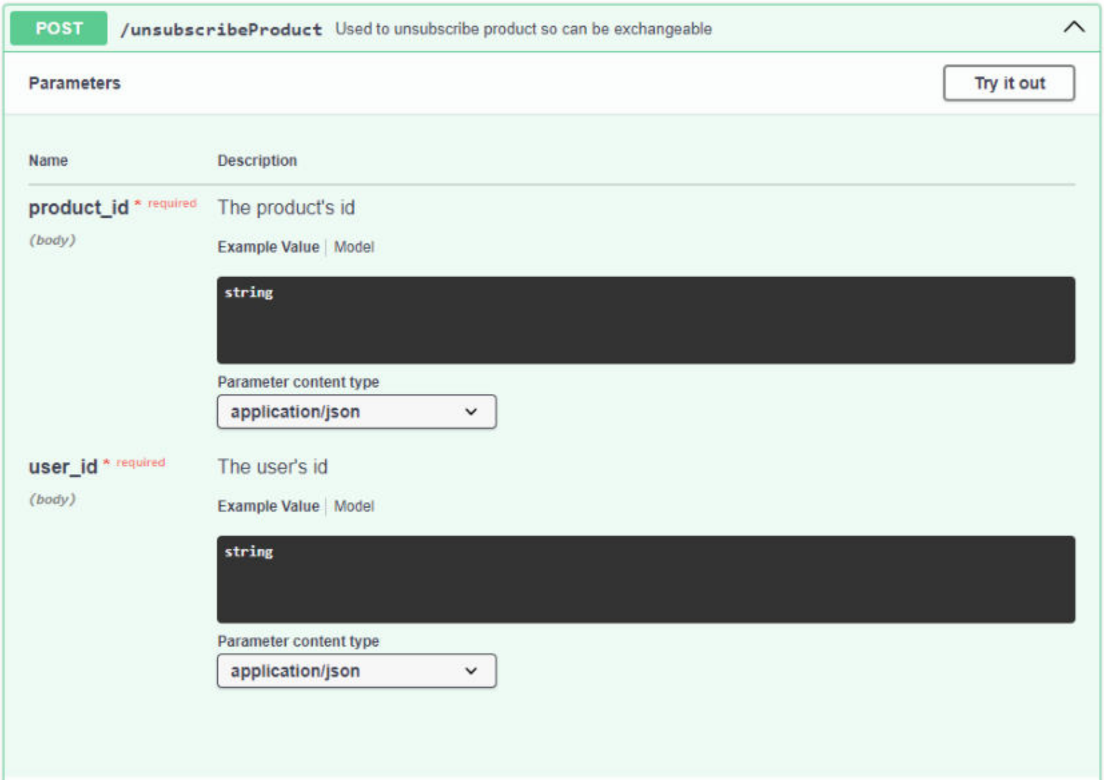
Εικόνα 55: Το αντικείμενο που επιστρέφεται μετά από επιτυχή ανάκτηση του wallet του χρήστη.

Τέλος, στην Εικόνα 56 παρουσιάζεται το αντικείμενο που περιγράφει το wallet του χρήστη.

Εικόνα 56: Το αντικείμενο που περιγράφει το wallet του χρήστη.

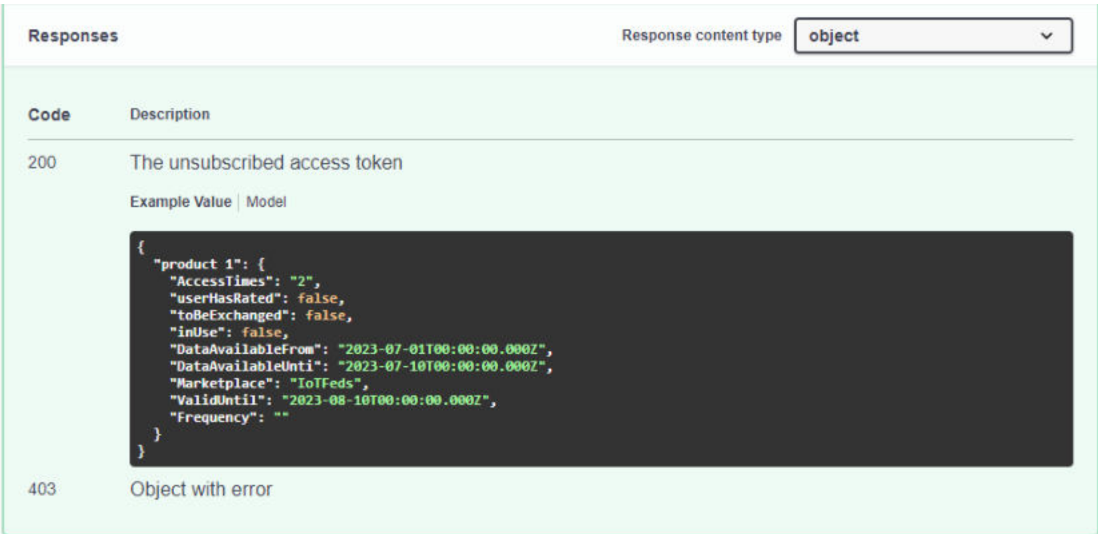
8.2.6 Απεγγραφή Προϊόντος από το BaaS

Σχετίζεται με την απεγγραφή του προϊόντος του χρήστη σε περίπτωση λήξης ή πρόωρης κατάργησης της συνδρομής του, με την προϋπόθεση ότι αυτό δε βρίσκεται πλέον σε χρήση, όπως θα περιγραφεί στο Π3.2. Στη συγκεκριμένη περίπτωση δημιουργείται από το χρήστη ένα αίτημα απεγγραφής μέσω του marketplace και προωθείται τόσο στις εκάστοτε IoT πλατφόρμες, όσο και στο BaaS. Όσον αφορά την πλευρά του BaaS, η αίτηση απεγγραφής περιλαμβάνει τα αναγνωριστικά (ids) του προϊόντος και του χρήστη, όπως φαίνεται στην Εικόνα 57, και επιστρέφει το access token του προϊόντος που απεγγράφη, ενώ σε περίπτωση αποτυχίας απεγγραφής του, εμφανίζεται κατάλληλο μήνυμα αποτυχίας.



Εικόνα 57: Παράμετροι του endpoint για την απεγγραφή προϊόντος από το BaaS.

Το αντικείμενο που επιστρέφεται περιλαμβάνει ένα JSON αντικείμενο που περιέχει το access token του χρήστη για το προϊόν (Εικόνα 58).



Εικόνα 58: Το αντικείμενο που επιστρέφεται μετά την επιτυχή απεγγραφή προϊόντος από το BaaS.

9 Συμπεράσματα

Το παρόν παραδοτέο αναφέρεται στη δεύτερη ΕΕ του έργου IoTFeds (ΕΕ2 – «Ομοσπονδίες IoT και Διαλειτουργικότητα») και, πιο συγκεκριμένα, στη Δ2.3 – «Διαφήμιση και Ανακάλυψη Ομόσπονδων Πόρων IoT» και περιλαμβάνει την ανάλυση των μηχανισμών αναζήτησης, διαφήμισης και ασφαλούς πρόσβασης τόσο σε IoT πόρους, όσο και σε προϊόντα, οι οποίοι προσφέρονται από τα βασικά συστήματα της IoTFeds πλατφόρμας (BaaS και symbIoTe API).

Οι βασικές συνεισφορές του συγκεκριμένου παραδοτέου είναι η εξερεύνηση του τεχνολογικού υποβάθρου για υφιστάμενες λύσεις μηχανών αναζήτησης, αλγορίθμων ταξινόμησης και συστημάτων ασφαλείας σε blockchain, η περιγραφή των μηχανισμών που υλοποιούνται από το BaaS και το symbIoTe για την υλοποίηση της συγκεκριμένης δράσης καθώς και οι η παρουσίαση των εμπλεκόμενων διεπαφών των υποσυστημάτων του IoTFeds (BaaS, symbIoTe API και marketplace) που αναπτύχθηκαν. Πιο συγκεκριμένα, οι μηχανισμοί που περιγράφονται περιλαμβάνουν αρχικά τους μηχανισμούς αναζήτησης βάσει των οποίων ο χρήστης δύναται να αναζητά πόρους IoT και προϊόντα δεδομένων στην IoTFeds πλατφόρμα. Στη συνέχεια, ακολουθεί η περιγραφή των αλγορίθμων που χρησιμοποιήθηκαν για την υλοποίηση της διαφήμισης τόσο των IoT πόρων, όσο και των προϊόντων που περιλαμβάνονται στην πλατφόρμα. Επιπλέον, γίνεται ανάλυση των μηχανισμών των βασικών συστημάτων της πλατφόρμας που επιτρέπουν την ασφαλή πρόσβαση στα IoT δεδομένα. Τέλος, περιλαμβάνεται επίσης ανάλυση του μηχανισμού που επιτρέπει στο χρήστη τη σύνθεση ενός προϊόντος στα πλαίσια της IoTFeds πλατφόρμας και περιγραφή της πλήρους ροής της διαδικασίας μέσω ενός κατάλληλου διαγράμματος ακολουθίας.

Βιβλιογραφία

Alansari, S., Paci, F., & Sassone, V. (2017). A distributed access control system for cloud federations. *2017 IEEE 37th international conference on distributed computing systems (ICDCS)*, (σσ. 2131–2136).

BitClave. (2017). Active Search Ecosystem. *Active Search Ecosystem*. Ανάκτηση από https://cryptorating.eu/whitepapers/BitClave/BitClaveWhitePapernewdesign(current).pdf

Cai, C., Weng, J., Yuan, X., & Wang, C. (2018). Enabling reliable keyword search in encrypted decentralized storage with fairness. *IEEE Transactions on Dependable and Secure Computing, 18*, 131–144.

Demsyn-Jones, R. (2022). Measurement and applications of position bias in a marketplace search engine. *arXiv preprint arXiv:2206.11720*.

Do, H. G., & Ng, W. K. (2017). Blockchain-based system for secure data storage with private keyword search. *2017 IEEE World Congress on Services (SERVICES)*, (σσ. 90–93).

Du, Y., Fang, M., Yi, J., Xu, C., Cheng, J., & Tao, D. (2018). Enhancing the robustness of neural collaborative filtering systems under malicious attacks. *IEEE Transactions on Multimedia, 21*, 555–565.

Hardjono, T., & Pentland, A. (2019). Verifiable anonymous identities and access control in permissioned blockchains. *arXiv preprint arXiv:1903.04584*.

He, P., Yu, G., Zhang, Y., & Bao, Y. (2017). 区块链技术与应用前瞻综述 (Survey on Blockchain Technology and Its Application Prospect). *计算机科学, 44*, 1–7.

Herlocker, J. L., Konstan, J. A., & Riedl, J. (2000). Explaining collaborative filtering recommendations. *Proceedings of the 2000 ACM conference on Computer supported cooperative work*, (σσ. 241–250).

HyperledgerFoundation. (2022). Hyperledger Aries. *Hyperledger Aries*. Ανάκτηση από https://www.hyperledger.org/use/aries

Jiang, S., Duan, Y., & Wu, J. (2019). A client-biased cooperative search scheme in blockchain-based data markets. *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, (σσ. 1–9).

Joachims, T., Granka, L., Pan, B., Hembrooke, H., Radlinski, F., & Gay, G. (2007). Evaluating the accuracy of implicit feedback from clicks and query reformulations in web search. *ACM Transactions on Information Systems (TOIS), 25*, 7–es.

Joo, M., Kim, S. H., Ghose, A., & Wilbur, K. C. (2022). Designing Distributed Ledger technologies, like Blockchain, for advertising markets. *International Journal of Research in Marketing*.

Jøsang, A. (1996). The right type of trust for distributed systems. *Proceedings of the 1996 workshop on New security paradigms*, (σσ. 119–131).

Jøsang, A. (2007). Trust and reputation systems. *Foundations of Security Analysis and Design IV: FOSAD 2006/2007 Tutorial Lectures*, (σσ. 209–245).

Kocher, G., & Agrawa, N. (2014). Analysis and review of sorting algorithms.

Li, W., Li, H., Chen, H., & Xia, Y. (2015). Adattester: Secure online mobile advertisement attestation using trustzone. *Proceedings of the 13th annual international conference on mobile systems, applications, and services*, (σσ. 75–88).

Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and computer-integrated manufacturing, 54*, 133–144.

Liu, D., Huang, C., Ni, J., Lin, X., & Shen, X. (2020). Blockchain-based smart advertising network with privacy-preserving accountability. *IEEE Transactions on Network Science and Engineering, 8*, 2118–2130.

Liu, H., & Chen, J. (2017). Distributed privacy-aware fast selection algorithm for large-scale data. *IEEE Transactions on Parallel and Distributed Systems, 29*, 365–376.

Liu, Y., Liu, J., Zhang, Z., & Yu, H. (2020). A fair selection protocol for committee-based permissionless blockchains. *Computers & Security, 91*, 101718.

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration, 15*, 80–90.

Matz, A., & Götz, C. (2020). Designing Human-Centered Interactions for Smart Environments Based on Heterogeneous, Interrelated Systems: A User Research Method for the "Age of Services"(URSERVe). *International Conference on Human-Computer Interaction*, (σσ. 99–116).

Mohammadi, V., Rahmani, A. M., Darwesh, A. M., & Sahafi, A. (2019). Trust-based recommendation systems in Internet of Things: a systematic literature review. *Human-centric Computing and Information Sciences, 9*, 1–61.

Nebulas. (2017). Nebulas Technical Whitepaper. *Nebulas Technical Whitepaper*. Ανάκτηση από https://www.nebulas.io/docs/NebulasTechnicalWhitepaper.pdf

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing, 22*, 14743–14757.

Paillisse, J., Subira, J., Lopez, A., Rodriguez-Natal, A., Ermagan, V., Maino, F., & Cabellos, A. (2019). Distributed access control with blockchain. *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, (σσ. 1–6).

Parra-Arnau, J., Achara, J. P., & Castelluccia, C. (2017). Myadchoices: Bringing transparency and control to online advertising. *ACM Transactions on the Web (TWEB), 11*, 1–47.

PreSearch. (2017). PreSearch Whitepaper. *PreSearch Whitepaper*. Ανάκτηση από https://whitepaper.io/coin/presearch

RapidInnovation. (2021, November). Why Decentralized Search Engines are the Future of Censorship-Free Search. *Why Decentralized Search Engines are the Future of Censorship-Free Search*. Ανάκτηση από https://blog.rapidinnovation.io/decentralized-search-engines-future-censorship-free-search/

Raza, A., Han, K., & Hwang, S. O. (2020). A framework for privacy preserving, distributed search engine using topology of DLT and onion routing. *IEEE Access, 8*, 43001–43012.

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM, 43*, 45–48.

Rogers, I. (2002). The Google Pagerank algorithm and how it works.

Rouhani, S., Belchior, R., Cruz, R. S., & Deters, R. (2021). Distributed attribute-based access control system using permissioned blockchain. *World Wide Web, 24*, 1617–1644.

Shahbazi, Z., Hazra, D., Park, S., & Byun, Y. C. (2020). Toward improving the prediction accuracy of product recommendation system using extreme gradient boosting and encoding approaches. *Symmetry, 12*, 1566.

Sovrin. (2022). Sovrin. *Sovrin*. Ανάκτηση από https://sovrin.org/

Sudeepthi, G., Anuradha, G., & Babu, M. S. (2012). A survey on semantic web search engine. *International Journal of Computer Science Issues (IJCSI), 9*, 241.

Tahir, S., & Rajarajan, M. (2018). Privacy-preserving searchable encryption framework for permissioned blockchain networks. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, (σσ. 1628–1633).

Tang, J., Lu, X., Xiang, Y., Shi, C., & Gu, J. (2022). Blockchain search engine: Its current research status and future prospect in Internet of Things network. *Future Generation Computer Systems*.

Venkatadri, G., Mislove, A., & Gummadi, K. P. (2018). Treads: transparency-enhancing ads. *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*, (σσ. 169–175).

Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *Ieee Access, 6*, 38437–38450.

Zhang, Y., Yutaka, M., Sasabe, M., & Kasahara, S. (2020). Attribute-based access control for smart cities: A smart-contract-driven framework. *IEEE Internet of Things Journal, 8*, 6372–6384.

Zhu, L., Zhang, J., Xiao, Z., Cao, X., Wu, D. O., & Xia, X.-G. (2019). Joint Tx-Rx beamforming and power allocation for 5G millimeter-wave non-orthogonal multiple access networks. *IEEE Transactions on Communications, 67*, 5114–5125.

Zyskind, G., Nathan, O., & others. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, (σσ. 180–184).