Dr hab. inż. Adam Ziębiński prof. PŚ
Wydział Automatyki, Elektroniki i Informatyki
Katedra Systemów Rozproszonych i Urządzeń Informatyki
Politechnika Śląska
ul. Akademicka 16
44-100 Gliwice
email: adam.ziebinski@polsl.pl

Gliwice 28.06.2024

# Recenzja rozprawy doktorskiej

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

Autor rozprawy: **mgr inż. Michał Jarosz**

Promotor rozprawy: **dr hab. inż. Zbigniew Zieliński**

Promotor pomocniczy: **dr inż. Konrad Wrona**

Dziedzina: **nauki inżynieryjno-techniczne**

Dyscyplina: **informatyka techniczna i telekomunikacja**

## 1. Podstawa opracowania recenzji

Niniejsza recenzja została przygotowana w związku z Uchwałą 18/RDN ITiT/2024 Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego z dnia 14 maja 2024 r. w sprawie powołania komisji doktorskiej w celu przeprowadzenia postępowania w sprawie nadania stopnia doktora mgr. inż. Michałowi Jaroszowi w dziedzinie nauk inżynieryjno-technicznych, dyscyplinie informatyka techniczna i telekomunikacja.

Ocenę merytoryczną przeprowadzono na podstawie dostarczonej rozprawy doktorskiej i dokumentacji elektronicznej.

## 2. Cel, zakres, teza i charakter rozprawy

Jako osiągnięcie naukowe, kwalifikujące do uzyskania stopnia doktora nauk technicznych w dyscyplinie informatyka techniczna i telekomunikacja, doktorat przedstawił rozprawę doktorską pt. „Uwierzytelnianie i autoryzacja urządzeń Internetu Rzeczy w środowisku federacyjnym z wykorzystaniem technologii rejestrów rozproszonych".

Badania doktoranta obejmują swoim zakresem zastosowanie metod kryptograficznych, w szczególności dedykowanych rozwiązaniom IoT metod lekkich (Lightweight cryptography), technologii rejestrów rozproszonych oraz wybranych metod uwierzytelniania i autoryzacji, w celu zapewnienia urządzeniom uczestniczącym w środowisku federacyjnym wiarygodności, jednolitych zasad i metod niezbędnych do automatycznego zabezpieczenia transmitowanych danych.

Integracja informacyjna organizacji należących do poszczególnych podmiotów tworzących federację pozwala na wymianę informacji oraz wzajemne korzystanie z zasobów. W dzisiejszych czasach zapewnienie bezpieczeństwa wymiany informacji pomiędzy różnymi podmiotami jest konieczne, ze względu na coraz liczniejsze cyberataki na różnorodną infrastrukturę informatyczną. Problem zapewnienia bezpieczeństwa wymiany informacji jest najistotniejszy w przypadku infrastruktury krytycznej. Jednak coraz częściej pojawia się w przypadku infrastruktury przemysłowej, transportowej, publicznej, w tym typowo pomiarowej, która ogólnie uważana jest za nie wartą przeprowadzenia cyberataku. Niemniej tego typu ataki miały już miejsce i coraz częściej pojawiają się w przypadku wymiany informacji pomiędzy

urządzeniami IoT, autonomicznymi platformami jezdnymi i latającymi czy też pojazdami autonomicznymi i infrastrukturą publiczną, przemysłową i transportową.

Biorąc to pod uwagę niezbędny jest rozwój nowych metod uwierzytelniania i autoryzacji, w szczególności w środowisku federacyjnym pozwalającym na wymianę danych pomiędzy różnego typu infrastrukturą. Dotyczy to szczególnie Internetu rzeczy który coraz powszechniej jest stosowany zarówno w rozwiązaniach przemysłowych jak i publicznych. Przy czym często wymagane jest aby urządzenia IoT były: niewielkich rozmiarów, wykorzystywały do transmisji danych różnego typu interfejsy bezprzewodowe, zasilane bateryjnie, a przez to energooszczędne. W efekcie do ich konstrukcji stosuje się często systemy wbudowane wykorzystujące energooszczędne jednostki przetwarzające o małej mocy obliczeniowej, które w niewielkim stopniu zapewniają funkcjonalność bezpieczeństwa przesyłanych danych. W zaawansowanych rozwiązaniach stosowane są jednostki przetwarzające, które pozwalają na wykorzystanie wbudowanych funkcji szyfrowania danych za pomocą kryptografii asymetrycznej lub/i symetrycznej. W efekcie systemy IoT są wykonywane w rożnych technologiach i zapewniają funkcjonalność kryptograficzną na rożnym poziomie. Aby umożliwić wszystkim uczestnikom wymiany danych bezpieczny dostęp do środowiska federacyjnego, konieczne jest zwykle zastosowanie rozwiązań, które wykorzystują zasoby sprzętowe na niskim poziomie.Z tego powodu aktualnym problemem jest odpowiedni dobór metod kryptograficznych i protokołów, uwierzytelniania i autoryzacji w celu zapewnienia wszystkim urządzeniom uczestniczącym w środowisku federacyjnym wiarygodności, jednolitych zasad i metod niezbędnych do automatycznego zabezpieczenia transmitowanych danych.

Stwierdzam zatem, że tematyka badawcza poruszana w rozprawie doktorskiej ma duży potencjał dla rozwoju dyscypliny informatyka techniczna i telekomunikacja oraz wpisuje się w aktualne trendy związane z zwiększeniem wymagań bezpiecznej wymiany danych pomiędzy urządzeniami IoT i infrastrukturą, co jest spowodowane dużym natężeniem cyberataków na infrastrukturę publiczną i przemysłową. Ponadto problematyka badawcza podjęta w rozprawie wykazuje duże cechy oryginalności i innowacyjności, pozwalające na zapewnienie bezpiecznej wymiany danych pomiędzy różnej klasy urządzeniami IoT. Dodatkowo holistyczne podejście do problemu ma duży potencjał do zapewnienia bezpiecznej wymiany danych, pomiędzy różnego typu federacjami urządzeń, co jest szczególnie istotne podczas sytuacji kryzysowych.

## 3. Teza rozprawy

Autor rozprawy doktorskiej stawia tezę naukową „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". Postawiona hipoteza badawcza dotyczy aspektu związanego z zapewnieniem bezpiecznej wymiany danych pomiędzy różnej klasy urządzeniami IoT oraz federacjami urządzeń. Hipoteza badawcza została przedstawiona w sposób jasny.

W pracy doktorskiej Autor zaproponował rozwiązanie wykorzystujące rejestr rozproszony, w celu ustalenia wspólnych reguł wymiany informacji pomiędzy podmiotami tworzącymi federację. Automatyzację procesu uwierzytelniania i autoryzacji umożliwia wykorzystanie kodów łańcuchowych, które zapewnia jednocześnie przestrzeganie ustalonych zasad. Do uwierzytelniania urządzeń w środowiskach federacyjnych Autor wykorzystał metody z zakresu kryptografii symetrycznej, wykorzystując do generowania kluczy dostępne informacje o urządzeniu IoT.

W celu weryfikacji oraz sprawdzenia poprawności postawionej tezy badawczej Autor postawił sobie za cel opracowanie prototypowego rozwiązania protokołu umożliwiającego uwierzytelnianie i autoryzację urządzeń IoT w środowisku federacyjnym z wykorzystaniem rejestru rozproszonego, ocenę skalowalności i wydajności opracowanego rozwiązania oraz formalną ocenę bezpieczeństwa opracowanego protokołu.

Badania prowadzone przez Doktoranta w dużej mierze mają charakter badań stosowanych z ukierunkowaniem na wypracowanie koncepcji systemu uwierzytelniania i autoryzacji urządzeń IoT w środowisku federacyjnym.

Stwierdzam, że spełnione są warunki poprawności hipotezy badawczej. Hipoteza badawcza jak i cel rozprawy są sformułowane w sposób jednoznaczny oraz umożliwiający ich weryfikację za pomocą mierzalnych wskaźników. W kontekście aktualnych trendów rozwojowych obowiązujących w branży IoT, przedstawiona teza i cel są ważnym elementem zapewnienia bezpiecznej wymiany danych pomiędzy urządzeniami IoT i infrastrukturą.

## 4. Zawartość rozprawy

Zasadnicza część rozprawy składa się z 7 rozdziałów. Na początku pracy autor przedstawił streszczenie pracy oraz spis rysunków, tabel i akronimów, które ułatwiają zaznajomienie się pracą.

Pierwszy rozdział stanowi wstęp, w którym Autor zawarł genezę, motywację, analizę literatury poruszanej tematyki, tezę i cele rozprawy.

Rozdział 2 zawiera przegląd technologii i zagadnień związanych z problematyką rozprawy w tym wprowadzenie do środowisk federacyjnych w szczególności w zastosowaniach IoT. Autor przedstawił podtypy rejestrów rozproszonych oraz budowę łańcucha bloków. Dodatkowo wykonał porównanie wybranych implementacji rejestru rozproszonego, co pozwoliło mu wskazać wybrane rozwiązanie niezbędne do zrealizowania systemu uwierzytelniania i autoryzacji urządzeń IoT w środowisku federacyjnym. Ponadto Autor przedstawił metody zarządzania tożsamościami w środowiskach IoT oraz uwierzytelniania urządzeń IoT.

Rozdział 3 zawiera opracowany przez Autora protokół uwierzytelniania, autoryzacji i bezpiecznej komunikacji urządzeń IoT w środowiskach federacyjnych (LAAFFI). W tym założenia, architekturę, protokół uwierzytelniania urządzeń, metodę wykonywania operacji na rejestrze rozproszonym oraz sposób autoryzacji urządzeń IoT w protokole.

Rozdział 4 zawiera ocenę bezpieczeństwa opracowanego protokołu, w tym analizę możliwości przeprowadzenia ataków w środowisku federacyjnym IoT oraz formalną weryfikację modeli bezpieczeństwa protokołu.

Rozdział 5 przedstawia wyniki badań wydajnościowych opracowanego protokołu z wykorzystaniem urządzeń Raspberry Pi i rejestru rozproszonego. Badania nadmiaru przesyłanych danych oraz modelowanie wydajności podstawowych operacji z wykorzystaniem czasowych kolorowanych sieci Petriego.

Przedostani rozdział zawiera podsumowanie pracy oraz kierunki dalszych badań. Natomiast ostatni rozdział zawiera parametry urządzeń wykorzystywanych w badaniach wydajności.

Pracę kończy bibliografia na którą składają się 204 pozycje, a cytowane w tekście rozprawy pozycje oraz analiza ich zawartości potwierdzają znajomość stanu wiedzy doktoranta.

Kolejność rozdziałów rozprawy doktorskiej jest poprawna i odzwierciedla właściwą metodologię prowadzenia badań naukowych. Praca zawiera poprawnie sformułowane założenia metodologiczne, w tym właściwy opis stosowanych technik i metod oraz wykorzystywanych narzędzi badawczych. Autor po sformułowaniu hipotezy badawczej przedstawił schemat postepowania pozwalający na weryfikację postawionej tezy badawczej przez przedstawienie opracowanego protokołu uwierzytelniania, autoryzacji i bezpiecznej komunikacji urządzeń IoT w środowiskach federacyjnych, ocenę bezpieczeństwa opracowanego protokołu oraz szereg eksperymentów, które służyły do wykonania badań wydajnościowych opracowanego protokołu (w tym nadmiaru przesyłanych danych) oraz modelowania wydajności podstawowych operacji z wykorzystaniem czasowych kolorowanych sieci Petriego.

## 5. Ocena rozprawy

Rozprawa doktorska dotyczy aktualnych zagadnień związanych zabezpieczeniem wymiany danych pomiędzy urządzeniami IoT i federacjami tych urządzeń.

Na wstępie Autor przeprowadził szerokie badania literaturowe podejmowanego problemu badawczego w zakresie aspektów naukowych związanych z dyscypliną Informatyka Techniczna i Telekomunikacja. Opracowany protokół LAAFFI zbudowany jest z bramy aplikacyjnej i rejestru rozproszonego. Zastosowanie takiego rozwiązania wpływa na rozdzielnie funkcjonalności protokołu. Dodatkowo wykorzystanie bramy aplikacyjnej pozwala na równoważenie obciążenia pomiędzy węzłami rejestru rozproszonego oraz nawiązywanie i weryfikację połączeń. Autor wykorzystał protokół CoAP i metodę Concise Binary Object Representation (CBOR) zapisu danych, opracowane do implementacji dla urządzeń z ograniczonymi zasobami. Natomiast operacje uwierzytelniania i autoryzacji wykonywane są w węźle rejestru rozproszonego. Ponadto Autor wybrał implementację rejestru rozproszonego typu Hyperledger Fabric wymagającą TLS, która została zaimplementowana w powszechnie wykorzystywanym w tym przypadku języku Golang. W procesie uwierzytelniania wykorzystywana jest infrastruktura klucza publicznego Membership Service Provider (MSP). Autor zaproponował wykorzystanie unikatowych parametrów urządzenia IoT do generacji 128 bitowego klucza dla potrzeb szyfrowania algorytmami symetrycznymi. Zbiór wybranych parametrów dla danego urządzenia jest zapisywany w tablicy parametrów bazujących na danych sprzętowych jak i programowo-konfiguracyjnych. Ponadto autor uwzględnił parametry, które ze względu bezpieczeństwa nie powinny być wykorzystywane do generacji klucza. Parametry urządzenia IoT są zapisywane w rejestrze rozproszonym w postaci wyniku funkcji skrótu Hash-based Message Authentication Code. Wykorzystanie metody HMAC jest wystarczające do nawiązania szyfrowanego połączenia. Aby zapewnić integralności danych Autor wykorzystał algorytm uwierzytelnionego szyfrowania z powiązanymi danymi - Authenticated Encryption with Associated Data. Dodatkowo w wymianie danych uwzględnił znacznik czasu, który zabezpiecza przed przetwarzaniem powtórzonych lub przeterminowanych danych. Zaletą proponowanego rozwiązania jest generowanie osobnych kluczy do komunikacji pomiędzy poszczególnym urządzeniami IoT. W efekcie każdy kanał transmisyjny jest szyfrowany innym kluczem, co wpływa na zwiększenie bezpieczeństwa przesyłania danych w danej federacji urządzeń. Proces autoryzacji uczestników wymiany danych jest realizowany przez kod łańcuchowy, na bazie weryfikacji ustanowionych uprawnień metodą ACL wykorzystującą listę kontroli dostępu. W efekcie przyjęty proces autoryzacji gwarantuje, że reguły autoryzacji są identyczne dla wszystkich organizacji. Dodatkowym atutem wykorzystania rejestru rozproszonego, może być wprowadzenie funkcjonalności nadawana uprawnień do wykonania operacji oraz możliwość wykorzystania różnych protokołów kryptograficznych.

W kolejnym etapie przedstawione rozwiązanie zostało szeroko zbadane i przeanalizowane przez Autora. Autor przedyskutował w pracy oszacowanie entropii: na bazie literatury dla układów PUF, losowo wygenerowanego zestawu parametrów dla urządzeń IoT, oraz zestawu dobranych unikatowych danych konfiguracyjnych urządzenia. Dodatkowo oszacował entropię dla wybranych parametrów, niezbędnych do tworzenia klucza. Pozwoliły one na uzyskanie 274 bity entropii wejściowej, co było wystarczające do utworzenia klucza o entropii 128 bitów. Oszacowana przez Autora średnia odległość Hamminga pozwoliła na wskazanie parametrów sprzętowo-programowych urządzeń IoT, które są najodpowiedniejsze do identyfikacji urządzeń i generowania kluczy kryptograficznych. Ponadto Autor wykonał w pracy analizę możliwości przeprowadzenia ataków w środowisku federacyjnym IoT w 3 warstwach: percepcji, sieciowej i aplikacyjnej. W wyniku tej analizy wskazał na problem związany z atakami powtórzeniowymi których wystąpienie jest zależne od poprawnej synchronizacji czasu oraz wymiany danych pomiędzy węzłami o otrzymanych wiadomościach. Dodatkowo Autor przeprowadził formalną weryfikację modeli bezpieczeństwa protokołu, w celu potwierdzenia spełnienia cech bezpieczeństwa informacji przez opracowywany protokół. Weryfikacji poddano następujące operacje: rejestrację urządzenia IoT, komunikację urządzenia IoT z węzłem rejestru rozproszonego oraz komunikację pomiędzy urządzeniami

IoT. Autor wykazał, że wyszególnione podczas weryfikacji ataki są niemożliwe do zrealizowania przy poprawnej implementacji protokołu.

W ostatnim etapie autor przeprowadził badania wydajności opracowanego protokołu dla urządzeń IoT, z uwzględnienie wskaźników: opóźnienia, przepustowości i stopnia wykorzystania zasobów sieciowych. W wyniku przeprowadzonych badań autor wykazał, że wykorzystanie CoAP bazującego na TCP i nawiązywaniu jednej sesji dla całego procesu wymiany informacji jest najlepszym rozwiązaniem. W wyniku badań wydajność stosowanych protokołów kryptograficznych autor wykazał, że dla różnych algorytmów HMAC oraz AEAD nie widać większej różnicy. Różnice są dopiero zauważalne przy zastosowaniu innych długości stosowanego klucza. Wyniki badań rejestru rozproszonego wykazały, że wydajność rejestru można w prosty sposób zwiększać poprzez zwiększenie zasobów sprzętowych węzłów oraz liczby węzłów rejestru. Natomiast wydajność rejestru rozproszonego maleje, w przypadku zwiększania liczby organizacji wymaganych do zatwierdzenia bloku. Ponadto opracowany protokół charakteryzuje mniejszy nadmiar przesyłanych bajtów niż protokół TLS lub DTLS. Do przeprowadzenia symulacji dodawania danych do rejestru rozproszonego autor wykorzystał czasowe kolorowane sieci Petriego. W wyniku przeprowadzonych badań autor wykazał, że różnica między wynikami symulacyjnymi a eksperymentalnymi wynosi kilka procent, więc zaprojektowane narzędzie do przeprowadzenia symulacji działa poprawnie.

Na podstawie analizy rozprawy doktorskiej mgr. inż. Michała Jarosza, do osiągnięć Kandydata można zaliczyć opracowanie protokołu LAAFFI z wykorzystaniem umiejętnej kombinacji znanych metod: generowania parametrów, HMAC, AEAD oraz wykonywania operacji na rejestrze rozproszonym, które umożliwiły bezpieczną wymianę danych pomiędzy urządzeniami IoT, poprzez zapewnienie funkcjonalności generowania kluczy, szyfrowania algorytmami symetrycznymi, integralności danych, uwierzytelniania i autoryzacji.

Należy podkreślić, że przedstawiony problem badawczy jest kluczowy dla rozwoju i zapewnienia bezpiecznej komunikacji pomiędzy urządzeniami IoT i federacjami urządzeń. Zgodnie z założeniami Autora opracowany protokół LAAFFI jest przystosowany do obsługi mało wydajnych urządzeń IoT. Wykorzystuje kryptografię symetryczną do uwierzytelniania oraz zabezpieczenia komunikacji. Ponadto wykorzystuje protokoły komunikacji uznawane za lekkie, czyli w niewielkim stopniu obciążające jednostkę centralną. W rezultacie opracowany przez Autora protokół jest odpowiedni do uwierzytelniania i autoryzacji urządzeń IoT w środowisku federacyjnym. Ponadto możliwe jest jego wykorzystanie do bezpiecznej wymiany informacji pomiędzy różnego typu infrastrukturą informatyczną w tym: publiczną, cywilną, przemysłową a nawet jak autor wskazał wojskową.

Przedstawione rozwiązanie zostało szeroko zbadane i przeanalizowane przez Autora poprzez przeprowadzenie oceny bezpieczeństwa opracowanego protokołu oraz wykonanie eksperymentalnych badań wydajnościowych z wykorzystaniem urządzeń Raspberry Pi i rejestru rozproszonego. Kandydat pokazał też ich praktyczne wykorzystanie, podczas testów eksperymentalnych. Biorąc to pod uwagę, przedstawione przez Kandydata osiągnięcie naukowe oceniam pozytywnie, uważam je za wartościowe i wnoszące oryginalny wkład w rozwój dyscypliny informatyka techniczna i telekomunikacja.

## 6. Ocena dorobku publikacyjnego

Kandydat opublikował wyniki swoich badań w postaci 5 artykułów w materiałach konferencyjnych i jednego artykułu w czasopiśmie naukowym.

Należy podkreślić, że Kandydat brał udział w opracowaniu artykułu w czasopiśmie naukowym IEEE Communications Magazine, którego wartość pkt MN wynosi 200 - „K. Wrona, F. M. Scharf and M. Jarosz, "Security Accreditation and Software Approval with Smart Contracts," in IEEE Communications Magazine, vol. 59, no. 2, pp. 56-62, February 2021, doi: 10.1109/MCOM.001.2000802". Kandydat jest pierwszym autorem w jednej publikacji konferencyjnej, w której przedstawił wyniki weryfikacji przeprowadzonych badań „M. Jarosz, K. Wrona and Z. Zieliński, "Formal verification of security properties of the Lightweight Authentication and Key Exchange Protocol for Federated IoT devices," *2022 17th Conference*

*on Computer Science and Intelligence Systems (FedCSIS)*, Sofia, Bulgaria, 2022, pp. 617-625, doi: 10.15439/2022F169".

Tematyka opracowanych publikacji przez Autora w większości mieści się w obszarze badawczym związanym z osiągnięciem naukowym Kandydata, obejmuje zagadnienia związane z:

- formalną weryfikacja właściwości bezpieczeństwa protokołu lekkiego uwierzytelniania i wymiany kluczy dla sfederowanych urządzeń IoT,
- bezpiecznego wdrażanie i zarządzanie kluczami w sfederowanych środowiskach IoT,
- wymiany informacji w sfederowanych inteligentnych środowiskach,
- wykorzystania łańcuchów bloków do bezpiecznego wiązania metadanych w zastosowaniach IoT.

Wartości wskaźników bibliometrycznych zidentyfikowano przeszukując bazy Web of Science i Scopus. Uzyskane wyniki naukometryczne oceniam bardzo dobrze:

- Sumaryczny Impact Factor wynosi 8.3.
- Liczba cytowań według bazy: Scopus 33, Web of Science 21.
- Indeks Hirscha według bazy: Scopus 4, Web of Science 2.

Można więc stwierdzić, że wyniki badań prowadzonych przez Kandydata są na dobrym poziomie i są zauważalne w międzynarodowym środowisku, co potwierdza rosnąca liczba cytowań publikacji. Biorąc to pod uwagę stwierdzam, że przedstawione osiągnięcie naukowe stanowi znaczny wkład w rozwój dyscypliny informatyka techniczna i telekomunikacja.

## 7. Analiza źródeł

Bibliografia recenzowanej rozprawy jest obszerna i obejmuje 204 pozycje, w tym 2, których współautorem jest Autor rozprawy. Pozycje zawarte w literaturze są związane z problemem omawianym w pracy i dobrze przedstawiają bieżący stan wiedzy. Pozycje literatury cytowane są w odpowiednim kontekście. Do pracy dołączono także dysk USB z treścią pracy oraz wynikami przeprowadzonych badań. Poruszona przez Autora problematyka rozprawy obejmuje wiedzę teoretyczną i praktyczną z obszaru informatyki technicznej i telekomunikacji.

## 8. Poprawność pracy

Tytuł rozprawy doktorskiej odzwierciedla zawartość pracy. Praca została napisana w języku polskim, starannie i zgodnie z piśmiennictwem stosowanym w literaturze. Forma drukowana recenzowanej rozprawy obejmuje 218 stron. Przyjęty układ pracy jest właściwy. Praca zawiera wystarczający materiał ilustracyjny, składający się z 41 rysunków i 31 tabel. Niewielka część rysunków jest za mała, przez co słabo czytelna 5.7, 5.9, 5.11-5.14. Forma rozprawy, rysunki i tabele są poprawne. Dostrzeżono jednak nieliczne błędy w formułowaniu zdań (np. „pozwala na dla ciągu wejściowego"), powtórzenia, brak spacji przed nawiasami czy cudzysłowem, literówki, brak wstępu w rozdziale 5.2. i 5.5. Drobne uchybienia edytorskie nie mają jednak wpływu na pozytywny odbiór pracy i nie utrudniają jej lektury.

## 9. Uwagi dyskusyjne i słabe strony rozprawy

Przedstawiony na początku pracy spis akronimów pozwala na usystematyzowanie zagadnień i dużo łatwiejsze zapoznanie z treścią pracy. Jednak ze względu na wykorzystywanie powszechnie w języku angielskim skrótów dotyczących wąskich dziedzin bezpieczeństwa, byłoby wskazane ich wyjaśnienie w języku polskim.

Opis klas znajduje się w tekście rozdziału 2.6 ale Tabela 2.5 byłaby czytelniejsza gdyby zawierała dodatkowo wiersz informujący o klasie urządzenia IoT.

Rozdział 3.1 dotyczy opisu założeń dotyczących konstrukcji protokołu LAAFFI, niestety z rozdziału nie wynika jasno jakiego typu założenia autor zdecydował się wykorzystać w omawianym protokole, np. jakie parametry generowania klucza zostaną wykorzystane w protokole.

W rozdziale 3.1 Autor napisał „w rejestrze rozproszonym muszą być przechowywane wszystkie parametry urządzeń IoT" wszystkie możliwe (wyszczególnione w 3.1) czy wybrane parametry?

W rozdziale 3.1 Autor napisał „Proces wysłania tablicy parametrów do rejestru następuje w fazie rejestracji urządzenia" jednak wcześniej nie opisano przyjętej metody wymiany tablicy parametrów i fazy rejestracji urządzenia – brak odwołania do rozdziału 3.3.1.

W rozdziale 3.2 na rys 3.2 i w tekście Autor pisze „W ramach tego systemu zaleca się wdrożenie systemu Security Information and Event Management (SIEM) do przechowywania, korelowania oraz analizy zdarzeń z węzłów rejestru rozproszonego. Wykorzystanie tego systemu umożliwi wykrywanie naruszeń bezpieczeństwa w ramach każdej organizacji.", potem wspomina o tym w rozdziale 4.3. Z tekstu wynika, że SIEM nie jest integralną częścią zaprojektowanego protokołu przez Autora, tylko opcją o którą może być poszerzony, co powinno być zaznaczone na rys 3.2.

Biorąc powyższe pod uwagę brakuje schematu ukazującego wymaganych w protokole metod/funkcjonalności, niezbędnych do jego działania i wykorzystywanych przez jego Autora. W rozdziale 3.1 lub 3.3 mógłby się pojawić schemat przepływu danych, który odzwierciedlałby ogólne działanie opracowanego przez Autora protokołu. Czytelnik musi polegać na schemacie komponentów składowych protokołu (rys 3.2), w którym nie zaznaczono modułów opcjonalnych.

Rysunek 5.15 i 5.16 nie zawiera jednostek.

Odwołanie do tematyki kolorowanych sieci Petriego na stronie 171, powinno dotyczyć rozdziału 5.

W podsumowaniu brak porównania opracowanego protokołu z innymi rozwiązaniami (PKI, Kerberos,..). Mogłoby by ono być zrealizowane w postaci tabeli na bazie funkcjonalności dostępnych protokołów z punktu ich zastosowania dla urządzeń IoT i federacji tych urządzeń. Dyskusja na ten temat została przeprowadzona w rozdziale 2. Jednocześnie wyniki wydajnościowe tego typu porównania Autor pokazał w rozdziale 5.4. Takie porównanie mogłoby jednak podkreślić potrzebę powstania opracowanego protokołu oraz wstępnych zaleceń dotyczących budowy systemów federacyjnych.

## 10. Wniosek końcowy

Przedstawione do recenzji osiągnięcie naukowe pt. „Uwierzytelnianie i autoryzacja urządzeń Internetu Rzeczy w środowisku federacyjnym z wykorzystaniem technologii rejestrów rozproszonych" w postaci rozprawy doktorskiej, stanowi oryginalny wkład w dyscyplinę informatyka techniczna i telekomunikacja.

Za oryginalne osiągnięcia, uznaję opracowanie protokołu LAAFFI przeznaczonego do ustanowienia bezpiecznej komunikacji urządzeń IoT w środowiskach federacyjnych, z wykorzystaniem kombinacji znanych metod: generowania parametrów, HMAC, AEAD oraz wykonywania operacji na rejestrze rozproszonym. W pracy Autor przedstawił wyniki oceny bezpieczeństwa, wydajności i skalowalności zaproponowanego rozwiązania, a uzyskane wyniki potwierdzają jego skuteczność.

Konkludując, stwierdzam, że przedstawione osiągnięcie naukowe mgr. inż. Michała Jarosza, stanowi osiągnięcie naukowe w rozumieniu art. 219 ust. 1 pkt. 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021 r. poz. 478 z późn. zm.).

Biorąc to pod uwagę, wnioskuję o kontynuację postępowania w sprawie nadania stopnia doktora mgr. inż. Michałowi Jaroszowi w dziedzinie nauk inżynieryjno-technicznych, dyscyplinie informatyka techniczna i telekomunikacja i popieram wniosek o dopuszczenie jej Autora mgr. inż. Michała Jarosza do publicznej obrony pracy.

dr hab. inż. Adam Ziębiński prof. PŚ

Adam Ziębiński