Warszawa, 20 września 2023r.

dr hab. Mirosław Kurkowski, prof. UKSW, prof. APwSz

- **Instytut Informatyki**
  Uniwersytet kard. St. Wyszyńskiego w Warszawie
- **Instytut Służby Kryminalnej**
  Akademia Policji w Szczytnie

Recenzja rozprawy doktorskiej mgr inż. Gerarda Wawrzyniaka
Wykorzystanie łańcuchów bloków zintegrowanych z formularzami elektronicznymi w realizacji bezpiecznych transakcji
Promotor: dr hab. inż. Imed El Fray, prof. ZUT

Niniejsza recenzja została sporządzona na prośbę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Zachodniopomorskiego Uniwersytetu Technologicznego wyrażonej w odpowiednim piśmie. Opiniowana rozprawa dotyczy wykorzystania technologii XML i blockchain do tworzenia bezpiecznych formularzy elektronicznych. Praca ma charakter projektowo/implementacyjny.

Zawartość rozprawy

Recenzowana rozprawa razem ze Spisem Treści, Bibliografią oraz Załącznikami liczy 222 strony. Układ rozprawy budzi zastrzeżenia. Na przykład traktowanie jako rozdział (Rozdział 8) samego sformułowania Celu rozprawy i hipotezy badawczej (mimo wprowadzenia ich już we Wstępie) jest moim zdaniem niewłaściwe. Zebrana na cele pisania rozprawy i zacytowana bogata literatura przedmiotu liczy 226 pozycji. Z dużym szacunkiem należy podkreślić jej rozmiar i zawartość.

We Wstępie autor określił Cel i hipotezę badawczą:

Celem pracy jest ***opracowanie modelu transakcji rozproszonych sterowanych formularzami elektronicznymi****, a sformułowana hipoteza badawcza to:* ***zastosowanie formularza elektronicznego z własną logiką umożliwi realizację transakcji rozproszonych w heterogenicznym środowisku bez używania infrastruktury serwerowej i udziału scentralizowanej architektury PKI****.*

Poza Wstępem (numerowanym jako Rozdział pierwszy) recenzowana rozprawa zawiera dwanaście rozdziałów właściwych, Słownik pojęć, Spis rysunków, tabel i wydruków, Spisu literatury oraz Załączników. Te ostatnie są bardzo rozbudowane. Zawierają one szczegółowo opisaną syntaktykę formularza elektronicznego zaproponowanego przez autora.

Kolejne rozdziały rozprawy od drugiego do siódmego przedstawiają szeroko wprowadzenie oraz przegląd stanu wiedzy w zakresie technik i metod transakcji elektronicznych oraz rozwiązań zapewniających bezpieczeństwo ich realizacji.

I tak w rozdziale drugim opisano historię (od starożytności) transakcji oraz metod zapewniania własności związanych z ich bezpieczeństwem, w tym wiarygodności. Rozdział trzeci przedstawia formalne specyfikacje transakcji i dotyczących ich wymagań. Zawarto tutaj także opis technik potrzebnych do przetwarzania informacji podczas zawierania transakcji. Dodatkowo przedstawiono tutaj próbę definicji formularzy elektronicznych jako pewnej określonej klasy dokumentów elektronicznych. W rozdziale czwartym opisano problemy związane z interoperacyjnością, w tym interoperacyjność procesów czy reguł.

W rozdziale piątym autor zaprezentował techniki stosowania podpisów elektronicznych w formacie XML wraz z analizą ich generowania i podatności na różnego rodzaju ataki. Rozdział szósty traktuje o technologii blockchain. Mgr Wawrzyniak prezentuje tutaj historię, zastosowania oraz zalety i wady tych rozwiązań. Jako przykład podano możliwość zastosowania blockchain do autoryzacji danych medycznych. W rozdziale siódmym autor dokonał podsumowania najistotniejszych elementów opisanych dotąd w rozprawie.

Proponowany przez autora rozdział ósmy składa się tylko z przedstawienia Celu i hipotezy badawczej zaprezentowanych wcześniej we Wstępie.

Podsumowując tę część rozprawy stwierdzam, że mgr Wawrzyniak przedstawił tutaj w sposób co najmniej wystarczający ogólną wiedzę teoretyczną dotyczącą badanego obszaru.

W następnych rozdziałach autor zamieszcza propozycje własnych rozwiązań.

I tak kolejno, w rozdziale dziewiątym zaproponowano formalną syntaktykę do zastosowania w opracowanym przez siebie formularzu elektronicznym w środowisku XML. Mgr Wawrzyniak uwzględnił tutaj interakcję formularza z człowiekiem oraz automatyczne przetwarzanie danych. Dodatkowo autor zawarł tutaj wiele przykładów z formularzy występujących w praktyce.

Rozdział dziesiąty prezentuje autorskie rozwiązania w zakresie metod zastosowania technologii blockchain w formularzach elektronicznych. W rozdziale jedenastym mgr Wawrzyniak omawia opracowane rozwiązania w zakresie realizacji transakcji przy użyciu

formularzy elektronicznych. Zaprezentowano także listę firm/instytucji, które zaadaptowały opisane metody do realizacji.

Ostatnie dwa rozdziały zawierają podsumowanie rozprawy. Najpierw mgr Wawrzyniak prezentuje zestawienie cech spełnianych przez opracowane rozwiązanie w stosunku do wymogów stawianych transakcjom elektronicznym. Kolejno przedstawiono perspektywy dalszych prac badawczych.

Podsumowując wyniki przedstawione w rozprawie należy stwierdzić, że moim zdaniem mgr Wawrzyniak w odpowiedni sposób zrealizował stawiany sobie Cel badawczy, a tym samym wykazał hipotezę badawczą.

Zaznaczyć jednak należy, że odczuwam pewien niedosyt w związku z brakiem próby bardziej formalnego uzasadnienia własności badanych przez autora rozprawy.

Uwagi polemiczne i krytyczne oraz elementy dyskusyjne

1. W moim odczuciu w wielu miejscach pracy autor zastosował skróty myślowe, czy niezbyt precyzyjne sformułowania. Uważam, że praca mogłaby być pod tym względem lepiej opracowana. Przykładem może być często wymieniana tzw. *logika* systemu. Tymczasem w nauce *logika*, to albo nauka o poprawnym rozumowaniu lub po prostu dany, określony precyzyjnie system wnioskowania.
2. Pierwsza część pracy, składająca się z sześciu rozdziałów (2 – 6), stanowi wprowadzenie do dalszych rozważań. Składają się na nią: prezentacja pierwszych historycznie transakcji, omówienie pojęcia transakcji z punku widzenia definicji, omówienie interoperacyjności jako istotnej właściwości transakcji, a także bezpieczeństwo współczesnych dokumentów z perspektywy podpisów elektronicznych oraz łańcuchów bloków jako potencjalnego źródła inspiracji do wspomagania realizacji transakcji. Całość zakończona jest podsumowaniem (Rozdział 7), które zawiera wnioski z wcześniejszych rozważań mające stanowić uzasadnienie przyjętego celu pracy oraz hipotez badawczych. Wydaje się, że ta część pracy mogłaby być krótsza i ograniczyć się do bardziej zwięzłego i bardziej precyzyjnego omówienia prezentowanej problematyki.
3. Ważnym przedmiotem rozważań rozprawy są formularze elektroniczne. Co prawda w rozdziale dziewiątym autor zaprezentował koncepcję oraz podstawy implementacji autorskiego rozwiązania formularzy elektronicznych, ale można byłoby wspomnieć o innych, o ile takie istnieją, rozwiązaniach formularzy elektronicznych, ze wskazaniem najważniejszych różnic pomiędzy nimi i rozwiązaniem zaprezentowanym przez autora.
4. Tytuł pracy *Wykorzystanie łańcuchów bloków zintegrowanych z formularzami elektronicznymi w realizacji bezpiecznych transakcji* nie do końca oddaje intencje wyrażone w celu badawczym sformułowanym jako „opracowanie modelu transakcji

rozproszonych sterowanych formularzami elektronicznymi” oraz hipotezie badawczej mówiącej, że „zastosowanie formularza elektronicznego z własną logiką umożliwi realizację transakcji rozproszonych w heterogenicznym środowisku bez użycia infrastruktury serwerowej i udziału scentralizowanej infrastruktury PKI”. Cel i hipoteza pracy nie zawierają informacji dotyczących wykorzystania łańcuchów bloków.

5. Konsekwencję powyższej uwagi można zauważyć w rozdziałach dziewiątym i jedenastym, w których zaprezentowano oraz omówiono koncepcję cech formularza umożliwiających realizację transakcji sterowanych logiką formularza, bez korzystania z aplikacji serwerowych, ale z zapewnieniem bezpieczeństwa, a także zaprezentowano przykład realizacji takiej transakcji. Natomiast w rozdziale dziesiątym autor ograniczył się do zaprezentowania i wykazania możliwości i mechanizmów jakie daje prezentowany formularz elektroniczny w zakresie integracji z łańcuchami bloków. Nie pokazano jednak przykładów transakcji, w których funkcje formularza są zintegrowane z funkcjami łańcuchów bloków.
6. Podobną uwagę można sformułować w zakresie braku konieczności korzystania ze scentralizowanej infrastruktury PKI w transakcjach realizowanych z użyciem formularzy elektronicznych będących przedmiotem pracy. Autor, w podrozdziale 6.5.3 zaprezentował, na podstawie studiów literaturowych, liczne rozwiązania implementujące funkcje i usługi systemów infrastruktury klucza publicznego opartych na łańcuchach bloków. Jednak w dalszej części pracy nie odniósł się do tej problematyki zakładając prawdopodobnie, że problem weryfikacji ważności certyfikatów klucza publicznego nie jest bezpośrednio związany z procesami realizacji transakcji i weryfikacji wiarygodności dokumentów wspomagających te transakcje, a przedstawienie w rozdziale dziesiątym skutecznych mechanizmów współpracy formularza z łańcuchem bloków jest w tej mierze wystarczające.

Uwagi redakcyjne

W pracy znalazłem kilkanaście błędów literowych lub stylistycznych, ale nie mają one znaczenia przy ocenie rozprawy jako całości.

Wniosek końcowy

Przedstawione w recenzowanej rozprawie doktorskiej rozważania i zaproponowane rozwiązania projektowo implementacyjne związane z wykorzystaniem technologii XML i blockchain do tworzenia bezpiecznych formularzy elektronicznych dotyczą ważnych i bieżących problemów informatyki. Rozprawa doktorska mgr inż. Gerarda Wawrzyniaka zawiera oryginalny wkład autora w teorię i praktykę komunikacji prowadzonej drogą elektroniczną.

Biorąc pod uwagę wyniki przedstawione w recenzowanej rozprawie doktorskiej mgr inż. Gerarda Wawrzyniaka stwierdzam, że moim zdaniem, praca ta spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą aktualnie w Polsce Ustawę o Stopniach i Tytule Naukowym. Stawiam zatem wniosek o dopuszczenie mgr inż. Gerarda Wawrzyniaka do dalszych etapów przewodu doktorskiego prowadzonego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie Informatyka techniczna i telekomunikacja przez odpowiednią Radę Dyscypliny Naukowej Zachodniopomorskiego Uniwersytetu Technologicznego.