Prof. dr hab. Bogusław Pacek

Uniwersytet Jagielloński

Instytut Bliskiego i Dalekiego Wschodu

Warszawa, 31.05.2024 r.

Recenzja rozprawy doktorskiej

dla Rady dyscypliny Informatyka Techniczna i Telekomunikacja

Zachodniopomorskiego Uniwersytetu Technologicznego

Autor rozprawy doktorskiej: mgr inż. Kamil Kaczyński

Tytuł rozprawy doktorskiej: *„Zastosowanie zaawansowanych systemów blockchain do wzmacniania odporności systemów informatycznych”*

Promotor: prof. dr hab. n. mat. inż. Jerzy Gawinecki

Zakres i charakter rozprawy

Rozprawa mgra inż. Kamila Kaczyńskiego "*Zastosowanie zaawansowanych systemów blockchain do wzmacniania odporności systemów informatycznych*" ma charakter teoretyczno-praktyczny i analizuje możliwości zastosowania rejestrów rozproszonych oraz technologii zdecentralizowanego przechowywania danych do zapewnienia integralności, poufności i dostępności danych. Rozprawa skupia się na możliwościach decentralizacji systemów informatycznych, co jest szczególnie istotne w kontekście rosnących zagrożeń cybernetycznych oraz wymogów ochrony danych.

Poruszona przez autora tematyka decentralizacji systemów informatycznych stanowi istotny obszar badawczy. Zastosowanie technologii rejestru rozproszonego i zdecentralizowanego przechowywania danych jest aktywnie analizowane przez środowisko naukowe. Wykorzystane technologie takie jak IPFS, czy Hyperledger Fabric są szeroko wykorzystywane do tworzenia nowych i modernizacji istniejących systemów teleinformatycznych, w szczególności, gdy założone wymagania projektowe skupiają się na

zapewnieniu dostępności i integralności danych. Celowość stosowania tych technologii wskazuje stale rosnąca liczba incydentów cyberbezpieczeństwa nakierowanych na uzyskanie nieautoryzowanego dostępu do danych, a w szczególnych przypadkach na spowodowanie ich niedostępności dla dotychczasowych użytkowników.

Rozprawa oferuje nowe schematy zapewniania integralności, dostępności i poufności danych, które mogą być wykorzystane w różnych sektorach, w tym w infrastrukturze krytycznej i obronności. Dodatkowo praca wskazuje na potencjalne ścieżki dla dalszych badań, zwłaszcza w obszarze decentralizacji i ochrony danych wrażliwych.

Zawartość rozprawy

Rozprawa składa się z dziesięciu rozdziałów, streszczenia w języku polskim i angielskim oraz wykazu skrótów. Pierwszy rozdział to wprowadzenie przedstawiające tematykę rozprawy oraz wskazujący na motywy wyboru tematu przez doktoranta. Rozdział drugi przedstawia cele pracy oraz postawione przez autora hipotezy badawcze. W rozdziale trzecim zamieszczony został teoretyczny opis technologii blockchain pierwszej generacji. Autor wskazał historyczne początki tej technologii, najbardziej znaczącą implementację w postaci kryptowaluty Bitcoin. W rozdziale tym zawarty został opis najbardziej istotnych algorytmów konsensusu stosowanych w rejestrach rozproszonych. W rozdziale czwartym przedstawione zostały generacje rejestrów rozproszonych określone jako druga i trzecia. Autor skupił się w osobnych podrozdział na przedstawieniu specyfikacji technicznej Ethereum, IOTA oraz Hyperledger Fabric. Rozdział ten jest zakończony przedstawieniem specyfikacji technicznej usług zdecentralizowanego przechowywania danych IPFS oraz Arweave.

W rozdziale piątym przedstawione zostały praktyczne zastosowania analizowanych technologii w zapewnianiu integralności i dostępności danych a także realizacji obliczeń rozproszonych. Rozdział ten zawiera autorskie koncepcje dotyczące zastosowania rejestrów rozproszonych w oprogramowaniu zarządzania łańcuchem dostaw, zwiększaniu dostępności witryn internetowych i realizacji autonomicznych rojów dronów. W szóstym rozdziale recenzowanej rozprawy przedstawiony został autorski schemat uwierzytelnionego dostępu w środowisku rozproszonym. Autor przedstawia także ewaluacje utworzonego schematu, w szczególności w kontekście zapewnianych usług kryptograficznych. Rozdział siódmy podsumowuje pracę, określa spełnienie postawionych hipotez badawczych oraz przedstawia możliwości zastosowania wyników pracy. Ostatnie trzy rozdziały zawierają bibliografię oraz odpowiednio spisy tabel i rysunków.

Uważam, iż struktura rozprawy jest poprawa, a zastosowany przez doktoranta sposób przedstawienia zagadnień jest logiczny i przejrzysty. Praca jest wykonana w sposób staranny pod kątem poprawności edycyjnej i językowej.

Poprawność rozwiązania i oryginalność problemu naukowego

Doktorant sformułował następującą główną hipotezę badawczą: *„Zastosowanie technologii blockchain pozwala na realizację uwierzytelnionego dostępu do danych zdecentralizowanych.”*. Uważam, iż powyższa tez została sformułowania poprawnie, a mgr inż. Kamil Kaczyński rozwiązał ten problem naukowy z wykorzystaniem prawidłowych metod badawczych. Zamieszczona w podsumowaniu pracy weryfikacja hipotezy głównej przedstawia opracowany przez autora schemat i implementację uwierzytelnionego dostępu w środowisku rozproszonym wykorzystującym publiczne sieci blockchain Ethereum i Secret Network, usługę IPFS oraz autorską aplikację przeglądarkową jako uzasadnienie.

Rozprawa mgra inż. Kamila Kaczyńskiego jest zgodna z dyscypliną "Informatyka techniczna i telekomunikacja", skupiając się na kwestiach bezpieczeństwa, niezawodności i efektywności systemów informatycznych. Autor zastosował szereg technik badawczych, łącząc analizy teoretyczne z praktycznymi implementacjami w językach Rust, Solidity i Javascript. Praca wnosi istotny wkład do dziedziny Informatyki Technicznej i Telekomunikacji, proponując nowe schematy uwierzytelniania i przechowywania danych, które mogą być zastosowane w różnych sektorach, w tym w infrastrukturze krytycznej i obronności. Praca wskazuje także na potencjalne ścieżki dla dalszych badań, zwłaszcza w zakresie decentralizacji i ochrony danych wrażliwych.

W mojej ocenie mgr inż. Kamil Kaczyński rozwiązał postawiony problem naukowy w sposób poprawny, z zastosowaniem właściwego podejścia badawczego. Problem naukowy jest bez wątpienia oryginalny i ciekawy, co pozwala na dalsze zastosowanie osiągniętych przez autora wyników badań.

Ogólna wiedza teoretyczna kandydata w dyscyplinie

Doktorant zamieścił w pracy szeroki opis sieci blockchain pierwszej, drugiej i trzeciej generacji wzbogacony o podrozdziały dotyczące algorytmów konsensusu oraz usług zdecentralizowanego przechowywania danych. Bibliografia składa się ze 192 pozycji, w których zdecydowaną większość stanowią artykuły anglojęzyczne. W pracy znajdują się odniesienia do każdej pozycji literatury, pozwalające czytelnikowi na weryfikację zawartości rozprawy oraz uszczegółowienie opisywanej tematyki. Autor zamieścił w rozprawie szereg

przypisów i definicji ułatwiających zrozumienie zawartości przez czytelnika. Szczegółowa analiza bibliografii pozwala także na odnalezienie odniesienia do publikacji doktoranta traktujących o poruszonej w pracy tematyce. Dołączone do rozprawy ilustracje, schematy i tabele wskazują na posiadanie przez autora wiedzy na temat tworzenia publikacji naukowych i prezentacji wyników własnych badań. Po analizie powyższego, uważam, że doktorant posiada odpowiednią wiedzę teoretyczną w dyscyplinie Informatyka Techniczna i Telekomunikacja.

Uwagi krytyczne

Recenzując rozprawę zauważyłem, iż doktorant stosuje ilustracje pochodzące ze źródeł zewnętrznych, jak i ilustracje sporządzone własnoręcznie. Powyższe skutkuje powstaniem pewnego dysonansu w odbiorze pracy, gdzie nie wszystkie ilustracje zachowują podobną kolorystykę i przejrzystość. Dodatkowo, część z ilustracji zawiera opisy sporządzone w języku angielskim, podczas gdy inne są sporządzone w języku polskim. W mojej ocenie warto byłoby ujednolicić ilustracje w całej pracy, poprawiając tym samym jej czytelność.

Doktorant wykorzystuje w pracy wiele wzorów i odwzorowań matematycznych. Ich sposób formatowania nie budzi zastrzeżeń, jednakże brak numeracji powoduje, że analiza ciągu myślowego autora wymaga znacznie więcej wysiłku. Uważam, że warto byłoby wprowadzić odpowiednią numerację, tym samym poprawiając odbiór pracy przez czytelnika.

Autor zamieścił na początku pracy wykaz wykorzystywanych skrótów. Składa się on z 75 pozycji, które są w zdecydowanej większości skrótami rozwiniętymi z języka angielskiego. Praca została napisana w języku polskim, dlatego też niektóre z rozwinięć można byłoby zastąpić polskimi odpowiednikami, np. IoT – Internet of Things zastąpić poprzez IR – Internet Rzeczy.

Opracowany przez autora schemat uwierzytelnionego dostępu do danych w środowisku zdecentralizowanym został przedstawiony w postaci odwzorowań matematycznych i fragmentów kodu źródłowego implementującego najważniejsze funkcje systemu. Następnie autor dokonał ewaluacji, skupiając się na weryfikacji siły kryptograficznej składowych prymitywów kryptograficznych. W mojej ocenie dobrze byłoby dokonać także oceny wydajności takiego schematu, czy też oszacować koszty przechowywania i udostępniania danych z jego wykorzystaniem. Powyższe pozwoliłoby czytelnikowi na wyciągnięcie wniosków co do możliwości wykorzystania tych kodów w środowisku produkcyjnym.

Podsumowanie

Rozprawa mgra inż. Kamila Kaczyńskiego w sposób poprawny prezentuje ogólną wiedzę teoretyczną kandydata w dyscyplinie Informatyka Techniczna i Telekomunikacja oraz wskazuje na posiadanie przez doktoranta umiejętności samodzielnego prowadzenia pracy naukowej. Przedmiot rozprawy bezsprzecznie stanowi oryginalne rozwiązanie problemu naukowego, a autor we właściwy sposób wykazał umiejętność prowadzenia badań i właściwej interpretacji uzyskiwanych wyników. Wskazane przeze mnie uwagi krytyczne nie wpływają na pozytywną ocenę niniejszej rozprawy.

Konkludując, uważam że recenzowana rozprawa autorstwa mgra inż. Kamila Kaczyńskiego spełnia wymogi zawarte w ustawie z dnia 20 lipca 2018r., Prawo o szkolnictwie wyższym i nauce i wnoszę o dopuszczenie do jej publicznej obrony.