Uwierzytelnienie i autoryzacja urządzeń Internetu rzeczy w środowisku federacyjnym z wykorzystaniem technologii rejestrów rozproszonych

mgr inż. Michał Jarosz

Streszczenie

Realizacja procesu uwierzytelniania i autoryzacji urządzeń Internetu rzeczy jest szczególnie trudna w środowiskach federacyjnych, w których nie ma lub jest ograniczone zaufanie pomiędzy organizacjami. Jednym z podstawowych warunków funkcjonowania federacji jest integracja informacyjna organizacji, która umożliwia wymianę informacji oraz korzystanie z zasobów, należących do poszczególnych podmiotów tworzących federację. Kluczowym wyzwaniem podczas wdrażania i wykorzystywania środowiska federacyjnego jest zapewnienie bezpieczeństwa wymiany informacji pomiędzy różnymi podmiotami. Natomiast same operacje uwierzytelniania i autoryzacji w takim środowisku muszą być realizowane według wspólnie określonych reguł. Reguły te nie mogą być zmienione bez wiedzy i braku akceptacji któregokolwiek uczestnika federacji. Jeżeli procesy uwierzytelniania i autoryzacji dotyczą środowiska Internetu rzeczy, w których to liczba urządzeń jest ogromna, to procesy te muszą być realizowane w sposób wydajny, skalowalny oraz bez udziału operatora. Problemy uwierzytelnienia i autoryzacji urządzeń IoT działających w środowiskach federacyjnych są nielicznie poruszane w literaturze. A same rozwiązania prezentowane w znalezionych pracach badawczych nie mogą być uznane za w pełni satysfakcjonujące.

W pracy zaproponowano rozwiązanie bazujące na wykorzystaniu rejestru rozproszonego, który umożliwia ustalenie wspólnych reguł wymiany informacji pomiędzy organizacjami tworzącymi rejestr. Poprzez wykorzystanie kodów łańcuchowych możliwa jest automatyzacja procesu uwierzytelniania i autoryzacji przy jednoczesnym przestrzeganiu ustalonych zasad. Zaproponowane rozwiązanie cechuje się także wykorzystaniem kryptografii symetrycznej, co jest unikalne w porównaniu do znalezionych w literaturze propozycji uwierzytelniania urządzeń w środowiskach federacyjnych. W pracy przedstawiono wyniki oceny bezpieczeństwa, wydajności i skalowalności zaproponowanego rozwiązania. Ocena bezpieczeństwa obejmuje analizę jakościową, a także formalną z wykorzystaniem odpowiednich narzędzi. Badanie wydajności obejmuje różne konfiguracje opracowanego rozwiązania. W niniejszej pracy przedstawiono także model sieci Petriego, który umożliwia przeprowadzenie symulacji badań wydajności rejestru rozproszonego dla różnych jego konfiguracji.

Uzyskane wyniki potwierdzają skuteczność zaproponowanego rozwiązania.