Prof. dr hab. inż. Jordi Mongay Batalla
Politechnika Warszawska
Jordi.mongay.batalla@pw.edu.pl

Warszawa, 12 lipca 2024r.

Opinia recenzenta

na temat rozprawy doktorskiej autorstwa

Michała Jarosza

zatytułowanej:

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

1. Problem i jego wpływ

Przedstawiona przez doktoranta Michała Jarosza rozprawa liczy 197 stron i jest w całości napisana w języku polskim, z wyjątkiem abstraktu przetłumaczonego na język angielski.

Tematem rozprawy doktorskiej jest uwierzytelnianie i autoryzacja urządzeń IoT (Internet Rzeczy, ang. Internet of Things) w środowiskach federacyjnych, a rozwiązanie zaproponowane przez kandydata wykorzystuje technologię rozproszonych rejestrów (ang. Distributed Ledger Technology, DLT). Zaletą DLT dla zadań uwierzytelniania i autoryzacji jest to, że węzły mogą być heterogeniczne (tj. mogą to być różne węzły fizyczne lub zwirtualizowane), co zwiększa odporność na ataki i odporność całego systemu. Odporność jest zwiększona, ponieważ atak na jeden węzeł oparty na dowolnej znanej lub nieznanej podatności (atak zero-day lub one-day) nie oznacza, że inne węzły są również podatne na ataki. Wykorzystanie DLT do uwierzytelniania, zadań autoryzacyjnych i kilku innych zadań w środowiskach federacyjnych lub rozproszonych nie jest niczym nowym; należy jednak wziąć pod uwagę jego nowość w momencie, gdy kandydat rozpoczął swoje badania, czyli cztery lub pięć lat temu. W tamtym czasie naukowcy zaczęli proponować DLT do wielu innych zastosowań poza kryptowalutami. W tym kontekście musimy umiejscowić obecną pracę. Kandydat cytuje osiem publikacji (tj. [35, 115, 164, 184, 192, 196, 200, 202]), które wykorzystują DLT do uwierzytelniania i autoryzacji oraz innych zadań w środowiskach federacyjnych. Co ciekawe, najstarsza z tych publikacji ma zaledwie cztery lata (rok 2020). Potwierdza to, że pomysł jest stosunkowo nowy, a pracę wykonaną przez mgr Jarosza możemy uznać za innowacyjną.

Wyzwania związane z uwierzytelnianiem i autoryzacją urządzeń pojawiają się w sieciach IoT kontrolowanych przez jedną organizację, ale stają się jeszcze bardziej krytyczne, gdy wiele organizacji musi współpracować ze swoimi sieciami IoT. W takich przypadkach konieczne jest ustanowienie bezpiecznego, federacyjnego środowiska IoT, w którym podmioty mogą mieć ograniczone relacje zaufania i korzystać z zasobów już posiadanych przez poszczególne organizacje. Wykorzystanie tych istniejących zasobów wymaga rozwiązania kwestii interoperacyjności w zakresie wymiany danych, ponieważ każda domena może mieć inne zasady udostępniania i ochrony zasobów. Urządzenia mogą przesyłać dane bezpośrednio do systemu lub korzystać z węzłów brzegowych (bram, ang. gateways) w celu pośredniczenia w komunikacji, w tym zapewnienia bezpieczeństwa transferu danych, jeśli wydajność urządzenia jest niewystarczająca. Ustanowienie zaufania, zwłaszcza w sfederowanym

środowisku IoT obejmującym wiele domen organizacyjnych, jest kluczowym zagadnieniem badawczym. Zaufanie jest bardziej złożone w takich środowiskach, ponieważ oprócz zaufania do urządzeń znajdujących się pod naszą kontrolą, musimy również brać pod uwagę urządzenia innych organizacji i osób. Aby zbudować zaufanie w środowisku federacyjnym, potrzebny jest skuteczny mechanizm uwierzytelniania i autoryzacji urządzeń, z rejestracją urządzeń przeprowadzaną przez upoważnione strony.
W rejestrze rozproszonym dane są rejestrowane jako transakcje przesyłane przez użytkowników organizacyjnych. Proces dodawania transakcji do rejestru może się różnić w zależności od implementacji rejestru rozproszonego. Zasadniczo węzeł tworzy blok zawierający transakcje i wysyła go do innych węzłów w celu weryfikacji. Dodanie bloku do rejestru wymaga weryfikacji wszystkich transakcji w ramach bloku. Po weryfikacji przeprowadzane jest głosowanie konsensusowe w celu dodania bloku do rejestru. Jeśli węzły osiągną konsensus, blok jest dodawany do rozproszonego rejestru na każdym węźle.
Autor podsumował problem stawiając jedną tezę, która brzmi: "Umiejętne wykorzystanie unikatowych parametrów urządzeń IoT wraz z zastosowaniem technologii rejestrów rozproszonych zapewnia efektywne i bezpieczne uwierzytelnianie i autoryzację urządzeń IoT, a także umożliwiającą bezpieczną komunikację urządzeń IoT w środowisku federacyjnym". Doktorant z powodzeniem zademonstrował powyższą tezę podczas swoich prac badawczo-rozwojowych.
Problem postawiony przez doktoranta jest ważny dla sieci z dwóch głównych powodów: z jednej strony, urządzenia IoT są uważane za ograniczone pod względem zasobów, co oznacza, że mogą wykorzystywać niewiele zasobów do swoich zadań, w tym zadań bezpieczeństwa, które zwykle są dość wymagające pod względem zasobów. Dlatego konieczne jest znalezienie nowych rozwiązań dla zadań bezpieczeństwa, takich jak uwierzytelnianie i autoryzacja. Z drugiej strony, technologie takie jak DLT mogą wnieść wartość dodaną do zarządzania siecią, a obszar ten jest wciąż daleki od właściwego wykorzystania.
Ogólnie rzecz biorąc, pomysł jest zarówno praktyczny, jak i łatwy do wdrożenia. Oznacza to, że możliwość praktycznego wdrożenia i komercyjnego wykorzystania proponowanego systemu jest wysoka.
Główny wkład autora polega na wdrożeniu systemu. Autor zakodował dużą część systemu, co stanowi duży wkład w praktyczne badania. Praca doktorska ma jednak pewne wady, opisane w następnych sekcjach.

2. Wkład

Rozprawa jest wyraźnie praktyczną pracą z silnym komponentem wdrożeniowym i nieco słabszym wkładem badawczym.

Główny wkład wniesiony przez doktoranta ma następującą strukturę:

- Rozdział pierwszy służy jako wprowadzenie do rozprawy, przedstawiając motywację, tezę i cele pracy;
- Rozdział drugi zagłębia się w podstawowe zagadnienia problemu badawczego. Rozpoczyna się od omówienia koncepcji federacji i wyzwań napotykanych w sfederowanym środowisku Internetu rzeczy, w tym metod uwierzytelniania i autoryzacji stosowanych w takich ustawieniach. W rozdziale tym wyjaśniono również, czym jest rozproszona księga rachunkowa i opisano różne jej rodzaje, ze szczególnym uwzględnieniem struktury blockchain. W oparciu o przedstawione klasyfikacje, rozdział identyfikuje najbardziej odpowiedni typ rozproszonego rejestru do budowy systemu uwierzytelniania i autoryzacji w

środowisku federacyjnym. Dodatkowo, porównano kilka implementacji rozproszonego rejestru, przedstawiając uzasadnienie wyboru odpowiedniego dla systemu uwierzytelniania i autoryzacji urządzeń IoT w środowisku federacyjnym. W dalszej części omówiono metody zarządzania tożsamością w środowiskach IoT i sklasyfikowano urządzenia IoT, opisując możliwości każdej klasy. Rozdział kończy się analizą obwodów PUF (ang. Physically Unclonable Functions) i ich zastosowaniem w uwierzytelnianiu urządzeń IoT;

- Rozdział trzeci przedstawia opracowany protokół, Lightweight Authentication and Authorization Framework for Federated IoT (LAAFFI). Podkreślono w nim charakterystyczne cechy tego rozwiązania w porównaniu do innych protokołów. Rozdział rozpoczyna się od nakreślenia ogólnych zasad protokołu, po czym następuje szczegółowy opis jego działania i schematów komunikacji. Wyjaśniono również proces autoryzacji urządzeń IoT w ramach protokołu LAAFFI. Rozdział kończy się uwagami dotyczącymi implementacji Proof of Concept (ang. "Proof of Concept", PoC) protokołu;
- Rozdział czwarty zawiera ocenę bezpieczeństwa opracowanego protokołu. Rozpoczyna się od analizy entropii wybranych parametrów używanych w algorytmach kryptograficznych i określa minimalną odległość Hamminga dla tych parametrów. Następnie opisano potencjalne ataki na protokół i przeanalizowano ich skuteczność;
- Rozdział piąty przedstawia wyniki testów wydajności opracowanego protokołu dla urządzeń IoT wykorzystujących różne protokoły kryptograficzne. W pierwszej kolejności zidentyfikowano najbardziej wydajną konfigurację protokołu CoAP. Następnie oceniono wydajność opracowanego protokołu w odniesieniu do rozproszonego rejestru, a także skalowalność rejestru. Kluczowym wymogiem było zapewnienie minimalnego narzutu transferu danych między urządzeniami IoT a bramą aplikacji, co skłoniło do przeprowadzenia badania porównawczego protokołu LAAFFI z innymi podobnymi rozwiązaniami. W rozdziale opisano również model sieci Petriego, który pomaga określić wydajność w różnych konfiguracjach rozproszonego rejestru z różną liczbą przychodzących transakcji;
- Rozdział szósty kończy rozprawę.

Wkład wniesiony przez mgr. inż. Michała Jarosza wykracza poza aktualny stan wiedzy. Najbardziej wyróżniającym się wkładem jest implementacja całego systemu uwierzytelniania i autoryzacji dla urządzeń IoT w oparciu o rozproszone rejestry. Autor opracował niektóre części systemu od podstaw i przeprowadził testy end-to-end, aby zademonstrować poprawność rozwiązania. Zadania wdrożeniowe zostały wykonane przy użyciu hyperledger fabric, który jest globalnym ekosystemem open-source dla technologii blockchain klasy korporacyjnej. Konkretnie, projekt hyperledger fabric wywodzi się z Linux® Foundation i stał się nieoficjalnym standardem dla platform blockchain klasy korporacyjnej. Warto wspomnieć, że wiele biznesowych rozwiązań alla-blockchain jest obecnie opartych na hyperledger. Ponadto Europejska Infrastruktura Usług Blockchain (ang. European Blockchain Services Infrastructure, EBSI) jest prawie w pełni zaimplementowana przy użyciu hyperledger fabric (EBSI ma na celu wykorzystanie mocy blockchain dla dobra publicznego i jest inicjatywą Komisji Europejskiej i European Blockchain Partnership).

Interesującą częścią rozprawy jest analiza literatury. Analiza ta jest szeroka, również ze względu na fakt, że Internet Rzeczy i jego problemy z bezpieczeństwem wypełniły tysiące stron prac badawczych. Analiza stanu techniki jest, niestety, znacznie mniej obszerna dla części oceny bezpieczeństwa (rozdział 4) i części oceny wydajności (rozdział 5).

Czwarty i piąty rozdział poświęcone są badaniom. Można znaleźć kilka wad w tych rozdziałach.

W rozdziale 4 autor twierdzi, że bezpieczeństwo systemu zależy od niektórych parametrów (losowość i entropia, niektóre wybrane zagrożenia). Nie przeprowadzono jednak rzeczywistej oceny bezpieczeństwa, a czytelnik może mieć wątpliwości, czy proponowana analiza zawiera wszystkie

zagrożenia zaproponowanego systemu. W literaturze istnieje kilka metod oceny bezpieczeństwa protokołów i mechanizmów; wiele metod jest opisanych w międzynarodowych standardach. Wydaje się, że autor zignorował je i postanowił przeanalizować tylko wybrane parametry.
W podrozdziale 4.1 autor analizuje losowość kluczy używanych do szyfrowania. Odbywa się to dla trzech rozważanych scenariuszy szyfrowania, tj. silnika PUF, programowego generatora liczb losowych i generatora opartego na unikalnych parametrach urządzenia IoT. W tym podrozdziale można zauważyć pewną niekompletność badań: proponowana analiza omawia kilka otwartych kwestii, które nie zostały rozwiązane przez autora. Na przykład autor słusznie twierdzi, że pomiar entropii nie wystarcza do potwierdzenia losowości kluczy; jednak nie analizuje niczego więcej niż entropii. Innym przykładem jest analiza programowego generatora liczb losowych: autor rzetelnie wyjaśnia ograniczenia urządzeń IoT w korzystaniu z programowego generowania (liczb losowych); jednak nie modeluje, nie oblicza ani nie mierzy entropii ani pseudolosowości kluczy, więc nie wiemy, jak niedokładne są te mechanizmy.
W podrozdziale 4.2 autor proponuje kilka potencjalnych ataków i analizuje ich wpływ na LAAFFI. Wybór ataków opiera się na lekturze pięciu artykułów: [79, 134, 157, 159, 177], ale autor nie wyjaśnia powodów wyboru tych ataków. Wydaje się, że nie przyjęto jasnej metodologii i wydaje się, że przyszłe powtórzenie oceny może z łatwością dostarczyć nową listę ataków, wpływając na powtarzalność wyników.
Podrozdział 4.3 dotyczy analizy bezpieczeństwa protokołu. Tutaj analiza jest konceptualna i znacznie jaśniejsza. Autor zapewnia systematyczną dyskusję i dochodzi do jasnych i niepodważalnych wniosków.
Rozdział 5 dotyczy wydajności systemu LAAFFI. Autor bada protokoły telekomunikacyjne, działanie urządzeń IoT oraz działanie infrastruktury hyperledger. Warto podkreślić wysiłek doktoranta włożony w analizę całego systemu. Doceniam to, nawet jeśli widzę, że niektórym analizom (np. analizie protokołu CoAP) brakuje dogłębnego zrozumienia mechanizmów telekomunikacyjnych, a to mogłoby uprościć analizę (np. teoretyczny wpływ protokołu transportowego TCP/UDP/SCTP na przeciążenie ruchu sieciowego jest pomijany w tekście dysertacji). Autor dołożył jednak starań, aby pokazać, że rozwiązanie działa w środowisku IoT. Najbardziej wyróżniającą się częścią jest analiza zastosowanego DLT. Analiza oparta na modelowaniu sieci Petriego jest przekonująca, a wnioski są bardzo interesujące.

Główne mocne strony rozprawy są moim zdaniem następujące:
- Wdrożenie systemu;
- Analiza infrastruktury blockchain dla rozproszonych rejestrów;
- Wysiłki poświęcone analizie całego systemu.

Główne braki w rozprawie są moim zdaniem następujące:
- Nie ma modelowania matematycznego ani głębszej analizy wpływu mechanizmów, z wyjątkiem modelu sieci Petriego;
- Wątpliwa metodologia badań w wielu częściach pracy;
- Rozprawa opiera się tylko na jednym artykule badawczym, najprawdopodobniej z powodu braku jasnej metodologii badań.

Uważam, że pozytywne aspekty wyraźnie przewyższają wady tej rozprawy. Ogólnie rzecz biorąc, praca wykonana przez doktoranta jest krokiem naprzód w wykorzystaniu technologii rozproszonego rejestru do uwierzytelniania i autoryzacji urządzeń, zwłaszcza w środowisku IoT.

3. Poprawność

Wdrożenie systemu jest prawidłowe. System działa i spełnia postawione wymagania. Wdrożenie przebiega zgodnie z odpowiednią metodologią, a wyniki spełniają oczekiwania.
W przypadku części badawczej trudno jest stwierdzić, czy wyniki są poprawne, ponieważ autor nie podaje wystarczających informacji w rozprawie. Jednocześnie autor nie dostarcza wystarczających informacji, aby umożliwić powtarzalność wyników.
Jako przykład tego, tabela 4.2 przedstawia wyniki entropii niektórych wybranych instrukcji. Autor używa narzędzia *ent* do obliczania entropii. Niestety, autor nie wyjaśnia dokładnie, w jaki sposób narzędzie to oblicza entropię, w związku z czym wyniki są dość enigmatyczne. Ponadto autor nie wyjaśnia, które parametry różnych urządzeń wykorzystywanych w testach mają wpływ na entropię i w jaki sposób. Dlatego też powtórzenie testów poza laboratorium kandydata wydaje się bardzo trudne.
To samo dzieje się w tabeli 4.3. Wartość odległości Hamminga jest obliczana dla wybranych parametrów urządzenia IoT. Autor podaje nawet wzór na obliczenie wartości przedstawionych w tabeli. Nie jest jednak jasne, w jaki sposób kilka parametrów wzoru jest obliczanych dla konkretnego przykładu urządzenia IoT. W związku z tym wyniki tabeli 4.3 nie są możliwe do sprawdzenia przez innych badaczy.
Mój wniosek jest taki, że trudno jest zrozumieć, czy wyniki są wolne od wad. Jednocześnie nie mam żadnego powodu, by sądzić, że zawierają one błędy, ponieważ wydają się całkiem rozsądne.

Rozprawa posiada wysoką wartość koncepcyjną, a Doktorant włożył wysiłek w zrozumienie i ocenę pełnego funkcjonowania systemu. Po zapoznaniu się z rozprawą jestem przekonany, że Autor osiągnął cele szczegółowe postawione na początku rozprawy, tj:

1. 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;
2. Opracowanie prototypowego rozwiązania z wykorzystaniem Hyperledger Fabric;
3. Ocena skalowalności i wydajności opracowanego rozwiązania w środowisku rzeczywistym;
4. Jakościowa, jak i formalna ocena bezpieczeństwa opracowanego protokołu z wykorzystaniem odpowiednio wybranych narzędzi weryfikacji protokołu;
5. Modelowanie i ocena wydajności protokołu z wykorzystaniem hierarchicznych kolorowych sieci Petriego. Po wykonaniu badań w środowisku rzeczywistym wykorzystać wyniki do skalibrowania modelu oceny wydajności wykorzystującego model sieci Petriego.

4. Znajomość kandydata

Opis treści rozdziałów rozprawy doktorskiej znajduje się w części 2 niniejszej opinii. W rozprawie doktorskiej doktorant wykazał się zaawansowaną znajomością materii swoich badań w dyscyplinie *Informatyki Technicznej i Telekomunikacji.*
Rozprawa zawiera 204 referencji. Wszystkie są cytowane w tekście rozprawy i dostępne w Internecie. Doktorant wskazał, kiedy uzyskał dostęp do stron internetowych cytowanych w referencjach. 204 odniesienia są niezbędne do zaoferowania kompletnych ram dla obszernego tematu, jakim są sieci IoT i problem uwierzytelniania. Liczba referencji jest wysoka jak na rozprawę doktorską, co pokazuje, że autor włożył wiele wysiłku w analizę aktualnego stanu wiedzy i dobre umiejscowienie własnych pomysłów w ramach podobnych badań.

Praca doktorska opiera się głównie na jednej publikacji:

- Jarosz Michał, Wrona Konrad, Zieliński Zbigniew Ekspedyt, W: Proceedings of the 17th Conference on Computer Science and Intelligence Systems. 4-7 września 2022. Sofia,

Bulgaria / Ganzha Maria [i in.] (red.), Annals of Computer Science and Information Systems, 2022, vol. 30, Warszawa, Polskie Towarzystwo Informatyczne (PTI) , s.617-625, ISBN 978-83-965897-1-2. DOI:10.15439/2022F169

Doktorant jest pierwszym autorem i przedstawił główne badania pracy doktorskiej we wspomnianej publikacji.

W tekście rozprawy autor nie podał listy swoich publikacji i wydaje się, że praca została opublikowana tylko w tej publikacji. Jednak szybkie wyszukiwanie w Internecie pokazuje, że niektóre wcześniejsze koncepcje pracy kandydata zostały przedstawione w:

- K. Kanciak, M. Jarosz, P. Głębocki i K. Wrona, "Enabling civil-military information sharing in federated smart environments," 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2021, pp. 897-902, doi: 10.1109/WF-IoT51360.2021.9595715.

Kolejnym artykułem doktoranta związanym z tematyką Distributed Ledger Technology jest następujący artykuł (referencja ta została zacytowana w rozprawie doktorskiej). Artykuł ten został opublikowany w IEEE Communications Magazine, który jest jednym z najpopularniejszych czasopism w dziedzinie telekomunikacji:

- K. Wrona, F. M. Scharf i M. Jarosz, "Security Accreditation and Software Approval with Smart Contracts," w IEEE Communications Magazine, vol. 59, nr 2, s. 56-62, luty 2021, doi: 10.1109/MCOM.001.2000802

Inne starsze artykuły autora są również w jakiś sposób związane z tematem rozprawy. Dwa z nich dotyczą DLT, a jeden uwierzytelniania w IoT. Te trzy artykuły to:

- K. Wrona i M. Jarosz, "Does NATO Need a Blockchain?", MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 2018, pp. 667-672, doi: 10.1109/MILCOM.2018.8599845
- K. Wrona i M. Jarosz, "Use of blockchains for secure binding of metadata in military applications of IoT," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 213-218, doi: 10.1109/WF-IoT.2019.8767315
- Michał Jarosz, "Metody uwierzytelniania urządzeń w sieciach Internetu Rzeczy", Przegląd Teleinformatyczny 2019; 7(25) (3-4): 15-30, doi: 10.5604/01.3001.0013.6595

Warto wspomnieć, że doktorant jest jedynym autorem ostatniej publikacji. Ta ostatnia publikacja jest przeglądem metod uwierzytelniania w IoT i posłużyła do analizy literatury w tekście rozprawy.

Indeks H (Hirscha) kandydata nie jest dostępny w Google Scholar i Web of Science, przynajmniej ja nie mogłem go znaleźć. W gscholar można policzyć cytowania wspomnianych prac z sumaryczną liczbą ~45.

Uważam, że kandydat ma solidną wiedzę na temat nowych technologii, takich jak DLT, i doskonale zna problematykę uwierzytelniania w telekomunikacji.

5. Wnioski

Biorąc pod uwagę to, co przedstawiłem powyżej oraz wymogi nałożone przez art. 13 *Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki* (ze zmianami)[1] , moja ocena rozprawy według trzech podstawowych kryteriów jest następująca:

[1] http://www.nauka.gov.pl/g2/oryginal/2013_05/b26ba540a5785d48bee41aec63403b2c.pdf

- Rozprawa doktorska przedstawia oryginalne rozwiązanie problemu naukowego. Problem naukowy dotyczy sposobu zapewnienia ulepszonego uwierzytelniania i autoryzacji w środowisku IoT (ograniczonych urządzeń);
- Po przeczytaniu rozprawy uważam, że kandydat posiada ogólną wiedzę teoretyczną i zrozumienie dyscypliny **Informatyki Technicznej i Telekomunikacji**, a w szczególności obszaru **technologii rozproszonego rejestru dla zadań bezpieczeństwa**;
- Rozprawa doktorska potwierdza twierdzenie, że kandydat jest w stanie prowadzić pracę naukową.

Jordi Llongay Batalla

Podpis