

Streszczenie rozprawy doktorskiej

mgr inż. Michał Drozdowicz
pod opieką dr. hab. Marcina Paprzyckiego

Temat pracy

Semantyczne wspomaganie kontroli dostępu do danych i usług w Internecie rzeczy.
Semantic technologies for support of access control to data and services in the Internet of Things.

Motywacja

W ostatnich latach można zaobserwować prawdziwą eksplozję w obszarze Internetu rzeczy (ang. Internet of Things, IoT). W tym kontekście kluczowe staje się zapewnienie należytej kontroli nad dostępem do powstających w Internecie rzeczy zbiorów informacji, a także do usług realizowanych przez setki (nieługo tysiące, a w niedalekiej perspektywie dziesiątki tysięcy) połączonych urządzeń.

Rozmiar, różnorodność i dynamika środowisk IoT sprawiają, że niezbędne są nowe podejścia do definicji polityk dostępu. W obszarach takich jak e-zdrowie, logistyka, inteligentne sieci energetyczne (ang. Smart Grid), czy też społeczne współdzielenie danych (ang. Crowd Sensing) szczególnie widać wzrost znaczenia technologii Internetu rzeczy, przy jednoczesnej konieczności zapewnienia wysokiego stopnia bezpieczeństwa i prywatności.

Zakres i cel pracy

W tym kontekście, sformułowana została następująca teza badawcza:

Połączenie modelu Attribute Based Access Control i technik wnioskowania semantycznego stanowi efektywną metodę zarządzania dostępem do zasobów w sieciach sensorów i w Internecie rzeczy.

Szczegółowe cele badawcze, prowadzące do realizacji głównego celu badawczego to:

1. Opracowanie wielowarstwowej architektury ontologicznej, pozwalającej na maksymalne wykorzystanie istniejących ontologii do celów kontroli dostępu.
2. Opracowanie metody reprezentacji wiedzy o podmiotach i zasobach przy użyciu ontologii, oraz sposobów mapowania ontologii na atrybuty ABAC, a także zaprojektowanie wymaganych ontologii i wykazanie możliwości zastosowania stworzonego systemu w zakresie dostępu do zasobów w obszarach: e-zdrowia, logistyki, Smart Grid, a także zarządzania prywatnością w Smart City.
3. Opracowanie i implementacja semantycznego systemu kontroli dostępu do zasobów, który w sposób naturalny (i „nieinwazyjny”) rozszerza standardową architekturę języka XACML.

4. Opracowanie i implementacja metod wspomaganie (nie posiadającego wiedzy semantycznej) użytkownika w definicji i zarządzaniu (semantycznymi) regułami kontroli dostępu.

Realizacja głównego celu badawczego

W ramach pracy przygotowana została implementacja systemu łączącego technologie semantyczne z modelem Attribute Based Access Control (ABAC) do kontroli dostępu w dynamicznych środowiskach takich jak Internet rzeczy.

System obejmuje strukturę ontologii, wzbogacającą reguły dostępu ABAC o możliwość modelowania powiązań między danymi, oraz silnik zarządzania dostępem do danych i usług, oparty o połączenie języka XACML i technologii semantycznych, w tym języka OWL i wnioskowania semantycznego.

Rozwiązanie zaprezentowane jest w kontekście czterech scenariuszy użycia, powiązanych z Internetem rzeczy i/lub sieciami sensorów: kontroli dostępu do portu, administracją dostępu do elementów elektronicznej dokumentacji medycznej, zarządzaniem prywatnością danych zbieranych przez osobiste sensory, a także kontrolą dostępu do urządzeń połączonych ze Smart Grid. Przeprowadzono także analizę dostępnych ontologii dziedzinowych dla tych obszarów, której efektem jest powstanie kompletnych ontologii łączących aspekty domenowe i polityki XACML.

W ramach przeprowadzonych badań powstało także narzędzie pozwalające na zarządzanie ontologiczną stroną systemu bez konieczności posiadania wiedzy dotyczącej projektowania ontologii i technologii semantycznych. Narzędzie to wspiera użytkownika w definiowaniu klas i instancji oraz "prowadzi użytkownika za rękę", nie wymagając znajomości wszystkich elementów stosowanej ontologii.

Zarówno silnik kontroli dostępu, semantyczny interfejs użytkownika, jak i zestaw ontologii dostępne są publicznie w serwisie Github w repozytoriach: SXACML, OntoPlay i Ontologies.