Legionowo, 24. 10. 2024

dr hab. inż. Andrzej Paszkiewicz

Dowództwo Wojsk Obrony Cyberprzestrzeni

ul. gen. Buka 1

05-119 Legionowo

Dobry doktorat jest niczym gwóźdź, który przebija ścianę gmachu nauki. Nie niszczy konstrukcji ale pozwala zajrzeć i zobaczyć co jest na zewnątrz gmachu, za ścianą.

RECENZJA ROZPRAWY DOKTORSKIEJ

DLA RADY DYSCYPLINY NAUKOWEJ

INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

WOJSKOWEJ AKADEMII TECHNICZNEJ

Tytuł rozprawy: **Uwierzytelnianie i autoryzacja urządzeń Internetu Rzeczy w środowisku federacyjnym z wykorzystaniem technologii rejestrów rozproszonych**

Autor rozprawy: mgr. inż. Michał Jarosz

Promotor: dr hab. inż. Zbigniew Zieliński

Promotor pomocniczy: dr inż. Konrad Wrona

Rozprawa dotyczy wykorzystania technologii rejestrów rozproszonych (ang. *Distributed Ledger Technology*) do uwierzytelniania i autoryzacji, rozumianej jako nadawanie (kontrola) uprawnień dostępu do zasobów rozproszonych baz danych. Technologię rozproszonych rejestrów wykorzystują niektóre rodzaje kryptowalut m.in. do rejestrowania zaszyfrowanych danych. Autor zaproponował wykorzystanie technologii rejestrów rozproszonych w odniesieniu do urządzeń wspomagających działanie Internetu Rzeczy (IoT), funkcjonującego w środowisku federacyjnym. Środowisko takie może skupiać różnorodne instytucje i firmy, często rozproszone geograficznie i kierujące się własną, wewnętrzną polityką dostępu do danych i ich wykorzystania. System dostępu do danych musi w związku z tym zapewnić współdzielenie danych i ich filtrację.

1. Cele badawcze w kontekście tezy rozprawy

Na podstawie rozległego studium literaturowego i własnych rozważań autora została sformułowana następująca teza rozprawy:

Umiejętne wykorzystanie unikatowych parametrów urządzeń IoT wraz z zastosowaniem technologii rejestrów rozproszonych zapewnia efektywne i bezpieczne uwierzytelnianie i autoryzację urządzeń IoT a także umożliwia bezpieczną komunikację urządzeń IoT w środowisku federacyjnym.

Aby potwierdzić słuszność postawionej tezy wyodrębniono następujące cele szczegółowe:

i. Opracowanie protokołu umożliwiającego uwierzytelnianie i autoryzację urządzeń IoT w środowisku federacyjnym z wykorzystaniem rejestru rozproszonego. Protokół powinien dostarczać mechanizmu ustalania kluczy kryptograficznych dla komunikujących się urządzeń IoT.
ii. Opracowanie prototypowego rozwiązania z wykorzystaniem platformy Hyperledger Fabric.
iii. Ocena skalowalności i wydajności opracowanego rozwiązania w środowisku rzeczywistym.
iv. Jakościowa oraz formalna ocena bezpieczeństwa opracowanego protokołu z wykorzystaniem odpowiednio dobranych narzędzi weryfikacji protokołu.
v. Modelowanie i ocena wydajności protokołu z wykorzystaniem hierarchicznych kolorowych sieci Petriego oraz wykorzystanie wyników badań w środowisku rzeczywistym do skalibrowania modelu oceny wydajności wykorzystującego model sieci Petriego.

2. Charakter rozprawy

Rozprawa ma charakter badawczo-teoretyczno-praktyczny z głównym naciskiem położonym na aspekt praktyczny. Autor w warunkach bardzo ograniczonych zasobów informatycznych, jakie posiadają urządzenia IoT opracował praktyczny protokół ustalania kluczy kryptograficznych oraz metodę uwierzytelniania i autoryzacji tych urządzeń w środowisku federacyjnym, nie korzystając przy tym z „dobrodziejstw" kryptografii asymetrycznej. Na bazie platformy Hyperledger Fabric opracował prototyp rozwiązania. Część teoretyczną rozprawy stanowi modelowanie i ocena wydajności protokołu z wykorzystaniem sieci Petriego.

3. Analiza źródeł literaturowych i sposób i sposób sformułowania wniosków wynikających ze studiów literaturowych

Recenzowana praca obejmuje 204 pozycje literatury. Są to głównie artykuły z renomowanych, wysoko punktowanych czasopism naukowych, które ukazały się na przestrzeni ostatnich 5-10 lat. Duża część cytowanych prac to artykuły z ważnych międzynarodowych konferencji naukowych dotyczących problematyki poruszanej w dysertacji. Wśród tych pozycji znajdują się dwie prace, w których autor rozprawy jest współautorem. Stanowią one merytoryczne wprowadzenie w tematykę realizowanej pracy doktorskiej i określają raczej *state of the art* w zakresie podjętej tematyki, jako że podjęty problem jest oryginalny. Praca zatem nie jest sklejanką wyników uzyskanych przez innych autorów ale samodzielnym rozwiązaniem istotnego problemu technicznego. Wśród źródeł znajduje się również adres repozytorium dający dostęp do szczegółowych wyników uzyskanych przez autora. Sposób i umiejscowienie cytowań w tekście pracy nie budzi zastrzeżeń co do kompetencji autora.

4. Sposób rozwiązania wynikających z tezy istotnych szczegółowych problemów

Zasadniczą sprawą dla dalszych kroków związanych z realizacją zadań szczegółowych jest wybór typu prywatnego rejestru z węzłami uprawnionymi. Na podstawie analizy właściwości kilku typów

dostępnych rejestrów, autor wybrał Hyperledger Fabric do przygotowania wersji PoC (Proof of Concept) protokołu uwierzytelniania i autoryzacji urządzeń IoT. Przy takim wyborze wymagane jest uwierzytelnienie wszystkich członków sieci tzn. użytkowników i węzłów i w przypadku ew. weryfikacji transakcji posiadanie stosownych uprawnień. Dzięki temu, że rejestry Hyperledger Fabric umożliwiają wykorzystanie kodów łańcuchowych, możliwe jest tworzenie własnych reguł dodawania danych i odczytywania danych w rejestrze rozproszonym. Do „pisania" kodu łańcuchowego dla rejestru rozproszonego wykorzystano język Golang, dzięki czemu uzyskano przewidywalność implementacji protokołu uwierzytelniania. Warto dalej zauważyć za autorem, że wykonanie dowolnej operacji na rejestrze rozproszonym możliwe jest wyłącznie poprzez kod łańcuchowy.

5. Poprawność wykonanej analizy, zaufanie do uzyskanych wyników

W pracy autor posiłkuje się głównie analizą jakościową. Posługuje się jednak sprawdzonymi i uznanymi narzędziami informatyczno-inżynierskimi. Uzyskane wyniki dokumentuje z wykorzystaniem licznych tabel, wykresów i zestawień. Ponadto zamieszcza zarówno w tekście pracy jak też w repozytoriach kody źródłowe implementacji, które, choć nie bez trudu, można zweryfikować. Zatem w żaden sposób ten typ podejścia do realizacji zagadnień zawartych w dysertacji nie umniejsza jej wartości.

6. Poprawność redakcyjna, zwięzłość językowa, jasność i umiejętność argumentacji

Praca jest napisana w sposób bardzo klarowny, jasny i poprawny pod względem inżynierskim. Autor unika żargonu. Nie znalazłem również w pracy niezręczności czy uchybień językowych, co oznacza, że została ona starannie i krytycznie zredagowana. Struktura (układ pracy), zawarty w spisie rozdziałów i podrozdziałów jest logiczny i występuje we właściwej kolejności. Tam, gdzie to jest potrzebne np. w definicjach pojęć pochodzących z języka angielskiego autor umieszcza nazwę pojęcia w dwóch językach – po polsku i po angielsku. Nie stosuje jałowych cytowań z literatury, nie mających związku z tematem pracy, mających zwiększać jedynie jej objętość. Przy niezwykle rozbudowanej literaturze bibliograficznej, autorowi udało się w pracy uniknąć niepotrzebnej redundancji. Sposób przeprowadzania wywodów i ich logika są w pełni przekonujące.

7. Słabe strony pracy i jej ewentualne wady

Generalnie nie znalazłem zbyt wielu mankamentów w recenzowanej pracy. Jak wcześniej wspomniałem pewien niedosyt, przynajmniej w moim przypadku, pozostawia niewielki udział w pracy aparatu matematycznego, który mógłby posłużyć np. do zbadania zjawisk wielkoskalowych związanych z tematyką pracy, jak zachowuje się sieć gdy środowisko federacyjne w sensie liczby urządzeń staje się asymptotycznie bardzo wielka. Rozumiem, że w pewnej mierze wyniki uzyskane doświadczalnie dla niedużej liczby urządzeń IoT można ekstrapolować ale już raczej trudno przewidzieć bez udziału aparatu matematycznego w jakim momencie nastąpi efekt „przemiany fazowej".

Nie mogę również zgodzić się, z tym, że do oceny losowości ciągu znaków wystarczy jedynie znajomość wartości entropii (patrz rozdz. 3). Autor zdaje się być świadomy tego faktu ale niefortunnie (str. 54 pkt. 3) pisze „Ciąg znaków posiadający entropię..." a powinien raczej napisać „Ciąg posiadający dużą entropię..." bądź „Ciąg posiadający maksymalną entropię...". Wydaje mi się także, że do jedynego wzoru matematycznego, zawartego w pracy (str. 85) autor mógł użyć edytora równań lub przynajmniej wykasować symbol „*" (gwiazdka) jako symbol mnożenia. Podobnie parę linii niżej na tej samej stronie ta sama uwaga dotyczy wartości współczynnika Newtona wyrażającego liczbę podzbiorów dwuelementowych zbioru M elementowego. Również na tej samej stronie autor używa

niepoprawnego sformułowania „L – długość wartości parametru". W innym miejscu nazwisko wielkiego niemieckiego uczonego Karla Friedricha Gaussa zostało napisane (str. 45) przez jedno s.

Na szczęście wymienione uwagi krytyczne nie mają wymiaru dyskredytującego tę pracę i raczej należy je uznać jako niezamierzone, drobne potknięcia językowe i drobne niedoróbki.

8. Przydatność wyników uzyskanych w badaniach wykonanych pod kątem rozprawy w naukach technicznych, w przemyśle i obronności

Praca posiada charakter techniczny i jak najbardziej jej wyniki mogą być implementowane w obszarze telekomunikacji. W tym przypadku niemal bez potrzeby dokonywania wielkich modyfikacji. Podobnie jak w przypadku technologii wykorzystywanych w niektórych rodzajach kryptowalut, tak też w przypadku zastosowań urządzeń IoT w środowisku federacyjnym firm biznesowych i korporacji pomysł jest „do kupienia". Sądzę jednak, że do wrażliwych zastosowań w armii czy instytucjach związanych z bezpieczeństwem państwa, pomysł należałoby wzbogacić o dodatkowe mechanizmy kryptograficzne. Nie wątpię jednak, że warto nad tą sprawą popracować.

9. Skrócony raport recenzenta, podsumowanie

Kryterium oceny	Punktacja	Wynik
Poprawność rozwiązania postawionego problemu, poprawność wniosków wyciągniętych z przeprowadzonych badań. Wykorzystanie nowoczesnych narzędzi wspomagających projektowanie i ocenę zaproponowanego rozwiązania	0-60 pkt.	60 pkt.
Trudność postawionego do rozwiązania problemu w sensie naukowym (technicznym)	0-20 pkt	17 pkt.
Adekwatność cytowanej literatury, jej aktualność i właściwe umiejscowienie w tekście pracy	0-10 pkt.	10 pkt.
Jakość języka, jego komunikatywność, jasność i zrozumiałość wywodów, błędy językowe	0-10 pkt.	8 pkt
Suma punktów		95 pkt.

Podsumowując, praca spełnia wymagania przewidziane dla rozpraw doktorskich w aktualnie obowiązującej ustawie i składam wniosek o przyjęcie jej jako rozprawy doktorskiej i dopuszczenie jej autora do publicznej obrony.

Andrzej Pasiekiewicz