Universitatea Tehnică a Moldovei

Managementul identităţilor în aplicaţii IoT

Identity management in IoT applications

Masterand:

Maximciuc Ion

Conducător:

Conf. univ., dr. Sudacevschi Viorica

Chişinău 2018

Adnotation

Nowadays, people are united in their need to be connected to the Internet anywhere, anytime, any place. Thanks to the evolution of Information communication technologies (ICT) more and more exclusive services (smart homes, telemedicine, e-Health applications etc.) are available for the users through heterogeneous Internet of Things (IoT) networks, driven by machine to machine (M2M) communication. Although, the communication is established primarily by using devices, the human users are real “generators” and “consumers” of the input and output information. Thus, the human user has to be considered as a “smart” IoT object, thus he/she should be identified, authenticated, authorized.

The process of user identification is considered to be very delicate due to the concerns for the people’s willingness of sharing private information and data. At the same time, the utilized by a certain user devices, should be taken into consideration. Within this context there is a need of attractive user identification and Identity Management (IdM) mechanisms, involving all of the objects in IoT. Furthermore, the active role of the user in the creation of the rules of identification, and having always responsive services, are extremely important and slightly moving the focus to the concept of ‘Internet of People’. The present master thesis addresses the problems of user identification and proposes the design of an IdM system where the end-user is in the middle of a user-centered services ecosystem. The proposed scheme enables user recognition and assigned services access only by identification of one of the “things” related to the user (personal computing devices, sensors etc). Besides, the author proposes a novel user identification method driven by computing device recognition algorithm (CDR algorithm). The proposed CDR algorithm and IdM system were evaluated through a set of technical and business analytical methodologies in order to proof the concept. The discussion confirms the importance of the researched matter and further clarifies the objectives.

Nowadays blockchain has gained the interest of both technological and business sectors. Accordingly, the energy sector is considering blockchain as the future of their infrastructure. There are two visions for energy system related to this, closed model and open model. Technically speaking, closed model related to the intranet system and open model to the internet system. Particularly, through its decentralized mechanism, blockchain could offer a decentralized energy transmission and supply system in an open model environment supported by the use of the Internet of Things and artificial intelligence. In an open model, there are interconnected devices and machine-to-machine interactions, and the transaction data is stored on the blockchain. Users and companies identify themselves using their digital identities. Therefore, due to the implementation of blockchain, there is a need for different kinds of digital identity management. In this study, we examine three categories of digital identity federated identity, user-centric identity, and hybrid identity to determine which is best suited for the open model energy system that is our case study. In order to move towards open model, we need to evaluate also the closed model implementation. Thus the basic method that we apply is a comparison of the digital identity categories based on their implementations for both closed and open model, advantages, disadvantages, and similarities with blockchain characteristics and open model characteristics. The proposed solution reveals that hybrid identity is most likely the most appropriate for an open model system. Additionally, this research also proposes some properties that are needed to be developed the selected digital identity category.

Adnotare

În zilele noastre, oamenii sunt uniți în ceea ce privește necesitatea lor de a fi conectați la Internet mereu, în orice loc și la orice oră. Datorită evoluției a Tehnologielor de comunicare a informației (TCI) din ce în ce mai multe servicii exclusive (case inteligente, telemedicina, aplicații e-Sănătate etc.) sunt disponibile pentru utilizatori prin rețelele eterogene a Internetului Lucrurilor (IL), conduse de comunicarea mașină către mașină (M2M). Deși, comunicarea este în primul rând stabilită prin folosirea dispozitivelor, utilizatorii sunt "consumatori" și "generatori" reali a informației de intrare și ieșire. Așa că, oamenii trebuie să fie considerați la fel de "inteligenți" ca obiectul IoT, așa că el/ea trebuie să fie identificați, autentificați și autorizați.

Procesul de indetificare a utilizatorului este considerat a fi foarte delicat datorită buneivoinței oamenilor de a împărtăși date și informații private. În același timp, utilizat de același tip de dipozitiv a utilizatorului, trebuie să fie luată în considerație. În acest context, este nevoie de o identificare atractivă a utilizatorilor și Gestionarea identității (Gid), implicând toate obiectele din IoT. În plus, rolul activ al utilizatorului în crearea regulilor de identificare, și având mereu servicii receptive, este extrem de important și se concentrează ușor pe conceptul de "Internet al oamenilor". Teza de masterat prezentă abordează problemele de identificare a utilizatorilor și propune proiectarea unui nou sistem IdM unde utilizatorul final se află în mijlocul unui ecosistem de servicii centrat pe utilizator. Schema propusă permite recunoașterea utilizatorilor și accesul la servicii alocate numai prin identificarea unuia dintre "lucrurile" legate de utilizator (dispozitive de calcul personale, senzori etc.). În plus, autorul propune o metodă nouă de identificare a utilizatorului condusă de algoritmul de recunoaștere a dispozitivelor de calcul (algoritmul CDR). Algoritmul propus CDR și sistemul IdM au fost evaluate printr-un set de metodologii analitice tehnice și de afaceri pentru a dovedi conceptul. Discuția confirmă importanța chestiunii cercetate și clarifică în continuare obiectivele.

În prezent, blockchain-ul a câștigat interesul atât al sectoarelor tehnologice, cât și al celor de afaceri. În consecință, sectorul energetic are în vedere blockchain-ul ca viitorul infrastructurii. Există două viziuni asupra sistemului energetic legat de acest model, modelul închis și modelul deschis. Din punct de vedere tehnic, modelul închis legat de sistemul intranet și modelul deschis către sistemul de internet. În special, prin mecanismul său descentralizat, blockchain-ul ar putea oferi un sistem decentralizat de transmisie și furnizare a energiei într-un mediu model deschis, susținut de utilizarea internetului tuturor lucrurilor și a inteligenței artificiale. Într-un model deschis, există dispozitive interconectate și interacțiuni dintre mașină și mașină, iar datele despre tranzacții sunt stocate în blockchain. Utilizatorii și companiile se identifică prin identitatea lor digitală. Prin urmare, datorită implementării blockchain-ului, este nevoie de diferite tipuri de gestionare a identității digitale. În acest studiu, examinăm trei categorii de identitate digitală identitate federalizată, identitate orientată spre utilizator și identitate hibridă - pentru a determina care este cea mai potrivită pentru sistemul de energie deschis model care este studiul nostru de caz. Pentru a trece spre un model deschis, trebuie să evaluăm și implementarea modelului închis.
Astfel, metoda de bază pe care o aplicăm este o comparație a categoriilor de identitate digitală bazate pe implementările lor atât pentru modelul închis, cât și pentru modelul deschis, avantajele, dezavantajele și asemănările cu caracteristicile blockchain-ului și caracteristicile modelului deschis. Soluția propusă demonstrează că identitatea hibridă este cel mai probabil cea mai potrivită pentru un sistem model deschis. În plus, această cercetare propune și câteva proprietăți care sunt necesare dezvoltării categoriei de identitate digitală selectată.

Table of contents