UDC: 337.71:004.738.5 Info M: str. 33-40

SPREČAVANJE ZLOUPOTREBA U ELEKTRONSKIM SISTEMIMA ZA RAD SA PLATNIM KARICAMA
AVOIDING FRAUD IN ELECTRONIC PAYMENT CARD SYSTEMS

Marija Bogićević
Fakultet organizacionih nauka, Univerzitet u Beogradu

REZIME: Fraud je danas glavni problem u elektronskim sistemima za rad sa platnim karticama. Predmet ovog rada je pregled postojećih tehnika za sprečavanje zloupotreba u elektronskim sistemima za rad sa platnim karticama. Prevencija i detekcija zloupotreba imaju izuzetno važnu ulogu u oblasti risk management-a kao i fraud management-a u industriji platnih kartica. Krajnji cilj je smanjiti zloupotrebe primenom multidisciplinarnog pristupa. Sistem za sprečavanje zloupotreba za rad sa platnim karticama je složen sistem koji prikuplja znanja iz više izvora. Prikazane tehnike za prevenciju i detekciju zloupotreba su svrstane u više grupa, po različitim kriterijumima. U radu je prikazano trenutno stanje u svetu i dato je detaljno poređenje savremenih tehnika za prevenciju, detekciju i upravljanje zloupotrebama u elektronskim sistemima za rad sa platnim karticama. Sa finansijskog aspekta prikazan je operativni rizik kao najznačajniji rizik u transakcionim sistemima, kao i model za merenje tog rizika. Dat je primer mogućih poboljšanja sprečavanja fraud-a u sistemima za rad sa platnim karticama.

KLJUČNE REČI: fraud management systems, upravljanje rizikom, elektronski platni sistemi, bezbednost, biometrija

ABSTRACT: Nowadays, fraud is a major issue in electronic payment systems. The aim of this paper is to give an overview of the existing techniques for preventing fraud in electronic payment systems. Prevention and detection of fraud play a very important role in risk management and fraud management in the payment cards industry. The end goal is to reduce fraud by applying a multidisciplinary approach. A system for the prevention of payment card fraud is a complex system which gathers knowledge from several sources. The techniques for the prevention and detection of fraud are classified in several groups, applying different criteria. The paper shows the current state of affairs in the world and gives a detailed comparison of modern techniques for the prevention, detection and management of fraud in electronic payment systems. From the financial point of view, the operational risk is shown as the most significant risk in transactional systems, and a model for measuring such risk. Example of possible improvements in the prevention of fraud in electronic payment systems is given.

KEY WORDS: fraud management systems, risk management, electronic payment systems, security, biometrics

1. UVOD

Jedan od najvećih problema elektronskog bankarstva je što se sve više i više zloupotrebljene transakcije javljaju kao ispravne, odnosno legitimne.

Što se tiče istorijskog razvoja *fraud*-a u elektronskim sistemima za rad sa platnim karticama, može se reći da je sedamdesetih godina prošlog veka bila zastupljena krađa i falsifikovanje kartica, gde su se fizički kartice krale. Naručivanje telefonom/mejlom je postalo uobičajeno osamdesetih i devedesetih godina. *Online fraud* se preselio na svetsku mrežu kako je Internet zaživeo svuda i postao nešto što omogućava anonimnost, dostupnost i brzinu da se komituje *fraud* širom sveta.

Jedan od najbržih načina kupovine je kupovina pomoću platne kartice, gde se dobija roba odmah a plaća se kasnije. Elektronski sistemi plaćanja imaju niz prednosti, poput nabavke proizvoda iz udaljenih delova sveta radi komfornosti potrošača. Međutim to ima i nedostatke, poput bezbednosti podataka koji se prenose i izloženosti riziku da isti budu kompromitovani. Glavni izazov kod elektronskih sistema plaćanja je njihova zaštita (Simić, 05). Samim tim zloupotreba kreditnih kartica je ozbiljan problem sa kojim se suočavaju svi učesnici u ovom lancu komunikacije.

Danas, većina ljudi koristi elektronsku trgovinu delom zbog ekonomskih razloga, a delom i zbog pogodnosti, jer nema potrebe ići negde van. Međutim, zloupotreba kartica je ozbiljan problem. Svake godine organizacije koje izdaju kartice kao i sami potrošači izloženi su velikim finansijskim troškovima, kao i potencijalnom gubitku prihoda. Sa nekim tehnikama koje napadači koriste da bi zloupotrebili kartice se jako teško izboriti, jer neke od metoda koje se koriste za autorizaciju su pogrešne i neadekvatne. Sam kupac u najvećem broju slučajeva i ne zna šta se dešava u sistemu nakon što kupi određeni proizvod. Kada su se koristile kartice sa magnetnom trakom, trgovac je mogao da proveri potpis na slipu sa potpisom na poleđini kartice. Međutim, ako je kartica ukradena, napadač će najverovatnije uvežbati potpis tako da upoređivanje više ne vredi. Može da se uvede viši nivo prevencije u tom slučaju da se zatraži još neki dokument koji potvrđuje identitet te osobe, poput lične karte ili vozačke dozvole. A još viši nivo zaštite koji je uveden je unos PIN-a, kada potpis korisnika nije potreban. Kod zloupotreba kada kartica nije prisutna, raznim metodama se dolazi do podataka koji su neophodni. Što se više koristi kartica za kupovinu putem interneta to je izloženija napadima i kompromitovanju. Jedna od metoda u nekim regionima je da se tehnikama socijalnog inženjeringa dođe do broja socijalnog osiguranja, koji se koristi da se dodatno utvrdi identitet osobe.

Banke su izuzetno zainteresovane za brzinu rada procesora po kojoj može biti detektovan *fraud*. Bilo koja aktivnost koja može da ugrozi vlasnika kartice, a samim tim i bankarsku insituciju koja stoji iza njega. To može biti banka gde vlasnik ima račun za koji je vezana kartica ili procesorska kuća koja stoji iza banke. Insitucije uglavnom kombinuju osnovne vidove prevencije sa složenijim i tako čine ono što se zove *Fraud Management* ili Upravljanje zloupotrebama. Tehnologije *fraud*-a se suočavaju sa mogućnostima aktivnog praćenja naloga da bi se otkrile i za početak naslutile sve nepravilnosti u radu transakcija.

Sa finansijskog aspekta ako se posmatraju zloupotrebe, to je kao rekurzivni životni ciklus koji ilustruje odgovor na po-

našanje napadača koji se dobija u kontinuitetu. Brzi trendovi u razvoju zloupotreba su doveli do toga da se sistemi usavršavaju i primenjuju složeni algoritmi poput tehnika *data mining* i kroz analize podataka. Cilj je da se osmisle novi sigurnosni protokoli kao i protokoli za autentikaciju. Kao odgovor na te inovacije, napadači osmišljavaju nove tehnike napada kojima će prevazići te mere odbrane. Novi paterni zloupotreba su identifikovani, kao rezultat raspoređivanja sigurnosnih poboljšanja a kroz razvoj novih softverskih rešenja, tačnije kroz jaču autentikaciju i bezbednosne procedure. Na slici 1. je prikazan životni ciklus zloupotreba.

Slika 1. *Životni ciklus zloupotreba (Wilhelm, 04)*

Bezbednost sistema je od izuzetnog značaja, pre svega se misli na zaštitu od zloupotreba, čemu u prilog ide Tabela 1, koja pokazuje procenu prometa u elektronskoj trgovini koja se kreće u milijardama dolara za najveće američke prodavce (maloprodaja). Ljudi sve više kupuju preko Interneta pa tako raste e-trgovina, koja čini da *online* finansijske transakcije budu oblast plaćanja koja se najbrže razvija. Zaštita transakcija na Internetu je od posebnog značaja već duži niz godina (Beljić, Simić, 06). U skladu s tim ako se očekuje veliki promet finansijskih sredstava, zapravo je reč o milijardama dolara na godišnjem nivou, sigurno je da će i napada biti sve više, tako da se mora raditi na povećanju bezbednosti takvih sistema. Istraživanje i procenu američke maloprodaje izvršile su vodeće svetske kompanije koje se bave istraživanjem tržišta u oblasti informacionih tehnologija pre svega u oblasti elektronskog bankarstva i bezbednosti sistema, poput Forrester Research, JMP Securities, eMarketer, RBC Capital Markets i mnogi drugi.

Kompanija	2014	2015	2016	2017
Forrester Research	291	319	345	370
JMP Securities	295	331	364	397
eMarketer	297	339	385	434
RBC Capital Markets	292	-	-	-
Cantor Fitzgerald	276	304	331	-
Robert W. Baird	272	299	329	-

Tabela 1. *Procena e-trgovine američke maloprodaje za period 2014.-2017. u milijardama dolara (Payments Council White Paper, 14)*

2. FINANSIJSKI GUBICI OD ZLOUPOTREBA KARTICA U SVETU

Zloupotrebe kartica poprimaju sve veće razmere, u prilog tome idu i sledeći statistički podaci. Samo u 2012. godini zloupotreba kreditnih i debitnih kartica prouzrokovala je gubitak od 11,7 milijardi dolara u celom svetu. Iste te godine najveći broj zloupotrebljenih finansijskih transakcija pomoću kartica iznosio je 47,3% ukupnog svetskog prometa. Čak 67% više u odnosu na 2010. godinu je bilo napadnutih američkih građana (Lindsay, 14).

U tabeli 2. prikazani su gubici od zloupotreba kartica po regijama u svetu, gde oznaka P-*predicted* predstavlja predviđene gubitke. Može se zaključiti na osnovu tabele da su veliki troškovi i da je sprečavanje zloupotreba u elektronskim platnim sistemima problem kome treba sistematično pristupiti.

Regionalna potrošnja u milionima američkih dolara	2011	2012	2013	2014P	2015P	2016P	Godišnji rast
Severna Amerika	$794	$794	$799	$800	$806	$816	0,5%
Evropa	$444	$453	$460	$463	$465	$466	1%
Pacifička Azija	$379	$416	$455	$491	$528	$564	8,3%
Latinska Amerika i Karibi	$98	$106	$114	$122	$130	$137	7%
Srednji Istok i Afrika	$31	$33	$34	$35	$36	$36	3,2%

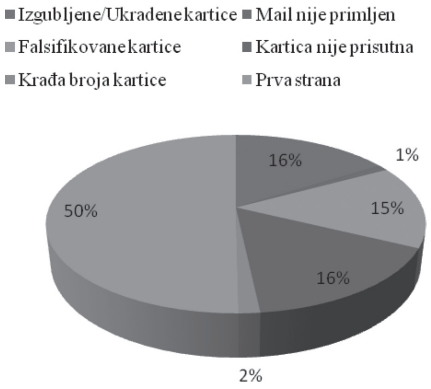
Tabela 2. *Predviđanje troškova i gubitaka u svetu (Riley, 12)*

2.1 *Vrste zloupotreba*

Prema izveštaju Aite Group iz 2010.godine zloupotrebe se mogu klasifikovati na sledeći način:

1. First-party fraud – Zloupotreba prve strane
2. CNP (*Card not present*) – kartica nije prisutna
3. *Counterfeit* – falsifikovanje kartice
4. Izgubljene i ukradene kartice
5. *Mail* nije stigao
6. Krađa broja kartice – krađa identiteta

Na Slici 2. prikazani su gubici po vrstama zloupotreba po Aite Group (Aite Group, 12). To istraživanje je pokazalo da su u 2008. godini u Sjedinjenim Američkim Državama bili najveći ukupni finansijski gubici. Zloupotreba CNP je najslabija tačka za gubitke kod trgovaca. CNP zloupotreba raste više od falsifikovanja kartica. Sledeća slika pokazuje da najveći udeo uzima zloupotreba prva strana.



Slika 2. *Udeo pojedinih vrsta zloupotreba za 2012. godinu (Aite Group, 12)*

2.2 *Najveći napadi u istoriji fraud management-a*

O značaju sprečavanja zloupotrebe kreditnih kartica govore veliki napadi koji su se desili u poslednjih deset godina, kada je ovaj problem postao ozbiljan. U periodu od jula 2005. do avgusta 2007. godine, napadi na sisteme u TJX kompaniji, razotkrili su podatke sa više od 45,6 miliona kartica (Jones, 2013). Albert Gonzales je optužen za glavnog napadača koji je organizovao grupu koja izvela ovaj napad. Smatra se da je Gonzales u saradnji sa deset istomišljenika izveo napad tako što je koristeći bežične skenere pronalazio prodavnice sa ranjivim mrežama da bi mogao da otkrije podatke sa kartica.

U avgustu 2009. godine, opet je Gonzales okrivljen kao glavni osumnjičeni za zloupotrebu kartica u ovom slučaju za više od 130 miliona kartica koje su ukradene u Heartland Payments Systems, maloprodajnom lancu 7-Eleven i Hannaford Brothers i još dve neidentifikovane kompanije (Godin, 2009). U najvećem broju slučajeva napadači u što kraćem vremenskom periodu, kada se domognu podataka sa kartice ili same kartice odmah skidaju što više novca sa žrtvinog računa. Ovo je jedan od najvećih napada u Sjedinjenim Američkim Državama. Napad je izveden *SQL injection* koji je upotrebljen da bi se instalirao program za prisluškivanje na serveru Heartland Payments System koji će prikupljati i presretati podatke sa kartica. Ovaj napad je bio velika sramota i narušavanje reputacije kompanije, koja mesečno obradi više od 100 miliona transakcija za više od 250.000 trgovaca.

U 2012. godini preko 40 miliona kartica je kompromitovano, hakovanjem kompanije Adobe Systems. Činjenica je da je u 2012. godini gubitak od zloupotreba kartica bio 11,3 milijardi dolara, što je 15% više u odnosu na prethodnu godinu (Economist, 2014). Amerika je jedna od retkih zemalja gde je falsifikovanje kartica i dalje u usponu. Po tom osnovu izdavaoci kartica su na gubitku od 3,4 milijardi dolara, a trgovci 1,9 milijardi dolara u toj 2012. Krajem 2013. godine 1,2 milijardi kartica, debitnih, kreditnih i pre-paid je upotrebi u Americi, što je znatno više nego u bilo kojoj drugoj regiji na svetu, a to je u proseku 5 kartica po čoveku. U 2012. godini je više od 45% platnih kartica u svetu i više od 75% terminala koristilo čip i pin.

Već u julu 2013. godine došlo je do novog napada koji je zabeležen pod imenom ”najveće hakovanje i razotkrivanje podataka u Americi ikada”(Benson, 2013). Rusi i Ukrajinci su bili umešani u ovaj slučaj koji se desio u New Jersey, a koji je razotkrio 160 miliona brojeva kreditnih kartica. Ti brojevi kartica su kasnije iskorišćeni za štampanje novih plastičnih kartica koje su korišćene u kupovini. Ovaj napad je prouzrokovao gubitke od nekoliko stotina miliona dolara.

U periodu 27. novembar 2013. - 15. decembar 2013.godine došlo je do kompromitovanja oko 40 miliona kartica, uključujući ime vlasnika, broj računa, datum važnosti kao i CVV vrednosti. Meta hakovanja je bila kompanija Target Corporation. A procenjuje se da je oko 70 miliona ljudi bilo oštećeno.

Još jedan noviji napad desio se u vremenskom periodu 16.jul 2013. - 30.oktobar 2013. na kompaniju Neiman-Marcus odakle je otkriveno milion brojeva kartica skladištenih u njihovom sistemu (Wagenseil, 2014).

Nedavno je došlo i do napada na banke u Indijani. Do informacija sa kartica se došlo sa ATM-ova ili plaćanjem debitnim karticama, gde je više od 100 korisnika bilo oštećeno. A transakcije od nekoliko stotina do nekoliko hiljada dolara su izvršene u Nigeriji, Rusiji, Ukrajini i Španiji. U istoj godini prijavljeno je puno slučajeva od strane Citibank-e, gde su samo dva čoveka izvela stotine transakcija sa ATM u New Jork-u uzevši oko 750.000 dolara. Server sa podacima u Citibank-u je bio meta napada. FTC je od 2007. godine zabeležio preko 800.000 korisnika koji su oštećeni gde je ukupna vrednost zloupotreba preko 1,2 milijardi dolara.

Godine 2012. desio se novi napad i to na platni procesor Global Payments koji je imao za posledicu kompromitaciju milion kartica. Platni sistemi Visa i MasterCard su bili meta, a sumnjalo se da su kompromitovane magnetne trake, traka 1 i traka 2. U maju 2012. mogao se izvesti zaključak da su se napadači pomerili iz Velike Britanije u Francusku i Nemačku, usled uvođenja EMV u VB.

U toku 2013. godine se desio veliki broj napada na kartice, tzv. *data breaches* , kada su napadači iskoristili sve svoje sposobnosti da što više zloupotrebe nedostatke nekih sistema, primer su kompanije Target i Neiman Marcus.

3. *Tehnike za prevenciju zloupotreba platnih kartica*

Razvoj novih tehnika za utvrđivanje *fraud*-a platnih kartica je složen, pre svega zbog ograničenja u razmeni ideja i informacija iz ove oblasti. Kada se detalji o tehnikama *fraud*-a obelodane, osobe koje su izvršile napad mogu da iskoriste informacije da bi izbegle svoje otkrivanje, ali isto tako ti detalji služe i za usavršavanje budućih tehnika za napad, koristeći trenutne propuste sistema. Set podataka koji je potreban za bilo koju tehniku *fraud*-a nije dostupan javnosti.

Tehnike za sprečavanje *fraud*-a mogu da se klasifikuju na razne načine, jedan od njih je sledeći:

1. Primena osnovnog seta pravila.
2. Implementacija EMV standarda.
3. Korišćenje složenih sigurnosnih protokola.
4. Korišćenje pametnih alata za prevenciju i detekciju.

3.1 *Komparativna analiza tehnika za prevenciju fraud-a*

Tabela 3. prikazuje evaluaciju tehnika za prevenciju *fraud*-a uzimajući u obzir opšte i konceptualne karakteristike tehnika kao što su *AVS, CVV2, Manual review*, Negativna i pozitivna lista, *Trusted e-mail* i biometrija (Bogicevic, 14). Za ove tehnike je izvršena komparacija po sledećim karakteristikama: da li su jednostavne za upotrebu, da li su jednostavne za implementaciju, koliko su brze, koja im je cena, da li se ta usluga naplaćuje, da li zahteva neku izmenu sistema ukoliko se implementira, da li obezbeđuje smanjenje zloupotreba, kakvo je realno da se primeni tehnika. Došlo se do zaključka da su najjednostavnije za upotrebu *AVS, CVV2*, negativna i pozitivna lista, autentikacija i *trusted e-mail*. Teška za implementaciju je biometrija, pa je samim tim i skupa za realizaciju. Dok su *AVS* i *CVV2* brze tehnike koje nisu skupe da se izvedu i koje ne menjaju gotovo ništa u sistemima da bi se realizovale, za razliku od biometrije. Najbolje utiču na smanjenje *fraud*-a autentikacija kupca, *mail* od poverenja i biometrija.

		Evaluacija tehnika						
KARAKTERISTIKE		**AVS**	**CVV2**	**Manual Review**	**Negativna i Pozitivna lista**	**Autentikacia Kupca**	**Trusted e-mail**	**Biometrija**
Opšte	**Jednostavno za upotrebu**	V	V	S	V	V	V	S
	Jednostavno za implementaciju	V	V	S	V	V	V	N
	Brzina	V	V	N	S	V	V	S
	Cena	N	N	S	S	S	N	V
Konceptualno	**Plaćanje usluge**	S	S	NI	NP	V	V	V
	Zahteva bilo kakvu izmenu sistema	N	N	N	S	S	N	V
	Prevencija fraud-a	S	S	N	N	V	V	V
	Realno vreme procesa	V	V	NP	V ili NP	V	V	V

Visoko -V, Srednje -S, Nisko -N, Nije indikovano -NI, Ne postoji –NP

Tabela 3. *Evaluacija tehnika za prevenciju fraud-a (Al-Furiah, 09)*

Tabela 4. predstavlja prednosti i nedostatke tehnika za prevenciju *fraud*-a, i to AVS, CVV2, *Manual review,* Negativna i pozitivna lista, Autentikacija kupca, *Trusted e-mail,* Biometrija.

Tehnike	**Prednosti**	**Nedostaci**
AVS	- jednostavno, brzo i lako za implementaciju - smanjuje rizik *fraud*-a - avs pomaže trgovcima da naplate uslugu - nema dodatnog troška jer može da se zahteva avs kao deo autorizacije	- nekad je stvarna adresa kupca različita od one koja je prijavljena pri izdavanju kartice - nije savršen pokazatelj da je nešto *fraud* - avs je neefektivan za *soft* proizvode
CVV2	- smanjuje *CNP fraud* - sprečava falsifikovanje kartica - nema dodatnog troška - smanjuje zloupotrebljene troškove	- nije primenjivo kod ukradenih i izgubljenih kartica - napadač može da upadom u sistem da dođe do CVV2 vrednosti
Manual Review	- najkorisnije kad se koristi sa još nekim tehnikama	- nije efektivna tehnika za prevenciju frauda - kvalitet posla zavisi od iskustva zaposlenih i povratnih informacija od njih - to je jako skupa metoda i zahteva puno vremena
Negativna i Pozitivna lista	- to je osnovna tehnika-polazna za sva dalja razmatranja - jednostavna upotreba - negativna lista je dobra za smanjenje fraud-a - pozitivna lista smanjuje vreme za proveravanje validne narudžbenice	- ne može da spreči *fraud* krađa broja kartice - neophodna je učestalo *update*-ovanje
Autentikacija Kupca	- to je početni alat koji obezbeđuje zaštitu trgovca od zloupotrebljenih dodatnih troškova - udruženja obezbeđuju ovu tehniku da bi kupci što više koristili online kupovinu - ukupna cena je niska - odgovornost u troškovima je protiv kupca	- samo Visa i Master card kupci mogu da koriste ovu uslugu - kupci ne vole ovu tehniku, jer oduzima vreme
Trusted e-mail	- to je efektivna tehnika da zaštiti trgovce i da smanji trošak - jednostavno za implementaciju i upotrebu - bolje od bilo koje druge metode koja koristi adresu isporučivanja ili neki kod za verifikaciju - niska cena - zahteva minimalne izmene za sve učesnike elektronskog plaćanja - ne sadrži smetnje nekih drugih rešenja	- nisu otkriveni nedostaci
Biometrija	- veoma efektivna tehnika za autentikaciju identiteta kupca	- teško za implementaciju - skupo - zahteva mnogo izmena

Tabela 4. *Prednosti i nedostaci tehnika za prevenciju fraud-a (Al-Furiah, 09)*

4. ALGORITMI ZA DETEKCIJU ZLOUPOTREBA PLATNIH KARTICA

Hakeri, koriste sve moguće načine da zloupotrebe neki deo lanca u komunikaciji između entiteta kod korišćenja platnih

kartica i da dođu do željenih podataka. Nameće se kao logično rešenje prevencija i implementacija svih tehnika da bi se sprečila zloupotreba. Postoji mnogo tehnika za prevenciju *fraud*-a, a u isto vreme se te tehnike usavršavaju i radi se na njihovom poboljšanju (Kou, 04).

Detekcija *fraud*-aje jako kompleksan informatički problem i sigurno ne postoji sistem koji zasigurno može da predvidi tip *fraud*-a koji će se desiti. Postoje osnovna pravila koje *fraud management* sistemi (FMS) mogu da implementiraju i da primene, ali nekad ona nisu dovoljna i koriste se složeni algoritmi za sagledavanje i predviđanje transakcija, da li su one zloupotrebljene ili ispravne. Ti složeni algoritmi rade na principu predviđanja verovatnoće da li će se desiti neki događaj, u ovom slučaju događaj je da li je transakcija fraud. Tehnike za prevenciju i detekciju moraju da utiču na smanjenje frauda, a one su jedan ključni deo za upravljanje rizikom u bankarskom sektoru, konkretno kod rada sa elektronskim sistemima za rad sa platnim karticama. Upravo tehnike za prevenciju sadrže niz osnovnih pravila, a kada ta pravila ne uspeju da spreče *fraud* primenjuju se tehnike za detekciju.

S obzirom na to da se razlikuju *online* i *offline* zloupotrebe, možemo kod FMS razlikovati *online* i *offline* monitoring. Za različite vrste *fraud*-a mogu se primeniti različite tehnike. FMS moraju da obezbede sledeće:

1. Da detektuju *fraud* rano i precizno.
2. Da obezbede relevantne informacije analitičarima *fraud*-a u pravo vreme.
3. Dobar sistem ne bi trebalo ispravnu transakciju da prepozna kao *fraud*.
4. Da automatizuju proces gde je to moguće.
5. Da se samoadaptiraju promenama u paternima *fraud*-a.
6. Da se samoadaptiraju promenama u ponašanju potrošača.

Tehnike za prevenciju i detekciju mogu biti implementirane na strani izdavaoca (*issuer*) i primaoca (*acquirer*), a glavna razlika je što se sumnjiva transakcija na strani izdavaoca uglavnom odbija.

Ovo su najčešće korišćeni algoritmi za detekciju zloupotreba kreditnih kartica (Zareapoor, 12):

1. Fusion pristup koristeći Demspter-Shafer teoriju i Bajesovo učenje
2. Blast-Ssaha hibridizacija
3. Skriveni Markovljev model
4. Neuronske mreže
5. Bajesova mreža
6. Genetski algoritmi
7. Veštački imuni sistemi
8. Algoritam k-najbližeg suseda
9. Vektori za podršku
10. Drvo odlučivanja
11. Fazi logički zasnovani sistemi
12. Samoučeća strategija

4.1 *Komparativna analiza algoritama za detekciju*

Trenutno su sistemi za monitoring transakcija kod elektronskih sistema za rad sa platnim karticama jedan od ključnih aspekata u bankarstvu. Postoji mnogo načina za detekciju frauda. Neki od primenjenih i implementiranih algoritama brže, neki sporije prepoznaju da li je transakcija *fraud* ili ne.

Prikazane su metode koje podrazumevaju složene algoritme za detekciju zloupotreba u elektronskim sistemima za rad sa platnim karticama. Uzeti su u razmatranje ključni pokazatelji kao što su tačnost, brzina i cena koštanja jednog takvog sistema. Tabela 5. prikazuje komparaciju ovih metoda po već pomenutim kriterijumima.

Sistem koji je zasnovan na fazi darvinovoj teoriji ima jako visoku tačnost, čak 100%, ali je brzina procesiranja izuzetno spora. Dok sa druge strane HMM ima veliku brzinu obrade transakcije ali je tačnost mala. Bajesove mreže su jako brze sa dobrom tačnošću u poređenju sa drugim tehnikama. U isto vreme brzina procesiranja kod tehnike drvo odlučivanja je dovoljno brza da omogući detekciju *fraud*-a. AIS algoritmi se izdvajaju od ostalih, jer imaju dobar rezultat a dobru brzinu izvršavanja. Drvo odlučivanja ima veliku brzinu izvršavanja, K-najbliži sused ima dobar rezulat.

Tako da sve ove tehnike imaju svoje nedostatke, ali isto tako i prednosti, tako da je najbolje formirati hibridni model koji će uzeti sve što je dobro i eliminisati loše iz nekih algoritama.

Metoda	Brzina detekcije	Tačnost	Cena
Skriveni Markovljev model	Brza	Niska	Izuzetno visoka
Fazi darvinov model	Veoma mala	Veoma visoka	Izuzetno visoka
Veštački imuni sistem	Veoma brza	Dobra	Jeftina
Fazi neuronska mreža	Veoma brza	Dobra	Skupa
Neuronska mreža	Brza	Srednja	Skupa
Drvo odlučivanja	Brza	Srednja	Skupa
Bajesova mreža	Veoma brza	Visoka	Skupa
K-najbliži sused	Dobra	Srednja	Skupa
SVM	Niska	Srednja	Skupa
Samo organizujuće mape	Brza	Srednja	Skupa
Back propagacija	Niska	Niska	Skupa
Genetski algoritmi	Dobra	Srednja	Jeftina

Tabela 5. *Komparacija različitih metoda za detekciju zloupotreba (Zareapoor, 12)*

5. UPRAVLJANJE RIZIKOM

Rizik i neizvesnost su dva ključna pojma u vezi donošenja odluka u bilo kojoj instituciji, posebno u bankarskim koje su ovde od posebnog značaja. Verovatnoća je mera slučajno izabrane neizvesnosti i statističkih modela da bi izračunali statistički rizik. Finansijski rizik se može definisati kao mera ne-

izvesnosti koju je kupac spreman da prihvati kada realizuje finansijsku transakciju. Ova vrsta rizika je povezana sa platnim sistemima i kreditnim opcijama koje se nude potrošačima. Na početku razvoja e-trgovine finansijski rizik se odnosio na one artikle koji nose manji stepen rizika poput knjiga, muzike, odeće, putovanja. Generalno gledano, više se cene proizvoda gledaju u *offline* režimu kupovine nego kod *online* transakcija, pa odatle i veći rizik kod ove vrste kupovine. Novija istraživanja pokazuju da finansijski rizik zavisi od godina korisnika, pola, obrazovanja, bračnog statusa.

Za izračunavanje bilo koje vrste rizika koristi se matematička formula, tzv. racio koji se koristi za formiranje složenih modela gde je u upotrebi više racia i njihova međusobna zavisnost. U radu sledi prikaz modela za merenje operativnog rizika. Upravo se operativni rizik bavi finansijskim transakcijama i svim mogućim događajima koji ih prate. Što se tiče operativnog rizika i zloupotreba kod finansijskih transakcija, banke u Srbiji nemaju modele za tu vrstu rizika, jer se smatra da je nivo zloupotreba jako nizak. Tako da se taj rizik reguliše uvođenjem standarda ali i svim metodama za prevenciju i detekciju algoritama, koje su opisane u prethodnim poglavljima rada. Ono što je ključno je to da svi događaji koji prouzrokuju neku vrstu *fraud*-a ulaze u razmatranje za operativni rizik i dodeljuje im se odgovarajući ponder, samo je bitno prepoznati i definisati sve događaje koji se mogu desiti.

Banke se suočavaju sa više vrsta rizika, kao što su kreditni rizik, tržišni i operativni (Li, 13). Ovi rizici su se u prvo vreme posmatrali i merili odvojeno. Međutim, vremenom se ta granica pomerala i 2007. godine kada je nastupila kriza došlo se do zaključka da oni utiču jedni na druge i da ih nije moguće razdvajati. Određuju se kvantitativne mere za izračunavanje rizika koje se mogu pridružiti svim vrstama rizika. Finansijski analitičari kreiraju finansijske podatke dostupne za operativni rizik kao jednu od vrsta finansijskog rizika, kroz različite metode, tako da statistički modeli mogu biti primenjivi na njega. Mnoge velike banke su počele sa prikupljanjem podataka o svojim gubicima i njihovim merenjem kroz operativni rizik. Većina njih ima ograničene vremenske serije, ali i pored manjeg broja podataka o velikim gubicima, oni predstavljaju obavezni model.

Kada se posmatra poslovanje jedne bankarske institucije, može se istaći da se kreditni rizik izdvaja sa učešćem od 60%, operativni rizik učestvuje sa 30% i tržišni sa 10%.

5.1 *Operativni rizik-OR*

Velika pažnja posvećena je operativnom riziku u poslednjih nekoliko godina usled uticaja sledećih događaja:

1. Globalizacija međunarodnih finansijskih tržišta povećala je kompleksnost finansijskih servisa u okviru kompanija kao i njihovu izloženost događajima koji se mogu svrstati u operativni rizik.
2. Konsolidacija industrije finansijskih servisa kreirala je veće, kompleksnije organizacije ali i rizik zbog nekompatibilnih sistema koji je sastavni deo te integracije.
3. Veliki uticaj informaciono komunikacionih tehnologija na finansijske transakcijedoprineo je većoj verovatnoći da sistem padne.
4. *Cross share-holdings* i među bankarske pozajmice proizvele su veliku izloženost događajima operativnog rizika.
5. Razvoj elektronskog bankarstva i elektronske trgovine doveo je institucije koje su uključene u te procese da budu izložene novim vrstama rizika, kao i onim već standardnim a to su sve vrste *fraud*-akoje su već pomenute u radu.
6. Investitori i pravnici su istakli transparentnost u finansijskim izveštajima, kao odgovor na Enron, WorldCom i druge instance računovodstvenih nepravilnosti.

Model operativnog rizika je skup funkcija koje predstavljaju neizvesne buduće događaje. Neizvesnost može biti pojava nekog događaja, vreme pojavljivanja, kao i visina gubitka koji prouzrokuje neki događaj (Kim, 08). Neizvesnost se može predstaviti putem verovatnoće, pa je s obzirom na to model merenja operativnog rizika zapravo model verovatnoće.

Ne postoji jedinstvena definicija pojma rizik. Rizik se može definisati kao mera neizvesnosti. Za rizik se može reći da je to mera uzimanja potencijalnog neprekidnog gubitka. A u kontekstu operativnog rizika, rizik se definiše kao mera verovatnoće da se desi gubitak. Na taj način definisan rizik se doživljava kao verovatnoća negativne devijacije, tj. izražava opasnost da efekti budućih ishoda događaja odstupaju od očekivanih ishoda na negativan način. Zbog prirode ove vrste rizika, ne postoji njegova opšte prihvaćena definicija. Definicija koju je usvojio Bazelski komitet za bankarski nadzor glasi (BIS, 11):

„Operativni rizik je rizik direktnih ili indirektnih gubitaka koji nastaju zbog neadekvatnih procedura ili neuspelih internih procesa, ljudskog faktora, sistemskih ili eksternih događaja."

Jedna od modela merenja operativnog rizika je Napredni pristup merenju (AMA) (BIS,11).

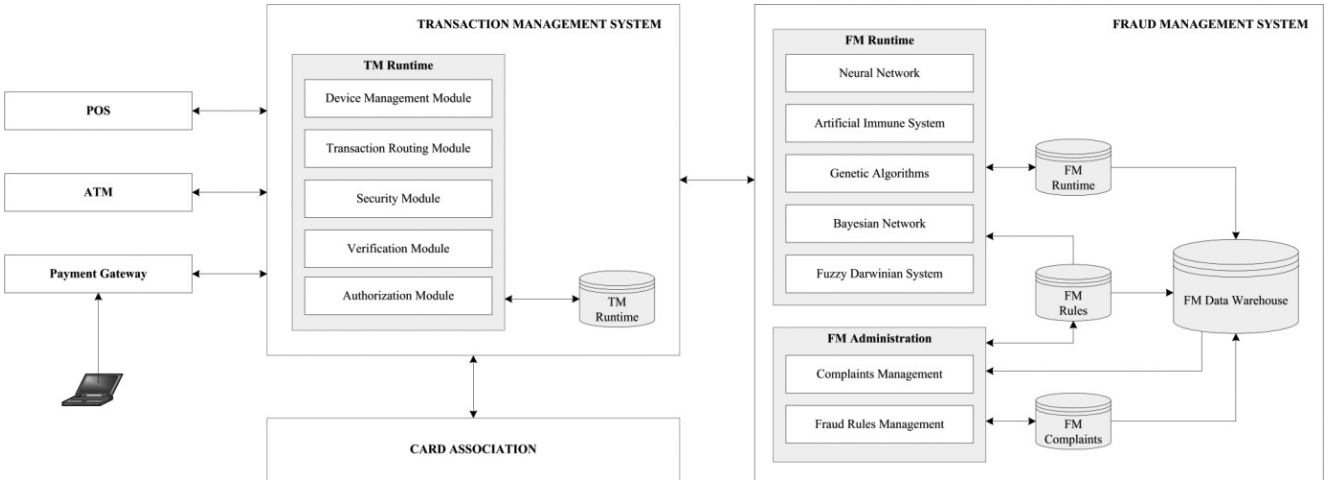
6. PREDLOG REŠENJA

Na slici 3. prikazana je arhitektura rešenja u slučaju kada banka izdavalac kartice, usluge procesiranja transakcije poverava Procerskoj kući, a proveru da li je transakcija *fraud* ili ne poverava svom rešenju koje je ovde predloženo. Dat je predlog rešenja kada su ATM, POS i Internet transakcije (preko *payment gateway* do banke) inicirane na uređajima banke. Na uređajima se mogu koristiti kartice banke izdavaoca –*Issuer*-a ali i kartice drugih banaka izdavalaca.

Komponente sistema:

I Transaction Management System-TMS

1. Transaction management Runtime
   - Ovo je deo TMS koji sadrži više modula koji obrađuju transakciju u *real-time* režimu
2. Device management module
   - Utvrđuje tip uređaja sa kog dolazi transakcija, *ATM; POS*; Internet tj. *payment gateway* i prevodi je odgovarajući format koji je neophodan TMS
3. Transaction Routing Module
   - Na osnovu *BIN*-a (*Bank Identification Number*) određuje kojoj banci pripada transakcija,
   - Vrši validaciju nekih polja, parsiranje transakcije



Slika 3. *Arhitektura i softverski moduli predloženog Fraud Management System-a*

4. Security module
   - Proverava *PIN* i vrši dekripciju kriptovanih elemenata transakcione poruke
5. Verification module
   - Validacija ispravnosti kartice, između ostalog proverava rok važnosti kartice
6. Authorization module
   - Proverava da li ima novca na računu i vrši autorizaciju transakcije
7. TM Runtime Database
   - U ovu bazu se skladište sve transakcije koje se dese, bile one *fraud* ili legitimne
   - Podrazumeva se, da se skladište i transakcije koje su odbijene u nekom od modula TM Runtime

II Fraud Management System

1. FM Runtime modul
   - U ovom modulu su definisani algoritmi za detekciju *fraud*-a i to Bajesove mreže, Neuronske mreže, Veštački imuni sistemi, Genetski algoritmi i Fazi Darvinov algoritam. Ovi algoritmi prepoznaju da li je transakcija *fraud* ili ne, jer oni implementiraju definisana pravila u okviru DB Rules.
2. Fraud management runtime database
   - Ovo je operativna baza podataka sa kojom radi FM RT modul i u kojoj su smešteni svi podaci u vezi transakcija koje su se desile.
3. Fraud management data warehouse database
   - Ovo je baza DW na osnovu koje se mogu donositi odluke i koja služi za prikaz npr.statističkih podataka i detaljnije razmatranje ponašanja vlasnika kartice, a samim tim donošenja odluka da li je transakcija *fraud* ili ne.
4. Fraud management administration
   - Ovaj GUI može da menja parametre i da uvodi nova pravila u FM Rules ili da donosi nove odluke o transakcijama a na osnovu informacija koje dolaze od FM Complaints.
5. FM Rules database
   - U ovoj bazi su smeštena sva pravila definisana za sprečavanje *fraud*-a i njihovim neispunjavanjem se transakcija definiše kao neligitimna i diže se stepen alarma.
   - Tu su definisane vrednosti parametara za ta pravila.
   - Nalaze se prilagođena potrebama banke, Visa-ina pravila
   - Opšta pravila:
     - vezana za lokaciju odakle dolazi transakcija
     - sa koje IP adrese dolazi ako je Internet transakcija
     - koliki je vremenski razmak između dve transakcije
     - tip računa koji se koristi
   - Kontrolna pravila:
     - koji je BIN
     - koji je iznos transakcije
     - vrednosti za AVS, CVV-za kartice sa magnetnom trakom, CVV2, PAN
     - limit korisnika
   - Pravila za merenje operativnog rizika gde se može pratiti:
     - rizik po teritoriji iniciranja transakcije
     - rizik po delatnosti trgovca
     - rizik po finansijskom efektu.
6. FM Complaints database
   - Ukoliko se desi da je neka transakcija izašla iz sistema kao ispravna, a ispostavi se da je došlo do greške u sistemu, odnosno da je ta transakcija *fraud* koji sistem nije prepoznao, neophodno je uneti ispravke u FM DW

III Card Association

1. To su kartične organizacije, koje u rešenju prikazanom u radu, dobijaju transakcije od TMS, koje su inicirane platnom karticom koju ne izdaje banka koja je vlasnik nekog od uređaja (ATM , POS) i dalje ih obrađuju.
2. Kartične organizacije mogu biti:
   - VISA
   - MasterCard
   - Diners.

Koraci kod procesiranja transakcije:

1. Transakcija je inicirana nekim uređajem, ATM, POS, Internet transakcija.
2. DMM utvrđuje sa kog uređaja dolazi transakcija i prevodi je u odgovarajući format TMS.
3. Nakon toga TRM na osnovu BIN-a utvrđuje o kojoj se banci radi i ukoliko je on-us (transakcija sa kartice koju je izdala banka *issuer* za koju se obavljaju procesorski poslovi) on šalje transakciju u FMS da se proveri da li je legitimna ili je *fraud*. U suprotnom ukoliko je transakcija sa kartice koja pripada banci čije poslove procesiranja ne obavlja naš procesor, transakcija se upućuje Kartičnoj organizaciji na dalju proveru.
4. Kad je transakcija stigla u FMS, FM Runtime na osnovu pravila definisanih u FM Rules obrađuje transakciju nekim algoritmom za detekciju *fraud*-a i smešta izvršene transakcije u operativnu bazu FM Runtime.
5. Po izvršenoj transakciji se u *real-time* puni FM Data Warehouse, koji se *update*-uje informacijama i iz FM Complaints.
6. FM Data warehouse na osnovu svih ulaznih tokova, uključujući i čitanje pravila iz FM Rules daje razne vrste izveštaja kojima FM Administration menja korisnička i sistemska pravila, a i rešava problem sumnjivih transakcija u FM Complaints.
7. Nakon obrađene transakcije dobija se odgovor pozitivan ili negativan od FMS.
8. Ukoliko je odgovor pozitivan, transakcija se sa svim neophodnim poljima šalje SM na obradu.
9. Nakon toga se prosleđuje VM.
10. AM vrši autorizaciju transakcije, tačnije proverava da li ima dovoljno novca na računu korisnika i šalje odgovor korisniku u vidu uspešno ili neuspešno obrađene transakcije. A istovremeno ažurira TM Runtime database.

ZAKLJUČAK

Došlo je do veće upotrebe elektronskih platnih sistema, ali i rizika koje oni prouzrokuju. Isto tako danas su sve više u upotrebi platne kartice pri kupovini, a sve manje se koristi gotovina, a sve to iz razloga što raste poverenje u bezbednost ovakvih sistema. Sistemi zloupotreba i krađa se sve više razvijaju, ali su bezbednosne mere za zaštitu od njih sve bolje i savremenije.

Jedan od pravaca budućeg istraživanja je odabir najboljih algoritama koje je potrebno primeniti, za modelovanje *Fraud Management System*-a (FMS) koji će se bazirati na više algoritama. Taj FMS će primeniti ono što je dobro od svakog algoritma primenom metode sinteze rešenja, a sinergističkim pristupom pokušaće da eliminiše nedostatke koje algoritmi pojedinčno imaju. S druge strane, nekada je biometrija u elektronskoj trgovini bila naučna fantastika, a danas je to nešto što je realnost. Danas je najviše u upotrebi primena otiska prsta za utvrđivanje identita korisnika, mada je skeniranje zenice budućnost elektronskih platnih sistema u cilju smanjenja *fraud*-a, a samim tim i finansijskih gubitaka i podizanja nivoa bezbednosti.

PRIZNANJE

Ovaj rad je deo projekta „Multimodalna biometrija u upravljanju identitetom“, finansiranom od strane Ministarstva prosvete i nauke Srbije, broj ugovora TR-32013.

REFERENCE

[1] (Aite Group, 12) Aite Group, Card Fraud in the United States: The Case for Encryption, 2012.
[2] (Al-Furiah, 09) Dr.S.Al-Furiah, L.Al-Braheem, Comprehensive study on methods of fraud prevention in credit card e-payement system, Procedings of iiWAS 2009.
[3] (Beljić, Simić 06) Dejan Beljić, Dejan Simić, “Zaštita elektronskih transakcija na Internetu”, InfoM, časopis za informacione tehnologije i multimedijalne sisteme, Beograd, Br. 18/2006., str. 22-27.
[4] (Benson, 2013) C. Benson, Russian hackers charged in biggest data breach case, 160mn credit card numbers stolen, 25 July 2013, Reuters, preuzeto sa http://rt.com/news/us-hacking-ring-charged-587/
[5] (BIS, 11) Bank for International Settlement-BIS, Basel Committee on Banking Supervision Operational Risk-Supervisory Guidelines for the Advanced Measurement Approaches, jun 2011, preuzeto sa http://www.bis.org/publ/bcbs196.pdf.
[[6] (Bogicevic, 14) M.Bogicevic, I.Milenkovic, D.Simic, “Identity Management – A Survey” , Palgrave Macmillan, Innovative Management and Firm Performance - An Interdisciplinary Approach, ISBN 9781137402226, 2014.
[7] (Economist, 14) The Economist, Skimming Off the Top: Why America has such a high rate of payment-card fraud, 15 February 2014, preuzeto sa http://www.businessinsider.com/why-america-has-such-a-high-rate-of-payment-card-fraud-2014-2
[8] (Godin, 09) D.Godin, TJX suspect indicted in Heartland, Hannafors breaches, 2009, preuzeto sa http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect/.
[9] (Jones, 13) D.Jones, J.F.Finkle, Largest Case Launched After Credit Card Info Stolen From J.C.Penney, Visa Licensee, 2013, preuzeto sa http://www.huffingtonpost.com/2013/07/25/credit-card-stolen-visa_n_3653274.html.
[10] (Kim, 08) Y.Kim, A.Savoldi, H.Lee, S.Yun, S.Lee, J.Lim, Design and Implementation of a Tool to Detect Accounting Frauds, IEEE Computer Society, DOI 10.1109/IIH-MSP.2008.257, 2008.
[11] (Kou, 04) Y. Kou, C. Lu, S. Sinvongwattana, Y.Huang, Survey of Fraud Detection Techniques, Proceedinges of the 2004, IEEE, International Conference on Networking, Sensing and Control, 2004.
[12] (Li, 13) J.Li, X.Zhu, C.F.Lee, D.Wu, J.Feng, Y.Shi, On the aggregation of credit, market and operational risks, Springer, DOI 10.1007/s11156-013-0426-0, 2013.
[13] (Payments Council White Paper, 14) Payments Council White Paper, Card not present fraud-a primer on trends and authenticaton processes, Smart Card Alliance, 2014.
[14] (Riley, 12) B. Riley, Card Fraud Management Systems, CEB TowerGroup , preuzeto sa http://www.fico.com/en/wp-content/secure_upload/Card_Fraud_FICO_CEB_TowerGroup.pdf, 2012.
[15] (Simić, 05) Dejan Simić, “Elektronski sistemi plaćanja i zaštita”, InfoM, časopis za informacione tehnologije i multimedijalne sisteme, Beograd, Br. 15-16/2005., str. 27-31.
[16] (Wagenseil, 14) P. Wagenseil, Neiman Marcus Data Breach FAQ: What to Do Now, 27 January 2014, Tom’s guide, preuzeto sa http://www.tomsguide.com/us/target-neiman-marcus-data-breach-faq,news-18199.html.
[17] (Wilhelm, 04) W.H. Wilhelm, “The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management”, Journal of Economic Crime Management Spring, Volume 2, Issue 2, 2004.
[18] (Zareapoor, 12) M. Zareapoor, K.R.Seeja, M.A.Alam, Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria, International Journal of Computer Applications, volume 52, issue 3, 2012.

Marija Bogićević – Univerzitet u Beogradu - Fakultet organizacionih nauka
Kontakt: marija.bogicevic@fon.bg.ac.rs
Oblast interesovananja: elektronski sistemi plaćanja, zaštita računarskih sistema