Zygmunt Mazur, Hanna Mazur, Teresa Mendyk-Krajewska

Technologia zbliżeniowa a bezpieczeństwo danych

Ekonomiczne Problemy Usług nr 87, 535-544

2012

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 702 EKONOMICZNE PROBLEMY USŁUG NR 87 2012

ZYGMUNT MAZUR, HANNA MAZUR, TERESA MENDYK-KRAJEWSKA
Politechnika Wrocławska

TECHNOLOGIA ZBLIŻENIOWA A BEZPIECZEŃSTWO DANYCH

Wprowadzenie

Coraz więcej kart, zarówno płatniczych jak i identyfikacyjnych, wykorzystuje technologię RFID (*Radio-Frequency Identification*). Technologia ta, oparta na transmisji fal radiowych, umożliwia identyfikację obiektu z pewnej odległości. Jej zastosowanie jest obecnie bardzo duże z uwagi na niezawodność identyfikacji, wszechstronne możliwości wykorzystywania oraz wygodę i prostotę stosowania. Istnieją jednak obawy o dostateczne bezpieczeństwo gromadzonych danych i przeprowadzanych w tej technologii transakcji. Zagadnienia te są przedmiotem rozważań w niniejszej pracy.

1. Technologia RFID

Jedną z najpopularniejszych i bardzo prężnie rozwijających się technologii wykorzystywanych do automatycznej identyfikacji danych jest obecnie technologia RFID. Chociaż została opracowana już w 1948 roku, to zastosowano ją komercyjnie dopiero w latach 80. XX wieku. Pierwsze urządzenie RFID z 16-bitową pamięcią zaprezentowano w 1971 roku w Nowym Jorku. Dzięki technologii RFID, przypominającej kody kreskowe, ale wykorzystującej fale radiowe, dane zapisane w transponderze[1] (zwanym w tym przypadku również tagiem lub znacznikiem) mogą być udostępniane na odległość. W odróżnieniu jednak od kodu kreskowego

[1] Bezprzewodowe urządzenie komunikacyjne odbierające nadesłany sygnał oraz odpowiadające na niego w czasie rzeczywistym.

technologia ta jest znacznie wygodniejsza w użyciu, ponieważ tag nie musi być widoczny na zewnątrz podczas odczytu. Pierwsze urządzenia RFID wykorzystywały fale LF (o niskich częstotliwościach), obecnie częściej wykorzystuje się pasma HF, VHF, UHF i Microwave[2]. W tabeli 1 zamieszczono zestawienie częstotliwości wykorzystywanych w systemach RFID[3].

Tabela 1

Zestawienie częstotliwości wykorzystywanych w systemach RFID

Pasmo	Zasięg	Częstotliwości	Opis
LF	1 m	125 kHz 134,2 kHz	Do kontroli dostępu, w handlu, w kluczach samochodowych, do znakowania zwierząt
HF	1,5 m	13,56 MHz	Do kontroli tożsamości i identyfikacji przedmiotów, np. wejść do obiektów, obiegu dokumentów, bagażu na lotniskach, książek w bibliotece, tagi mają najczęściej postać etykiet, możliwy jednoczesny odczyt wielu tagów
VHF	3 m	30–300 MHz	W firmach przewozowych, ochroniarskich, transporcie miejskim
UHF	6 m	860–960 MHz	W logistyce, do identyfikacji obiektów w ruchu
Micro wave	Ponad 10 m	2,45 GHz 5,8 GHz	Do identyfikacji obiektów w ruchu, banknotów, w medycynie; wykorzystywane są najczęściej tagi aktywne

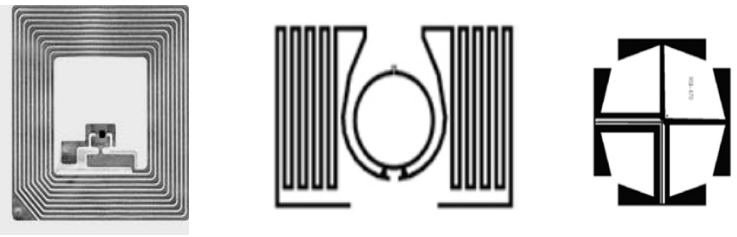
Źródło: opracowanie własne na podstawie: www.portalrfid.pl/wprowadzenie.php? it=6.

Od 23 listopada 2006 roku dyrektywa Komisji Europejskiej obliguje państwa Unii Europejskiej do przestrzegania dokumentu ETSI 302 208, określającego wymagania dla urządzeń do identyfikacji radiowej (RFID) pracujących w zakresie częstotliwości UHF.

Każdy transponder ma przypisany unikatowy numer seryjny, co zapewnia jego jednoznaczną identyfikację. Transpondery mogą mieć postać naklejki z kodem paskowym, można je umieścić wewnątrz opakowania towaru lub w obudowie umożliwiającej użycie na dowolnej powierzchni i w różnych warunkach czy też w postaci chipu wszczepić pod skórę (rysunek 1). Często mają postać karty plastikowej lub breloczka (rysunek 2).

[2] LF (*Low Frequency*) – niskie częstotliwości, HF (*High Frequency*) – wysokie częstotliwości, VHF (*Very High Frequency*) – bardzo wysokie częstotliwości, UHF (*Ultra High Frequency*) – ultra wysokie częstotliwości, Microwave – mikrofale.

[3] Portal RFID, www.portalrfid.pl/wprowadzenie.php?it=6.



Rys. 1. Przykładowe wyglądy transponderów RFID

Źródło:: http://phamthaiquy-rfid.blogspot.com/2009/04/week-1-introduction-to-rfid.html, http://upway.pl/tagi-rfid-inlay

Rys. 2. Przykłady urządzeń bezstykowych

Źródło: opracowanie własne.

Odczyt danych z transpondera możliwy jest dzięki czytnikom (skanerom, terminalom) o zróżnicowanej budowie i funkcjonalności. Również tagi różnią się między sobą wyglądem i budową, zawsze jednak posiadają mikrochip z pamięcią (o pojemności od kilkudziesięciu do kilku tysięcy bitów) i niewielkich rozmiarów antenę. W technologii RFID wykorzystywane są transpondery aktywne (wyposażone w baterie), pasywne (bez własnego źródła zasilania, na ogół o mniejszych rozmiarach i długim czasie użytkowania) lub półpasywne (z wewnętrznym zasilaniem, oczekujące na sygnał z zewnętrz) oraz urządzenia czytająco-programujące zawierające nadajnik i dekoder.

Tagi, ze względu na możliwość zapisu i odczytu danych, są oznaczane jako RO (*Read-Only*) – tylko do odczytu, WORM (*Write Once Read Many*) – jednokrotnego zapisu i wielokrotnego odczytu, lub RW (*Read Write*) – wielokrotnego odczytu i zapisu.

Etykiety RFID umożliwiają wykonywanie podstawowych operacji na danych (zapis/odczyt, dopisywanie, kasowanie). Znajdują zastosowanie na przykład jako naklejki samochodowe, do oznaczania towarów lub dokumentów. Drukarki RFID umożliwiają nie tylko drukowanie etykiet, ale także zapisywanie (dopisywanie) jawnych lub zaszyfrowanych danych i ich usuwanie.

Niezwykła popularność RFID wynika z możliwości korzystania z tagów w skrajnie niekorzystnych warunkach klimatycznych, na odległość, po ich ukryciu

czy zanieczyszczeniu. Ponadto w transponderach można zapisać znacznie więcej danych niż za pomocą kodów kreskowych. Terminale umożliwiają odczyt z wielu tagów (nawet kilku tysięcy) znajdujących się jednocześnie w polu odczytu. Urządzenia RFID są wykorzystywane na przykład do określania czasu pracy, identyfikacji przedmiotów, osób i zwierząt oraz obserwacji ich przemieszczania się, inwentaryzacji i kontroli przepływu towarów w czasie rzeczywistym, segregacji odpadów oraz do zabezpieczeń przed kradzieżą i fałszerstwem.

2. Rozwój technologii zbliżeniowej

Technologia RFID, umożliwiająca odczyt i/lub zapis danych z urządzeń będących w zasięgu odpowiedniego czytnika, jest stosowana w kartach bezstykowych (*proximity* lub *contactless card*) wykorzystywanych coraz częściej do regulowania płatności oraz identyfikacji. Parametry kart identyfikacyjnych (wymiary, trwałość, odporność na zginanie, temperaturę, wilgotność, światło i środki chemiczne) są zgodne z normą ISO/IEC 7810:2003, a inne parametry dla formatu ID-1 określane są przez dodatkowe normy: ISO/IEC 7811 (grubość, zaokrąglenie krawędzi), ISO/IEC 7813 (metody zapisu danych na karcie i na pasku magnetycznym) oraz ISO/IEC 7816 (dla kart z wbudowanym mikroprocesorem i punktami styku na przykład dla szeregowej transmisji danych). W normie ISO/IEC 7810:2003 zdefiniowano cztery formaty kart, ich opisy zawarto w tabeli 2.

Tabela 2

Formaty kart zdefiniowanych w normie ISO/IEC 7810:2003

Format	Wymiary (mm)	Zastosowanie
ID-1	85,60 × 53,98	W bankowości (m.in. karty zbliżeniowe), prawa jazdy, dowody osobiste (m.in. w Polsce)
ID-2 (A-7)	105 × 74	Dowody osobiste wydawane w Niemczech do listopada 2010 roku
ID-3 (B-7)	125 × 88	Ogólnoświatowy format paszportów i wiz
ID-000	25 × 15	Karty SIM

Źródło: opracowanie własne na podstawie normy ISO/IEC 7810:2003 *Identification cards – Physical characteristics*.

Występują różne standardy urządzeń RFID w zależności od parametrów technicznych, takich jak: prędkość transmisji, rozmiar pamięci transpondera, rodzaj kodowania czy rozróżnialność wielu urządzeń w zasięgu czytnika:

- TIRIS – jeden z pierwszych systemów RFID, wykorzystywany głównie w handlu do znakowania towarów (np. do zabezpieczania przed kradzieżą);
- Hitag – standard umożliwiający zdalny zapis i odczyt danych z prędkością 4 kb/s i częstotliwością 125 kHz oraz możliwością ich kodowania – wykorzystywany w przemyśle oraz przez systemy pobierania opłat (np. przy wejściu do obiektów rekreacyjno-sportowych, takich jak baseny czy wyciągi narciarskie), a także do znakowania zwierząt i produktów;
- Unique – najprostszy i powszechnie używany system do identyfikacji i kontroli dostępu, stosowany w legitymacjach studenckich i pracowniczych, do rejestracji czasu pracy; wykorzystuje częstotliwość 125 kHz w zasięgu czytnika do 15 cm; transfer danych odbywa się z prędkością 2 kb/s, pamięć całkowita ma pojemność 64 bity i jest przeznaczona tylko do odczytu;
- Q5 – system umożliwiający konfigurację transpondera i zabezpieczenie go hasłem (transponder składa się z 8 sektorów, z których pierwszy przechowuje dane konfiguracyjne, siódmy – ewentualne hasło zabezpieczające, a pozostałe sektory są wykorzystywane do odczytu i ewentualnie do zapisu, jeśli nie zostało ustawione zabezpieczenie);
- Mifare – standard umożliwiający pracę w częstotliwości 13,56 MHz (prędkość odczytu i zapisu danych wynosi 106 kb/s), wykorzystywany przede wszystkim w kartach bankowych, identyfikacyjnych i biletach; wszystkie typy kart (Ultralight, Ultralight C, Classic, Plus, DESFire, DESFire EV1, SmartMX, SAM AV2) są zgodne z normą ISO/IEC 14443 dla kart zbliżeniowych i protokołów transmisji danych między nimi;
- ICODE – system wykorzystujący transpondery bardzo płaskie, o dużej pojemności i pracujące w częstotliwości 13,56 MHz, stosowany głównie w sprzedaży detalicznej, logistyce (np. do śledzenia trasy przesyłki) oraz w bibliotekach.

Niestety, dotychczas stosowane standardy umożliwiają zdalne skopiowanie danych z karty w bardzo krótkim czasie (m.in. z powodu słabości mechanizmów szyfrujących).

Od 2005 roku mikrochipy RFID firmy Hitachi (pracujące w częstotliwości 2,45 GHz) są umieszczane w banknotach euro i dolarach w celu zabezpieczenia ich przed fałszerstwem i kontroli ich przemieszczania się. Pomimo mikroskopijnych rozmiarów (0,05 mm × 0,05 mm) mikrochipy mają pamięć ROM o pojemności 128 bitów. Oficjalnie mogą być odczytywane z odległości 40 cm, ale istnieje obawa, że zasięg dla odczytu i zapisu wynosi nawet kilka metrów.

Początkowo szerokie zastosowanie RFID ograniczała dość wysoka cena urządzeń, obecnie nie stanowi to już bariery dla ich coraz powszechniejszego użycia.

3. Rodzaje kart bezstykowych

W Polsce są wykorzystywane dwa typy zbliżeniowych kart płatniczych: MasterCard PayPass (wprowadzone przez BZ WBK w 2007 roku) oraz Visa payWave (wprowadzone przez BZ WBK w 2008 roku). Karty PayPass są używane w 37 krajach i dotychczas wydano ich ponad 100 mln. W Europie po raz pierwszy karty payWave wprowadzono w 2005 roku, a karty PayPass w 2006 roku w Turcji[4].

W Polsce w 2010 roku wydano ok. 2 mln kart zbliżeniowych (wzrost w ciągu roku z 320 tys. do 2,3 mln), w czerwcu 2011 było ich już ok. 5,9 mln, a w grudniu – 8 mln (na ok. 32 mln wszystkich rodzajów kart płatniczych). Większość z nich to karty Visa (5,5 mln)[5]. Nie jest to spowodowane tak dużym zainteresowaniem ze strony klientów, ale decyzjami banków, które wydają nowe karty płatnicze już tylko wykonane w tej technologii. Politykę taką wprowadziły banki PKO BP i Pekao SA wydając odpowiednio karty Visa payWave i MasterCard PayPass. Nowo instalowane terminale obsługują już oba rodzaje kart płatniczych (technologia PayPass była wprowadzana wcześniej, stąd nadal można spotkać czytniki obsługujące tylko karty MasterCard).

Karty zbliżeniowe bez jakiejkolwiek autoryzacji wykorzystywane są przede wszystkim do regulowania niewielkich płatności. Czas obsługi takiej transakcji jest bardzo krótki, ponieważ nie jest konieczne połączenie z bankiem i weryfikowanie stanu konta. Technologia payWave przy kwocie powyżej ustalonego w danym kraju limitu[6] wymaga wprowadzenia karty do czytnika przez sprzedawcę i autoryzacji klienta przez podanie numeru PIN. Natomiast technologia PayPass wymaga podania PIN-u i jedynie zbliżenia karty przez klienta do czytnika.

Banki starają się przekonać klientów do technologii RFID, oferując przeróżne gadżety (breloczki, zegarki) zamiast tradycyjnych kart plastikowych. Według danych z sierpnia 2011 roku Polska jest jednym z krajów o największej liczbie transakcji zbliżeniowych dokonywanych w Europie. Stale zwiększa się również liczba terminali POS (*Point Of Sale*) do obsługi kart zbliżeniowych – z ok. 10 tys. do ok. 40 tys. w ciągu 2011 roku, przy czym szacuje się, że w 2015 będzie ich 200 tys. Na stronach WWW Visa i MasterCard dostępna jest lista miejsc realizacji płatności w systemie bezstykowym. Z ankiety autorskiej przeprowadzonej wśród 190 studentów Politechniki Wrocławskiej w listopadzie 2011 roku wynika, że 51% z nich posiada zbliżeniowe karty płatnicze. Wszyscy studenci mają bezstykowe legitymacje studenckie, ale 20% nie zna i nie wykorzystuje ich możliwości.

---

[4] *MasterCard PayPass na świecie*. www.paypass.pl/#/na-swiecie

[5] Raport *Bankowość internetowa i płatności bezgotówkowe II kwartał 2011 r.*, 25.10.2011.

[6] W Polsce dla kart zbliżeniowych bez autoryzacji obowiązuje limit 50 zł, w USA 50 dol., w Wielkiej Brytanii 15 funta w krajach strefy euro 20 euro.

Płatność w technologii zbliżeniowej może być dokonana z użyciem dowolnego, odpowiednio przystosowanego przedmiotu (np. telefonu komórkowego czy klucza samochodowego) wyposażonego w aplikację płatniczą (np. Visa Mobile czy MasterCard Mobile). Rozszerzeniem technologii RFID jest technologia NFC (*Near Field Communication* – komunikacja bliskiego zasięgu) przeznaczona głównie dla telefonów komórkowych, umożliwiająca wymianę danych w zasięgu 20 cm.

Karty zbliżeniowe, posiadające wiele zalet, stwarzają również dużo zagrożeń. Dzięki wbudowanej antenie uaktywniają się tylko w odległości do 10 cm przy terminalach je obsługujących, ale istnieje tez prawdopodobieństwo odczytu danych z karty (na przykład daty ważności czy PIN-u) przez nieupoważnione osoby wyposażone w odpowiednie czytniki.

4. Zastosowania technologii bezstykowej a ochrona prywatności i danych

Wiele osób jest zachwyconych technologią zbliżeniową wykorzystywaną w kartach płatniczych, inni zdecydowanie są jej przeciwni. Sceptycy opowiadają się zwłaszcza przeciw praktykom banków zmuszających do posiadania kart zbliżeniowych, pomimo braku odpowiednich dla nich zabezpieczeń i małej liczby ogólnie dostępnych czytników. Od czerwca 2009 roku w Polsce wydawane są biometryczne paszporty z odciskami palców zapisanymi w chipie RFID wtopionym w okładkę (pierwszy e-paszport wydano w Malezji w 1998 roku). Od 2016 roku w kraju będą obowiązywały już tylko tego typu paszporty. Ochronne etui na paszporty i karty zbliżeniowe są już w sprzedaży, ale banki nie wydają kart w nie zaopatrzonych. Organy wydające dokumenty zbliżeniowe zapewniają o bezpieczeństwie ich użytkowania, ale firmy produkujące etui ochronne ostrzegają klientów przed możliwością zeskanowania danych i dowolnego ich wykorzystania. Dużym zagrożeniem, ze względu na możliwość powielenia urządzenia RFID, jest również wykorzystywanie technologii zbliżeniowej w kluczykach otwierających samochody lub bramy wejściowe.

Oprócz niewątpliwych zalet technologii zbliżeniowej można wymienić też wiele wad, a wśród nich możliwość użycia karty przez osoby niebędące właścicielem (brak konieczności autoryzacji przy niewielkich płatnościach), ograniczenie na kwotę i liczbę transakcji w ciągu dnia, brak możliwości zmiany limitu oraz wyłączenia funkcji obsługi zbliżeniowej, możliwość odczytu danych przez nieuprawnione osoby (urządzenia). Ponadto brak jednolitych standardów, niewystarczająca jest liczba czytników (terminali) i bywają one zawodne, a także istnieje możliwość zbierania poufnych informacji (np. o sposobie życia, podróżach użytkownika – co może prowadzić do utraty prywatności). Wprowadzenie kart zbliżeniowych stwarza możliwość rozwoju nowych rodzajów przestępstw. Dziwić może fakt zmuszania klientów banków do posiadania kart zbliżeniowych pomimo braku dostatecznej

liczby terminali je obsługujących, braku polityki w zakresie uświadamiania o możliwych zagrożeniach i promującej bezpieczne zachowania (np. przechowywania na koncie niewielkiej kwoty pieniędzy).

W Szwecji już w 1973 roku zezwolono na wszczepianie więźniom chipów RFID. Bywają one umieszczane w ciele pacjentów w domach starców i żołnierzy. Istnieje też kontrowersyjna koncepcja wszczepiania ich wszystkim noworodkom. W 2002 roku wszczepiono chipy firmy Applied Digital Solutions ochotnikom, którzy mogli je testować, automatycznie otwierając drzwi czy zapalając światło. Chip ten został zaakceptowany w 2004 roku przez amerykańską agencję do spraw żywności i leków – FDA (*Food and Drug Administration*) jako pierwszy biochip RFID, który może być wszczepiony w ciało człowieka. Brytyjski naukowiec Mark Gasson, chcąc ostrzec przed takimi praktykami, przeprowadził eksperyment (umieścił sobie pod skórą elektroniczny chip zainfekowany wirusem komputerowym, który został przekazany na inne chipy), wykazując możliwość niekontrolowanego infekowania tych urządzeń (np. rozrusznika serca), czego skutki mogą być groźne i nieprzewidywalne[7]. Zdaniem Europejskiej Grupy do spraw Etyki w Nauce i Nowych Technologiach (EGE) wszczepianie ludziom urządzeń RFID, ze względu na możliwe poważne skutki medyczne, powinno być precyzyjnie uregulowane.

W 2009 roku opublikowano raport o możliwości zdalnego skopiowania karty zbliżeniowej dowolnego typu w bardzo krótkim czasie, a w 2011 zademonstrowano możliwość uzyskania klucza zabezpieczającego z karty Mifare. W związku z licznymi obawami o bezpieczeństwo używania kart zbliżeniowych pracownicy MasterCard wydali oświadczenie[8], w którym potwierdzili możliwość nieuprawnionego odczytu z karty (numeru konta i data ważności), stwierdzając, że tak niewielka liczba pobranych danych jest bezużyteczna.

Wiele zastosowań technologii RFID dotyczy sektora medycznego. Niestety, przeprowadzone badania wykazują negatywny wpływ tagów RFID na pacjentów i na urządzenia medyczne[9].

Podsumowanie

Popularność i zakres wykorzystywania technologii RFID stale rosną. Znajduje ona zastosowanie niemal we wszystkich dziedzinach (handlu, bankowości, logistyce, motoryzacji, medycynie itd.). Wprowadzenie jej na masową skalę znacznie upraszcza i przyspiesza wykonywanie transakcji finansowych, czynności monitorujących i identyfikacyjnych, ułatwia zabezpieczanie towarów przed kradzieżą oraz

[7] www.reading.ac.uk/sse/about/news/sse-newsarticle-2010-05-26.aspx

[8] Ł. Szewczyk, *MasterCard, Płatności zbliżeniowe są bezpieczne*, 19.10.2011.

[9] www.di.com.pl/news/21523,0,RFID_zagrozeniem_dla_pacjenta.html

fałszowaniem. Być może wkrótce wszelkie informacje o obywatelu (dane osobowe, finansowe, medyczne itd.) będą zapisywane w jednym chipie RFID o wszechstronnym zastosowaniu (w urzędach, służbie zdrowia, bankowości, miejscu pracy, komunikacji, do identyfikacji przy otwieraniu drzwi mieszkania czy samochodu). Technologia ta jednak wymaga jeszcze ulepszenia. Brak jednolitych standardów ogranicza wykorzystywanie produktów wytwarzanych przez różnych producentów. Ponadto stosunkowo mała liczba zainstalowanych czytników dla urządzeń zbliżeniowych jest znaczącym ograniczeniem dla ich powszechnego wykorzystywania. Użytkownicy kart bezstykowych nie zawsze mają świadomość, że zapisane w nich dane mogą zostać zdalnie odczytane bez ich wiedzy. Jednak największe obawy wśród posiadaczy urządzeń zbliżeniowych wzbudza świadomość możliwości istnienia ukrytych funkcji i sposobów ich wykorzystywania (np. do obserwowania ich aktywności). Niestety, wszelkie działania zmierzające do zapewnienia bezpieczeństwa obywateli na jak najwyższym poziomie mogą prowadzić do zagrożenia ich prywatności.

Literatura

1. *Could humans be infected by computer viruses?* www.reading.ac.uk/sse/about/news/sse-newsarticle-2010-05-26.aspx (26.05.2010).
2. http://phamthaiquy-rfid.blogspot.com/2009/04/week-1-introduction-to-rfid.html
3. http://upway.pl/tagi-rfid-inlay
4. *Master Card PayPass na świecie*. paypass.pl/#/na-swiecie
5. Norma ISO/IEC 7810:2003 *Identification cards – Physical characteristics*.
6. Portal RFID: www.portalrfid.pl/wprowadzenie.php?it=6
7. Raport *Bankowość internetowa i płatności bezgotówkowe II kwartał 2011 r*. www.zbp.pl/site.php?s=MTM0NTkxMDU (25.10.2011).
8. Szewczyk Ł., *MasterCard: Płatności zbliżeniowe są bezpieczne*, media2.pl/technologie/84957-MasterCard-Platnosci-zblizeniowe-sa-bezpieczne.html (19.10.2011).
9. www.di.com.pl/news/21523,0,RFID_zagrozeniem_dla_pacjenta.html

PROXIMITY TECHNOLOGIES VERSUS DATA SECURITY

Summary

More and more id and payment cards are based on the RFID technology, which uses radio transmission that allows for object identification from a short distance. This technology becomes increasingly popular for the convenience it brings, high reliability and a diverse range of possible applications. There are, however, concerns related to the security of the stored data and the operations using this data; these issues are discussed in this paper.

Translated by Zygmunt Mazur