Cardholder's Reputation System for Contextual Risk Management in Payment Transactions

Albert Sitek[(✉)] and Zbigniew Kotulski

Institute of Telecommunications of WUT,
Nowowiejska 15/19, 00-665 Warsaw, Poland
asitek@tele.pw.edu.pl, zkotulsk@tele.pw.edu.pl

Abstract. Electronic card payments gained huge popularity mainly because of their simplicity, convenience and processing time. Unfortunately transaction processing rules are constant for every transaction, for example each transaction above some hard limit (50 PLN in Poland) must be authorized with PIN verification. One can notice that such an approach is simple, but is not optimal: that is why Contextual Risk Management systems for payment transactions started to be created. This paper presents a new Cardholder's Reputation System that can be used in Contextual Risk Management Systems. It is flexible thanks to a few parameters and allows to cover all possible transaction processes.

Keywords: Reputation systems · EMV · CVM · Payment systems

1 Introduction

Electronic card payments are getting more and more popular across the world. Only in Poland, there were more than 1 billion transactions performed in Q2.2016 [1]. Electronic payment transactions are performed in compliance with EMV specifications, see [2], the standard that has been firstly proposed by Europay, MasterCard and Visa in 1993. Currently it is promoted by EMVCo which associates all major Payment Card Schemes: Visa, Mastercard, JCB, American Express, Discover and UnionPay. Initially, payment card's data could be read by inserting card to the terminal: in a contact way, according to ISO 7810 specification [3]. Nowadays, Contactless Payment Cards (compliant with ISO 14443 [4]) are gaining huge popularity, especially in some countries like UK, Poland and Turkey. Transaction made with contactless card is 53% faster than a traditional magnetic stripe credit card transaction and 63% faster than using cash [2]. According to the newest report, more than 77% issued cards in Poland have contactless functionality [1]. Recently, thanks to services like Android Pay [5], or Samsung Pay [6], there is emerging trend observed on the market to emulate Contactless Payment Card with the smartphone [7]. Such a functionality is possible thanks to the Host Card Emulation technique (HCE) [8] and smartphones equipped with the Near Field Communication (NFC) interface [9]. Thankfully, contactless card emulated with the smartphone is treated and read as a physical

J. Rak et al. (Eds.): MMM-ACNS 2017, LNCS 10446, pp. 158–170, 2017.
DOI: 10.1007/978-3-319-65127-9_13

one, so no changes are required in the payment infrastructure to support those cards correctly.

Payment transaction, compliant with the EMV specification [10], can be processed in many ways, for example can be authorized on-line (by sending an authorization request to the bank), or locally authorized off-line (by the card). Also cardholder can be verified in a different way, e.g. using PIN On-line (verified by the issuer), PIN Off-line (verified by the card, only for contact EMV), Signature, or NoCVM (no cardholder verification at all). The decision which authorization method and cardholder verification method should be used is being made based on terminal's configuration and data retrieved from the card (encoded on the card by the issuer during its personalization phase). Those parameters are for example:

(a) CVM Limit (Cardholder Verification Method Limit), only for contactless transactions, the amount above which the cardholder must be verified: currently 50 PLN in Poland.
(b) Floor Limit, the amount above which the transaction must be authorized on-line.

Those parameters are constant for every transaction: it means that each cardholder is treated in the same way, no matter what's his history and whole transaction context. Such an approach is simple, but it causes that a lot of transactions are processed "time and user experience-ineffectively". One can imagine that transaction flow could be adjusted to the given cardholder and to particular transaction, based on various factors. It may give a lot of benefits, e.g. shorter transaction processing time, greater cardholder's loyalty, better user experience etc. This issue has been raised for the first time in [11]. In this paper, Sitek proposed a new Cardholder Verification Method: One-time PIN, and decision if this method should be used is made by the issuer, based on transaction context (transaction's time, place, cardholder's history etc.). Unfortunately, the author did not propose any algorithm that could be used to decide whether cardholder verification should be performed or not. Another approach has been proposed in [12]. Authors presented dedicated solution for huge merchants (such as Tesco, Auchan etc.), where historical data are kept on merchant's server. Their architecture assumed that payment terminal, during the transaction, sends contextual information (transaction's amount, location, tokenized card's number etc.) to merchant's server and receives the decision whether it should be authorized on-line or off-line. They also proposed a simple example of algorithm that calculates floor limit for current transaction based on cardholder's reputation, transactions' periodicity factor and transactions' amount stability factor. Unfortunately, their reputation system has a few flaws, for example it is unable to detect the situation where cardholder cancels the PIN Off-line, enters it with success on second attempt, or a transaction with PIN On-line that has been declined because of lack of funds (but PIN has been verified).

In this paper a new cardholder's reputation system has been proposed. It distinguishes all possible transaction processes that are significant for cardholder's reputation, including contact and contactless EMV cards. Moreover, it is open to any customization, because of many parameters. Such a system has been designed to generate single reputation value that could be taken into account (together with other contextual factors, e.g. exact time, location etc.) in dedicated decision system (like [12]) that could produce final verdict, how current payment transaction should be processed.

The rest of the paper is organized as follows: Sect. 2 briefly presents current knowledge regarding reputation systems, Sect. 3 describes presented reputation system based on possible transaction processes, Sect. 4 outlines the way how the proposed system has been verified, Sect. 5 contains tests' results, Sect. 6 summarizes the paper and maps out future work.

2 Reputation Systems

According to Cambridge Dictionary [13], reputation can be defined as follows: *Reputation: the opinion that people in general have about someone or something, or how much respect or admiration someone or something receives, based on past behavior or character.* The concept of reputation can be easily mistaken with trustworthiness. In order to explain the difference between trust and reputation, an example from [14] can be quoted: "I trust you because of your good reputation" or "I trust you despite your bad reputation". Those sentences show, that reputation is only one of the factors that can have an impact on the trust. There can be a situation when relying party has some private knowledge about the trustee (for example some direct experiences), and these factors may overwrite any reputation during decision making. On the other hand, in case of lack of additional information, reputation can have crucial meaning during decision making process. Generally speaking, reputation systems assess the reputation of the user by aggregating the ratings that he received from other users [15]. Based on how reputation values are calculated, reputation systems are divided into a few groups:

- *Arithmetic-based*, where reputation values are calculated as simply sum of positive and negative ratings (e.g. eBay) or an average of all ratings (e.g. Amazon). Advanced models in this category compute a weighted average of all the ratings, where the rating weight can be determined by factors such as distance between rating, age of the rating and current score etc. [16]. The reputation system presented in this paper belongs to this group;
- *Probabilistic approach-based*, where reputation values are calculated by the statistical updating of probability density functions (PDF), see [17];
- *Fuzzy logic-based*: in this group of systems, trust and reputation can be represented as linguistically fuzzy concepts, where the membership functions describe to what degree an agent can be described as trustworthy or not trustworthy, see e.g. [18].

Taking into account how reputation is maintained in whole system, there are two groups of reputation systems: centralized and decentralized. The centralized systems have a central authority being responsible for the collection and storage of user's ratings, and for the calculation of reputation values and their dissemination [19]. Such systems are widely used in e-commerce [20], experts sites [21], etc. The decentralized systems have neither a fixed network topology nor a central authority that can be used to control the entities within the system. Instead of that, each entity is responsible for controlling its data and resources. In these systems, the storage of ratings and calculation of reputation are distributed among the entities within the system [15]. Such systems are used in decentralized environment like Peer-to-Peer Networks [22,23], Mobile Ad-hoc Networks [24,25], Wireless Sensor Networks [26], Multi-agent Systems (MAS) [27,28], etc. One can read a few wide surveys of currently developed trust and reputation system, see for example [14,19,29,30].

3 Cardholder's Reputation System

As mentioned in Sect. 1, presented reputation system covers all possible transactions' flows. In order to illustrate and identify them, the transaction's flow diagram has been created. Figure 1 presents all possible transaction's scenarios that can happen during the transaction. It takes into account both contact and contactless transactions. The diagram shows that each transaction flow can be simplified to a set of answers to the questions written in lozenges. For example, the contactless transaction that has been successfully authorized on-line with on-line PIN verification can be translated into YES|NO|NO|NO|YES|YES|YES|YES|NO. When we change "YES" to "1", and "NO" to "0", this transaction flow can be translated into 100011110. This shows, that each transaction flow can be presented as unambiguous binary string. The same transaction flow can also be presented in more human-readable form as CTLS_PIN_ONL_VRFD_ONL_APPR. Both notations will be used in the rest of this paper.

Each transaction flow has constant rating assigned to it. The set of ratings for all possible transaction flows are parameters of the reputation system. The cardholder's reputation for a forthcoming transaction n can be calculated as weighted average of last N transactions limited to the range $<R_{MIN}, R_{MAX}>$, see Eq. (1). N, R_{MIN} and R_{MAX} are parameters of the reputation system.

$$R_n = \begin{cases} R_{MIN} & \text{if } \overline{R}_{n-i} < R_{MIN} \\ \overline{R}_{n-i} & \text{if } \overline{R}_{n-i} \in \langle R_{MIN}, R_{MAX} \rangle \\ R_{MAX} & \text{if } \overline{R}_{n-i} > R_{MAX} \end{cases}, \; where\, i \in \langle 1, N \rangle. \tag{1}$$

The proposed reputation system assumes that there must be at least N historical transaction stored in the system's database to calculate proper reputation value; otherwise cardholder's reputation is set to 0. Equation (2) shows the proposed formula how to calculate weights for the weighted average computation.

$$w_{Rni} = \frac{1}{2} e^{-\frac{t_n - t_i}{\tau_{RT} * AvgT}} * \mathrm{erfc}(\frac{(n-i-1)*2}{x_d} + x_m), \tag{2}$$

where n is the index of current transaction, i is the index of i-th transaction, t_n is time of current transaction, t_i is time of i-th transaction, $AvgT$ is the average distance between transactions, τ_{RT} is the reputation system parameter (the decay factor), erfc is the Complementary Error Function, x_d is the reputation system parameter (a dispersion parameter of the erfc function), x_m is the reputation system parameter (a concentration parameter of the erfc function [32]).

Equation (2) has been proposed based on a set of experimental simulations. Usage of exponential function assures that historical reputation values will be

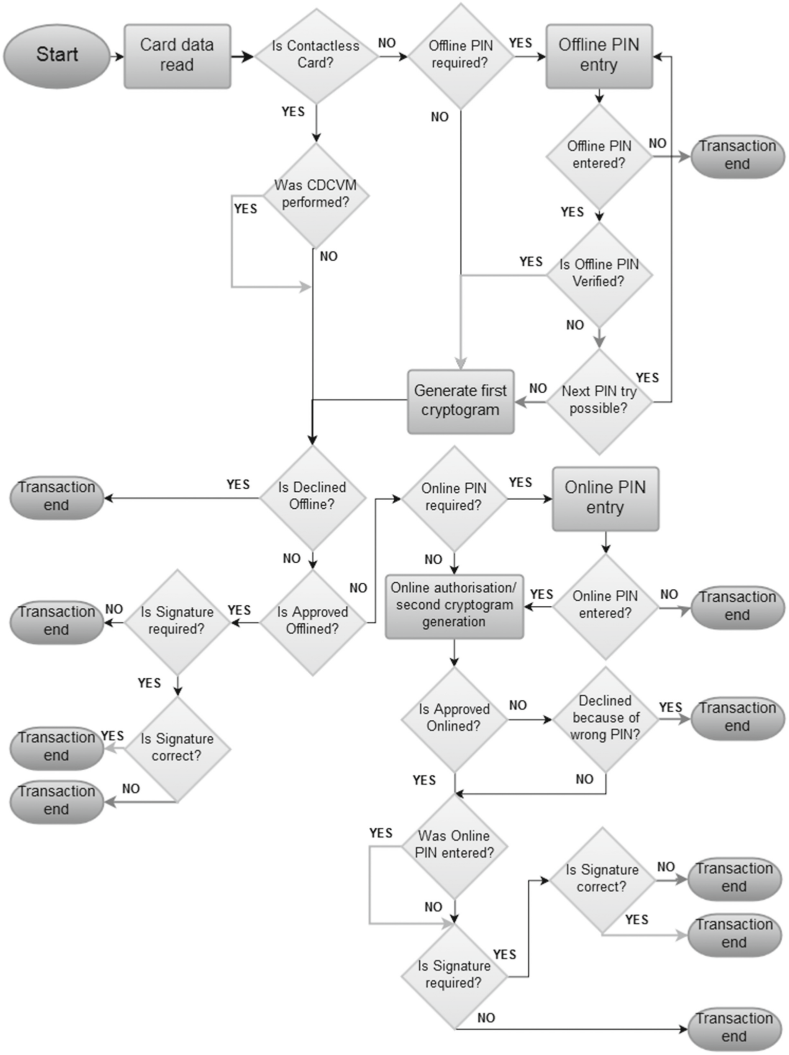

Fig. 1. Transaction's flow diagram

decaying accordingly to distance in time between current and historical transaction. On the other hand, the Complementary Error Function is responsible for decaying accordingly to how many transactions has been made between current and historical transaction.

4 Verification of the Model

In order to verify the reputation system, a lot of simulations need to be performed. The important thing is to select proper simulation software. According to [31], there are currently three options to develop and simulate models: spreadsheets, programming languages and dedicated software. Each of them have pros and cons, but in our opinion, the most suitable option is to simulate proposed model in spreadsheet. Simulating in spreadsheet is fast to develop and has all necessary features [33]. Therefore Microsoft Excel^{TM} 2013 has been used in our tests. In order to share common formulas across a few workbooks, dedicated Add-in has been developed.

As mentioned in previous sections, proposed reputation system has a lot of parameters. On the grounds of numerous simulation iterations, following values has been chosen for further simulations: $N = 5$, $R_{MIN} = -5$, $R_{MAX} = 10$, $\tau_{RT} = 6$, $x_d = 3$, $x_m = -1$. Table 1 presents chosen transaction flow's ratings for simulations, calculated by experts' knowledge, for transactions made according to Fig. 1. A reader must note that not all possible transaction flows has been listed. For example there is no Off-line Authorization for Contact transaction listed, because in real life this authorization method has been disabled in terminals' configuration. Moreover, some transaction flows are very rare, for example CTLS_ONL_APPR_SIG_VRFD (signatures for contactless cards, are uncommon). There are some interesting patterns that can be seen in Table 1:

(a) For PIN on-line: there is no difference whether transaction has been finally accepted or not. The key thing is if it has been declined because of wrong PIN code entered. For example CT_PIN_ONL_VRFD_ONL_APPR = CT_PIN_ONL_VRFD_ONL_DCLD = 7, but CT_PIN_ONL_FAILED = −10,

(b) PIN off-line: can be entered several times, in case of previous attempts appeared incorrect. Presented values assume that if cardholder made a mistake once, and finally transaction was accepted, then his reputation will increase (CT_2ND_PIN_OFFL_VRFD_ONLINE_APPR = 3). But if he made a mistake twice, his reputation will be decreased (CT_3RD_PIN_OFFL_VRFD_ONLINE_APPR = −2),

(c) After transactions, which flows have rating = 0: cardholder reputation for forthcoming transaction will slightly decrease because of decaying features of reputation weights.

Table 1. Chosen transaction flow's ratings

Description	Binary trace	Rating
CT_1ST_PIN_OFFL_VRFD_ONL_APPR	0111000100	7
CT_2ND_PIN_OFFL_VRFD_ONLINE_APPR	011011100100	3
CT_3RD_PIN_OFFL_VRFD_ONLINE_APPR	011011011100100	−2
CT_1ST_PIN_OFFL_CNCD	010	−15
CT_2ND_PIN_OFFL_CNCD	011010	−17
CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
CT_PIN_ONL_VRFD_ONL_DCLD	0000110000	7
CT_PIN_ONL_FAILED	00001101	−10
CT_PIN_ONL_CNCD	000010	−15
CT_ONL_APPR_SIG_VRFD	000001011	5
CT_ONL_APPR_SIG_FAILED	000001010	−10
CT_ONL_DCLD	00000000000	0
CT_ONL_APPR	000001000	0
CTLS_PIN_ONL_VRFD_ONL_APPR	100011110	7
CTLS_PIN_ONL_VRFD_ONL_DCLD	100011100	7
CTLS_PIN_ONL_FAILED	10001101	−10
CTLS_PIN_ONL_CNCD	100010	−15
CTLS_ONL_APPR	10000100	0
CTLS_ONL_DCLD	10000000	0
CTLS_OFFL_APPR	10010	0
CTLS_OFFL_DCLD	101	0

5 Tests' Results

There has been several transaction scenarios proposed to show reputation system's behavior in certain situations. Because of the limitations of this paper, only the most interesting scenarios has been presented. Each test has been described in details in following subsections.

Table 2. Transactions' history before test

Time	Description	Binary trace	Rating
01.03.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
08.03.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
15.03.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
22.03.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
29.03.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7

There is an assumption that before first transaction in given test case, there was constant transactions' history (described in Table 2), so that computation of cardholder's aggregated reputation using Eq. (1) is possible.

Test 1 shows how cardholder's reputation will be rebuilt after unsuccessful on-line PIN verification. Table 3 presents chosen transactions' history to illustrate such a situation.

Table 3. Transactions' history for Test 1

Time	Description	Binary trace	Rating
05.04.2016	CT_PIN_ONL_FAILED	00001101	−10
12.04.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
19.04.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
26.04.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
03.05.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
10.05.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7

Figure 2 shows results of Test 1. First successful transaction after transaction with incorrect on-line PIN causes reputation to increase to the medium level, around 2.7. Only second successful transaction raises the cardholder reputation to satisfactory level, around 8.5. After third transaction, calculated reputation (R Real) is above R_{MAX} parameter, so it is cut away to the R_{MAX} value.

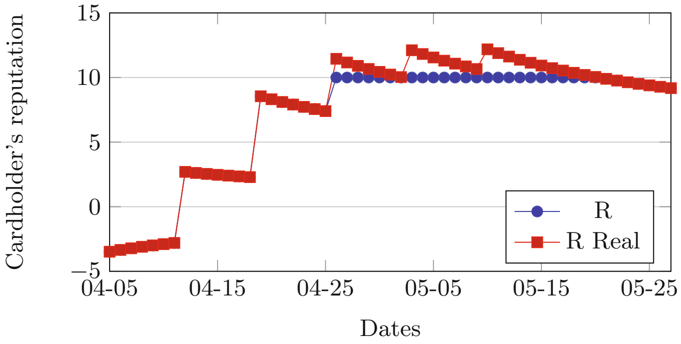

Fig. 2. Aggregated reputation from Test 1

Test 2 shows how cardholder's reputation will be rebuilt after two unsuccessful on-line PIN verifications. Table 4 presents chosen transaction history to illustrate such a situation.

Table 4. Transactions' history before tests

Time	Description	Binary trace	Rating
05.04.2016	CT_PIN_ONL_FAILED	00001101	−10
12.04.2016	CT_PIN_ONL_FAILED	00001101	−10
19.04.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
26.04.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
03.05.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
10.05.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7

As shown in Fig. 3, after two incorrect PIN verifications, calculated reputation drops down dramatically. It reaches level below R_{MIN}, so that R stays at the level of $R_{MIN} = -5$. After first successful transaction, calculated reputation still remains below 0. Only second successful transaction causes reputation to increase, while next successful transaction causes calculated transaction to be cut away to R_{MAX} value. Comparing results of Test 1 and Test 2, one can see that after two successful transactions, cardholder's reputation is set to the similar level, while after first successful transaction reputation in Test 2 is much more lower than in Test 1. This is because of proper values of parameters responsible for decaying old ratings.

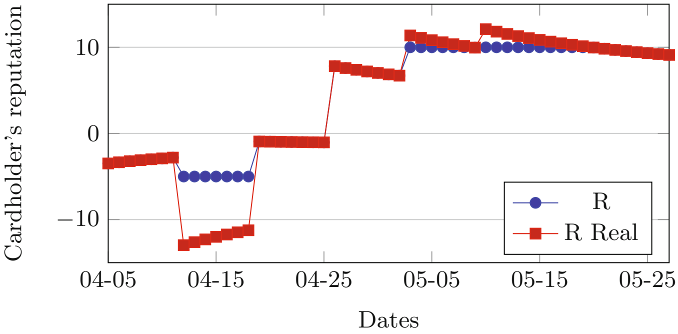

Fig. 3. Aggregated reputation from Test 2

Test 3 shows how good cardholder's reputation will decay because of set of transactions without cardholder verification. Table 5 presents chosen transactions' history to illustrate this scenario.

As shown in Fig. 4, excellent cardholder's reputation will decay completely after three transactions without any verification. Such a transaction may happen because the transaction amount was below CVM Limit, or some Contextual Risk

Management system (like [11,12]) decided to authorize the transaction without verification. Such a behavior is a result of decaying parameters and prevents Contextual Risk Management system from being abused.

Table 5. Transactions' history for Test 3

Time	Description	Binary trace	Rating
05.04.2016	CT_PIN_ONL_VRFD_ONL_APPR	000011110	7
12.04.2016	CTLS_ONL_APPR	10000100	0
19.04.2016	CTLS_ONL_APPR	10000100	0
26.04.2016	CTLS_ONL_APPR	10000100	0
03.05.2016	CTLS_ONL_APPR	10000100	0
10.05.2016	CTLS_ONL_APPR	10000100	0

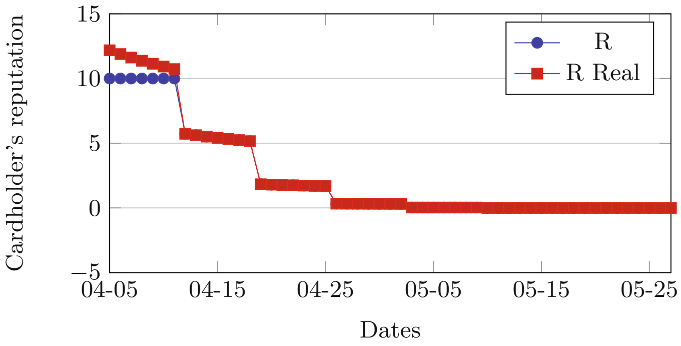

Fig. 4. Aggregated reputation from Test 3

Test 4 presents how presented reputation system will react on transaction canceled on second attempt of entering off-line PIN. Canceling off-line PIN on second attempt means that first attempt has failed and cardholder interrupted the transaction. It may indicate that this was an attempt to perform fraudulent transaction. Table 6 presents chosen transaction history to illustrate such a scenario.

As mentioned before, canceling PIN indicates suspicious behavior so that it is reflected in Fig. 5 correctly. Very good cardholder's reputation will drop down drastically after such a behavior. In this picture one can also see that cardholder's reputation slightly decreased after third transaction because of lack of verification, and it is constantly, slightly decreasing after some period of time without any transaction.

Table 6. Transactions' history for Test 4

Time	Description	Binary trace	Rating
05.04.2016	CTLS_PIN_ONL_VRFD_ONL_APPR	100011110	7
12.04.2016	CT_2ND_PIN_OFFL_CNCD	011010	−17
19.04.2016	CTLS_PIN_ONL_VRFD_ONL_APPR	100011110	7
26.04.2016	CTLS_PIN_ONL_VRFD_ONL_APPR	100011110	7
03.05.2016	CTLS_ONL_APPR	10000100	0
10.05.2016	CTLS_PIN_ONL_VRFD_ONL_APPR	100011110	7

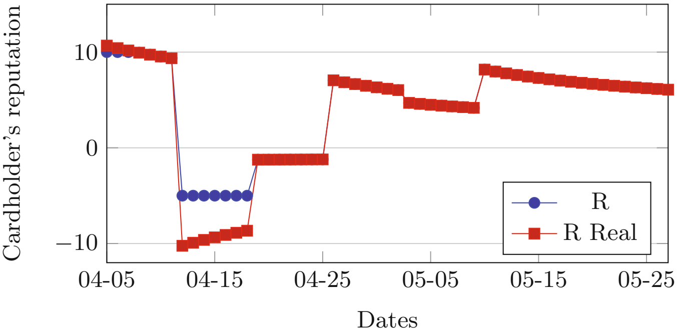

Fig. 5. Aggregated reputation from Test 4

6 Summary and Future Work

In this paper a new Cardholder's Reputation System has been proposed. It covers all possible transaction processes, what has been shown in Fig. 1. It also allows the end user to make some adjustments thanks to plenty of parameters. It is designed to be used in Contextual Risk Management systems like, for example, [12]. Such a system allows to control transaction processing based on various factors, mainly on cardholder's reputation, but also on other, like contextual information: transaction time, transaction amount, actual queue length, etc. The presented system has been validated with success by several simulations performed in the dedicated test environment based on Microsoft Excel$^{\text{TM}}$2013. Additional tests on real transactions' data (taken from one of the retail chain in Poland) are scheduled and will be finished in a few months. One can imagine the Contextual Risk Management System, that decides whether the Cardholder should enter the PIN number, or not. It makes its decision based on cardholder's reputation (calculated using the presented formulas), and some other factors like the Amount Stability Factor (a number indicating how current amount differs from previous ones), the Transaction Periodicity Factor (telling if the Cardholder is a loyal customer and she makes transactions frequently), etc. To prove its commercial applicability, such a system should be tested with production transaction data. In our opinion it is worth to focus future research in that topic.

References

1. Department of Payment System, National Bank of Poland: Information about payment cards 2nd quarter 2016 (2016). (in Polish)
2. EMVCo: EMV Specifications. http://www.emvco.com/specifications.aspx
3. ISO 7810 Specification. http://www.iso.org/iso/catalogue_detail?csnumber=31432
4. ISO 14443 Specification. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=70170
5. Android Pay homepage. https://www.android.com/intl/pl_pl/pay/
6. Samsung Pay homepage. http://www.samsung.com/us/samsung-pay/
7. http://www.bankier.pl/wiadomosc/Eksperci-Platnosci-HCE-to-rynkowy-przelom-3323308.html
8. Host Card Emulation. https://en.wikipedia.org/wiki/Host_card_emulation
9. Near Field Communication. http://nfc-forum.org/what-is-nfc/
10. EMV Transaction Steps. https://www.level2kernel.com/flow-chart.html
11. Sitek, A.: One-time code cardholder verification method in electronic funds transfer transactions. Annales UMCS ser. Informatica, AI **14**(2), 46–59 (2014)
12. Sitek, A., Kotulski, Z.: Contextual management of off-line authorisation in contact EMV transactions. Telecommun. Rev. Telecommun. News 88(84), 8-9, 953–959 (2015). (in Polish)
13. Cambridge Dictionary, definition of "Reputation". http://dictionary.cambridge.org/dictionary/english/reputation
14. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for on-line service provision. Decis. Support Syst. **43**(2), 618–644 (2007)
15. Vavilis, S., Petrovic, M., Zannoe, N.: A reference model for reputation systems. Decis. Support Syst. **61**, 147–154 (2014)
16. Jøsang, A.: Trust and Reputation Systems. Foundations of Security Analysis and Design IV, FOSAD (2007)
17. Ciszkowski, T., Mazurczyk, W., Kotulski, Z., Hoßfeld, T., Fiedler, M., Collange, D.: Towards quality of experience-based reputation models for future web service provisioning. Telecommun. Syst. **51**(4), 283–295 (2012)
18. Damiani, E., Capitani, D., di Vimercati, S., Paraboschi, S., Pesenti, M., Samarati, P., Zara, S.: Fuzzy logic techniques for reputation management in anonymous peer-to-peer systems. In: Proceedings of the Third International Conference in Fuzzy Logic and Technology, Zittau, Germany (2003)
19. Koutrouli, E., Tsalgatidou, A.: Reputation systems evolution survey. ACM Comput. Surv. **48**, 3 (2015). Article 35
20. Resnick, P., Zeckhauser, R.: Trust among strangers in internet transactions: empirical analysis of ebay's reputation system. In: The Economics of the Internet and E-Commerce, vol. 11 of Advances in Applied Microeconomics. Elsevier Science (2002)
21. Costagliola, G., Fuccella, V., Pascuccio, F.A.: Towards a trust, reputation and recommendation meta model. J. Vis. Lang. Comput. **25**, 850–857 (2014)
22. Gupta, M., Judge, P., Ammar, M.: A reputation system for peer-to-peer networks. In: NOSSDAV 2003, 1–3 June 2003, USA (2003)
23. Buchegger, S., Le Boudec, J.-Y.: A robust reputation system for P2P and mobile ad-hoc networks. In: Workshop on Economics of Peer-to-Peer Systems (2004)
24. Sen, J.: A distributed trust and reputation framework for mobile ad hoc networks. In: Third International Conference (CNSA 2010), Chennai, India, 23–25 July 2010 (2010)

25. Srinivasan, A., Teitelbaum, J., Liang, H.: Reputation and trust-based systems for ad-hoc and sensor networks. In: Boukerche, A. (ed.) On Trust Establishment in Mobile Ad-Hoc Networks. Wiley, New York (2007)
26. Roman, R., Fernandez-Gago, M.C., Lopez, J.: Trust and reputation systems for wireless sensor networks. In: Security and Privacy in Mobile and Wireless Networking, pp. 105–128 (2009)
27. Sabater, J., Sierra, C.: Reputation and social network analysis in multi-agent systems. In: First International Joint Conference on Autonomous Agents and Multiagent Systems, pp. 475–482 (2002)
28. Pujol, J.M., Sanguesa, R., Delgado, J.: Extracting reputation in multi agent systems by means of social network topology. In: The First International Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS 2002), 15–19 July (2002)
29. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for Internet of Things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
30. Noorian, Z., Ulieru, M.: The state of the art in trust and reputation systems: a framework for comparison. J. Theor. Appl. Electron. Commer. Res. **5**(2), 97–117 (2010). doi:10.4067/S0718-18762010000200007. Talca ago
31. Robinson, S.: Simulation: The Practice of Model Development and Use. Palgrave Macmillan, London (2014)
32. Kotulski, Z., Szczepinski, W.: Error Analysis with Application in Engineering. Springer, Dordrecht (2010)
33. Seila, A.F.: Spreadsheet simulation. In: Winter Simulation Conference, California, USA (2006)