1-1-2019

An empiric path towards fraud detection and protection for NFC-enabled mobile payment system

Pinki Prakash Vishwakarma

Amiya Kumar Tripathy
Edith Cowan University, a.tripathy@ecu.edu.au

Srikanth Vemuru

10.12928/TELKOMNIKA.v17i5.12290
Vishwakarma, P. P., Tripathy, A. K., & Vemuru, S. (2019). An empiric path towards fraud detection and protection for NFC-enabled mobile payment system. *Telkomnika, 17*(5), 2313-2320. https://doi.org/10.12928/TELKOMNIKA.v17i5.12290

TELKOMNIKA, Vol.17, No.5, October 2019, pp.2313~2320
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i5.12290

An empiric path towards fraud detection and protection for NFC-enabled mobile payment system

Pinki Prakash Vishwakarma*[1], Amiya Kumar Tripathy[2], Srikanth Vemuru[3]
[1,3]Department of Computer Science and Engineering, K. L. E. Foundation, Andhra Pradesh, India
[2]Department of Computer Engineering, Don Bosco Institute of Technology, Mumbai, India
[2]School of Science, Edith Cowan University, Perth, Australia
*Corresponding author, e-mail: vishwakarmapp@gmail.com

Abstract

The synthesis of NFC technology accompanying mobile payment is a state-of-the-art resolution for payment users. In view of rapid development in electronic payment system there is rise in fraudulent activity in banking transactions associated with credit cards and card-not-present transaction. M-Commerce aid the consumers and helps to bestow real-time information in payment system. Due to the familiarization of m-commerce there is cogent increase in the number of fraudulent activities, emerging in billions of dollar loss every year worldwide. To absolute the security breaches, payment transactions could be confined by considering various parameters like user and device authentication, consumer behavior pattern, geolocation and velocity. In this paper we formally assay NFC-enabled mobile payment fraud detection ecosystem using score-based evaluation method. The fraud detection ecosystem will provide a solution based on transaction risk-modeling, scoring transaction, business rule-based, and cross-field referencing. The score-based evaluation method will analyze the transaction and reckon every transaction for fraud risk and take pertinent decision.

Keywords*: fraud detection ecosystem, fraud prevention, mobile payment system, near field communication, score-based evaluation*

1. Introduction

Near Field Communication Technology assist the progress of mobile phone being used by billions of people all over the world for payment application [1, 2]. The synthesis of NFC technology accompanying mobile payment is a state-of-the-art resolution for payment users. Mobile phones used for communication, is also a payment instrument for performing financial transactions. NFC technology assists mobile payments using mobile phones to carry contactless payment transactions [3, 4]. In electronic payment system cashless transaction have a definite change in economic growth nevertheless, provide a scope for fraud. The growth in cashless payment sustains progress in Information Communication Technology (ICT) and smart phones [5]. In view of rapid development in electronic payment system there is rise in fraudulent activity in banking transactions associated with credit cards and card-not-present transaction [6].

To absolute the fraud in NFC-enabled mobile payment for an initiated transaction execution depends on various factors like velocity, geolocation, user and device authentication and consumer behavior pattern. Mobile banking elucidates the banking activities being carried out by virtue of mobile phone. The incursion of mobile phones has elevated usage of banking activities [7]. The way of access that is conducive and mobility in today's digital world has made people to spend more time on internet, smartphone. However, people use smart phone's to imperforate their mobile banking activities which in turn results in fraudulent activities. Understanding the denotation and ambit of security in mobile commerce for information systems is must. There is a need to impart consumer protection from fraud. Though fostering information systems from illegitimate access and the mobile banking activity that uses furtive process are an issue.

As consumers are espousing digital decorum at the same time mobile commerce is maturing across the world. The capability to accomplish payment transaction to be completed successfully with abatements provided on transactions finished through mobile apps bestow

Received January 12, 2019; Revised April 15, 2019; Accepted May 9, 2019

towards this development. M-Commerce aid the consumers and helps to bestow real-time information in payment system [7]. Due to the familiarization of m-commerce there is cogent increase in the number of fraudulent activities, emerging in billions of dollar loss every year worldwide [8, 9]. In peer to peer mode, the two NFC phones in close proximity can exchange data with each other [10].

In NFC-enabled mobile payments the consumer needs to tap their NFC mobile phone in front of the m-POS to make a purchase. Consumers find mobile payments more convenient and user friendly as the debit/credit cards are emulated in their mobile phone. Thereupon, it becomes easy for consumers to make purchase without carrying physical wallet or cards with them. A consumer's discernment about the security of payment instrument i.e. mobile phone being used for purchase is dependent on the volume and amount of transaction being performed.

The NFC devices do not bestow generic security protocol nevertheless, consent to the application definite performance is imperative [11]. The concernment of security in mobile payment system articulate that consumers by no means want to avow their payment credentials in view of increasing online frauds [12]. Fraud analytic embodies fraud detection and fraud prevention. Fraud detection should identify fraud instantly as soon as it gets impale while fraud prevention should include several measures to stop fraud from happening [13, 14]. Therefore, considering other parameters like velocity, user and device authentication, consumer behavior and double spending attack is essential to detect fraud.

Consumer behavior profile by behavioral advertiser's leg-up crucial privacy concern and personal data of mobile phone users. Therefore, consumer protection and privacy regulation should forbid unfair or deceptive business practices [15]. To secure payment transaction in mobile payments tokenization process is used. The tokenization process replaces a sensitive data i.e. primary account number of the consumer with a random number generated which is referred to as payment token. The tokenization process emanates as a neoteric fence facing fraud in mobile payments [16, 17]. Layered approach fraud detection and prevention solution must environ user and device authorization, data attribute analysis, consumer behavior analysis, fraud analytic engine and output of transaction execution [18].

2. Research Method

2.1. Related Work

In view of intricate constitution of finance services, fraud analytic inside the financial industry facade an ineluctable question. The security of electronic payment systems inheres card-present transactions which manifest deficiency in securing offline authentication method and appraisement of card-not-present transaction access. Therefore, it should evince to reinforce security of financial transactions in pursuance of user security, privacy, anonymity and execution. There are very few papers about fraud detection in NFC-enabled mobile payment system. Most published work concern about credit card fraud detection and online banking fraud. Prior fraud detection and prevention investigation aim attention at statistical models, machine learning and artificial intelligence [19].

Demiriz and Ekizoğlu proposed rule-based method for fraud detection and prevention using location data which can prevent financial loss [20]. Using only location data as an analysis parameter is not robustious for fraud detection and fraud prevention. Considering perpetual development of fraudulent patterns in payment system, rule-based detection methods are obsolete [21]. Thence, there is a requisite for real-time transaction audit and decision-making engine to identify fraud conjoined with multifactor authentication.

Anomaly detection uses behavior profiles to detect new patterns that detour from the behavior profiles. Alike, the detouring behavior patterns can be added to the existing behavior profile [22]. Mobile payment model based on precise and habitual consumer behavior pattern that, detour from such behavior patterns perchance fraudulent or suspicious [23]. Benmakrouha et al. to elucidate consumer behavior profile, transaction amount and time of shopping is thought-out as inputs and output is suspicious but the model have yet to be developed and tested with real data. Data mining techniques for fraud detection in credit card management based on customer behaviors can improve performance concerning accuracy and sensitivity [24].

A multifactor authentication system was proposed to which knowledge factor is a 4-digit pin, possession factor is NFC-enabled Smartphone and inherence factor is the face of the user [25]. Moreover, pattern matching techniques are not commensurable to identify fraudulent transaction [26]. In order to detect fraudulent transaction risk point calculation method is proposed [27], a malware forensics technique to detect malicious programs and pharming was recommended thereby, protecting the user while performing electronic financial transaction. In mobile payment system hiding consumer's identity plays an important role, as consumers choose to bide unidentified considering privacy and security issues [28].

Sänger et al. presented a study to detect fraud in online reputation system and malicious seller behavior. The study was based on eBay's feedback profile and limited to context-based attacks [29]. A hybrid model for customer credit scoring based on amalgamation of HMM and GMDH measures customer credit risk. However, the average accuracy and AUC performance measure of the hybrid model can be further improved [30]. Nonetheless, a distinct transaction is not feasible to determine fraud and the determination has to examine historic behavior of the consumer. In reality fraud detection concerns little defiance, viz. less number of transactions considered for fraud examination, consumer behavior progress, fraudsters change plan of action over a time and number of legitimate transactions exceeding number of fraudulent transactions. Howbeit majority of fraud detection algorithms do not reckon on real-time fraud detection systems.

Machine learning techniques used in fraud detection sometimes reject genuine transactions as the algorithms are not custom-made to the usual consumer behavior pattern. Machine learning algorithms are based on the input data if, inapplicable data is given to the algorithm it learns wrong things and it becomes difficult to identify fraudulent/suspicious/ legitimate transaction. Popular fraud management systems rest on business rules feel necessity for manual reviews and then the time from transaction initiation to execution takes longer. Data mining techniques also suffer from overfitting, imbalanced class problem. Unsupervised techniques for fraud detection have a lower accuracy than that of supervised techniques.

2.2. Description of NFC-Enabled Mobile Payment Fraud Detection Ecosystem

To prevent fraudulent transaction, we propose an NFC-enabled mobile payment fraud detection ecosystem. The fraud detection engine comprises data analysis and knowledge engine as shown in Figure 1.

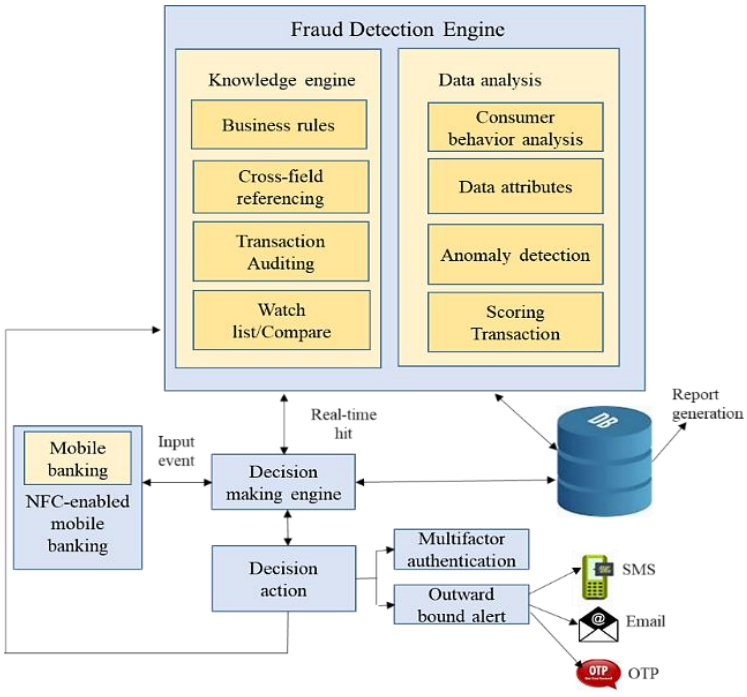

Figure 1. NFC- enabled mobile payment fraud detection ecosystem

2.2.1. Data Analysis

The inputs for the fraud detection ecosystem are device fingerprint, velocity, geolocation, transaction details and consumer details. The device fingerprint information (IMEI, mobile number) is sent along with geolocation information to the fraud detection engine. For geolocation the rules can be applied to the country, state or city. The velocity entity determines the threshold for the transaction amount (limit of transaction) and the number of transactions to be carried out. For velocity the rules can be defined for the volume (small amount and large amount) a threshold value is set the transaction execution e.g. three transactions only. The mobile device identification is by IMEI and mobile number information. Consumers tend to change their mobile device over a period. If a consumer device is not registered evaluate it for a unique behavioral pattern correlate with the risk/fraud and bestow an advice based on the business rules described. The mobile device with high score is considered more reliable, may be allowed for further processing. The devices with low score may be denied or deteriorated for manual review i.e. combination of OTP and Transaction PIN.

The spending pattern database of each consumer is created based on his/her spending habits. Thence, the spending habit is conjoining to the attributes like velocity, geolocation and merchant, is ascribing as normal or abnormal behavior. The transaction initiated for payment will be matched with the spending pattern database of the respective consumer behavior pattern if the pattern matches then the user is genuine user. Erstwhile, it may happen that the consumer behavior is abnormal but the consumer is a legitimate user. In this case it will go for OTP and transaction PIN verification. The historical behavior data of known fraud can be used to determine fraudulent patterns.

In anomaly detection, it identifies the discrepancy from the normal pattern which is based on the transaction monitoring values and generates outward bound alert. Anomalies like geolocation, time zone and geolocation discrepancy must avow to check suspicious transaction. The transaction is scored to access the level of risk. The higher score yields authentic, allow proceeding for further transaction processing whereas lower score may automatically deny or deteriorate for manual review. If the transaction score is negative, then it is considered to be fraudulent transactions and the outward-bound alert system authenticates the user by automatically fetching the OTP send to the user mobile along with the transaction pin entered by the user. Scoring of transaction makes use of score evaluation method.

The evaluation method uses a count variable to which a value is assigned after each attribute matching. The negative value is assigned whenever the attribute values are not matched and a positive value is assigned whenever attribute values are matched. Based on this count value analysis the consumer will be detected as legitimate user if the transaction score is greater than zero i.e. positive value. The consumer will be detected as fraudster/suspicious if the transaction score is less than zero i.e. negative value. If the transaction is detected as suspicious that is few attributes are matched, then it proceeds for OTP and transaction PIN for successful payment.

2.2.2. Knowledge Engine

The knowledge engine does a risk assessment on the payment transaction initiated. Howbeit, risk assessment takes into consideration business rules, cross-field referencing, transaction monitoring and watch list/compare to analyze the payment transaction. The business rules defined is the substantial tool used to identify or stop fraud. Single rule or amalgam rules are built for fraud detection. The rules are defined to percolate fraudulent transactions and suspicious behavior. Examples can be transactions carried out at odd hours, low velocity attack that deceive to colossal amount of loss. Describing deliberately consumer behavior authorize the fraud engine to detect the fraud sooner and decide on transaction processing. The cross-field referencing can expose more sophisticated fraud faster. Moreover, it correlates the attributes to find fraudulent patterns. Example can be cross-field like device browser language and geolocation is used to detect fraud. The preferences for cross-field searches are saved for future investigation. The post facto monitoring comprehends real time transaction monitoring and step-up alert if any fraudulent pattern identified. An early warning system detects the behavior before the actual fraud happens thereby, enabling fraud prevention.

The watch list/compare has the device fingerprint information as well the transaction information. A genuine and denial list is made for comparison purpose to manifest fraud.

Example is the device fingerprint information and geolocation can be compared with the watch list to manifest fraud. Double spending attack is performed by considering the same amount of money to be transacted more than once in a given period time. Detection of double spending attack is done by considering the same amount of money to be processed more than once in a given period.

3. Results and Analysis

3.1. Score based Evaluation

When the consumer initiates the payment transaction, the relevant attributes with respect to transaction are captured, consumer behavior pattern is matched. Subsequently, the next two parameters considered are geolocation and velocity, for geolocation currently the radius is set to 5 km which can be changed as per user spending behavior and velocity is set as large amount and small amount [16]. The small amount does not require user permission for further processing while large amount requires user permission as the payment amount is large. Then the fraud detection engine performs transaction scoring.

Scoring of transaction uses score-based evaluation method to analyze the transaction. Based on transaction score the consumer is detected as legitimate or fraudulent. Whenever a consumer initiates a transaction for payment, the behavior of the consumer is matched with the historic behavior pattern of the same consumer stored in the database. For each attribute match a score is assigned. The positive score is assigned for each attribute match, at the same time a negative score is assigned for each unmatched attribute and summed up to give a final score.

The data attributes a and ai as mentioned in (1) and (2) considered for transaction processing initiated by the consumer are device fingerprint (mobile number, IMEI, browser language), geolocation, velocity, transaction start date timestamp, transaction end date timestamp, transaction pin, merchant ID, payment token and consumer behavior pattern (normal/abnormal). The consumer behavior pattern b as referred in (1) and (2) target the espied characteristics of the consumer who they are and also regularly consumer behavior profiling i.e. spending pattern of the consumer.

Scoring of transaction is a mathematical model, by virtue of what based on the consumer behavior pattern determines whether transaction request is from a legitimate user or suspicious/fraudulent user. Thence, compute the score of the payment transaction t to the consumer behavior pattern b considering the data attributes a.

$$\text{Transaction Score} = \sum_{a \in t} s\,(a, b) \quad (1)$$

The impression behind the matching attributes is that it should count number of matched attributes and number of unmatched attributes. Based on this precept, we define the score of payment transaction s as

$$s\,(a, b) = \sum_{i=1}^{11} ai \quad (2)$$

Score based evaluation reckon every transaction for fraud risk and take pertinent decision. Throughout the payment transaction screening method an efficacious mobile payment fraud detection assures that the geolocation, velocity, device fingerprint etc. all be encountered and scored relevantly. The score is calculated as shown in (2). If the transaction does not match the historic behavior pattern of the consumer and the transaction score is positive, then the transaction is added as a new behavior to the behavior pattern of the consumer. Sometimes it may happen that genuine transactions may be detected as suspicious transaction owing to the transactions that aren't be spoken to the consumer behavior pattern.

3.2. Consumer Behavior Analysis and Transaction Analysis

Ensuing the behavioral patterns allows you to learn who the real user is in the background of the mobile payment system. If the spending behavior of the consumer is same every time with respect to the attributes like velocity, geolocation, device etc. we can affirm it as a genuine user and the behavior is termed as a normal behavior. Any substantial variation from the threshold in the normal behavioral pattern is found as an abnormal behavior.

In NFC-enabled mobile payment system the consumer mobile device is thought-out as the initiator device which initiates the payment process whereas the m-point of sale terminal is the merchant's device known as the target device. The consumer initiates payment transaction with NFC-enabled mobile phone touching on the mPOS terminal. The mobile point of sale (mPOS) allows the mobile phone to carry out a payment transaction instead of NFC-enabled point of sale terminal. Because of high cost and unavailability of NFC-enabled POS terminal we have used mPOS for our experiment study.

The data attributes for fraud detection conjoined with false positives are geolocation, velocity, device fingerprint, consumer behavior pattern, transaction pin, merchant id, payment token, transaction start date and transaction end date. Lamentably, it is implausible that a single attribute or technology will pay off zero false positives. Therefore, amalgamation of all the data attributes used for fraud identification results in a low false positive rate.

3.3. Evaluation of Fraud Detection System

In our experimental study, we obtain the evaluation of the proposed fraud detection ecosystem resting on low false positive rate. The consumers and their devices are registered to the mobile payment application in order to perform a payment transaction. When the fraud detection system characterizes an input transaction, one of the happening circumstances originate. The circumstances for fraudulent transactions used are:

- True positive (TP), legitimate transaction is identified as being legitimate.
- True negative (TN), a fraudulent transaction is being identified as fraudulent.
- False positive (FP), not fraudulent transaction is identified as fraudulent.
- False negative (FN), fraudulent transaction is identified as being legitimate.

The accuracy of the transaction score is described to outperform both a legitimate user and the suspicious/fraudulent user. The sensitivity measure refers to the true positive rate whereas the specificity measure refers to the true negative rate [22].

$$\text{Accuracy} = TP+TN/n \quad (3)$$

$$\text{Specificity} = TN/FP+TN \quad (4)$$

$$\text{Sensitivity} = TP/FN+TP \quad (5)$$

$$\text{False Positive Rate} = FP/TN+FP \quad (6)$$

The total transaction n recorded are 580; false positive rate is 6.89 percent. Thus, the accuracy of the proposed system calculated comes to 96.55 percent. Nevertheless, the efficiency of the system depends on the accuracy measure.

4. Conclusion

Fraud detection for mobile payments have been an important task for banks, merchants and consumers. The financial institutions are combating a viable risk of mobile payments fraud. As a result, real-time based fraud detection of transaction is desired to ease fraud risk to fence fraudulent transactions. Financial institutions are under encumbrance to keep low false positive rate at the same time sustaining fraud strength. Thus, in our proposed system the real-time based fraud detection house facet akin, real time transaction auditing, real time decision-making engine, consumer behavior analysis and multifactor authentication.

The formal security analysis is concluded by identifying a fraudster based on amalgamation of parameters like user and device authentication, consumer behavior pattern, velocity and geolocation. However, the multifactor authentication in fraud detection and prevention lead to better accuracy in mobile payment system and score based evaluation used yields a low false positive rate. Finally, we substantiate the proposed system with a good accuracy of 96.55 percent thereby preventing fraudsters to perform fraudulent transactions. Thereupon, it is analytical to identify the fraudulent transaction more precisely than the legitimate transactions.

References

[1] V Coskun, B Ozdenizci, K Ok. A survey on Near Field Communication (NFC) Technology. *Wireless Personal Communications.* 2013; 71(3): 2259-2294.

[2] Bangdao C, AW Roscoe. Mobile Electronic Identity: Securing Payment on Mobile Phones. In: Ardagna CA, Zhou J. *editors.* Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication. LNCS, Springer, Berlin, Heidelberg. 2011; 6633: 22-37.

[3] N Akinyokun, V Teague. *Security and Privacy Implications of NFC-enabled Contactless Payment Systems*. Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES), Article No. 47, Reggio Calabria, Italy. 2017.

[4] J Ondrus, Y Pigneur. Towards a holistic analysis of mobile payments: A multiple perspectives approach. *Electronic Commerce Research and Applications.* 2006; 5(3): 246-257.

[5] H Tee, HB Ong. Cashless payment and economic growth. *Financ Innov.* 2016; 2: 4.

[6] F Ghobadi, M Rohani. *Cost sensitive modeling of credit card fraud using neural network strategy*. 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS). Tehran, Iran. 2016: 1-5.

[7] Turban E, King D, Lee JK, Liang TP, Turban DC. Electronic Commerce Payment Systems. *Electronic Commerce. Springer Texts in Business and Economics. Springer, Cham.* 2015: 519-557.

[8] RF Lima, ACM Pereira. *A Fraud Detection Model Based on Feature Selection and Undersampling Applied to Web Payment Systems*. International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT). IEEE/WIC/ACM, Singapore. 2015: 219-222.

[9] Pozzolo AD, Caelen O, Borgne YL, Waterschoot S, Bontempi G. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications.* 2014.

[10] SK Timalsina, R Bhusal, S Moh. *NFC and its application to mobile payment: Overview and comparison*. 8th International Conference on Information Science and Digital Content Technology (ICIDT2012), Jeju. 2012: 203-206.

[11] M Roland, J Langer. Comparison of the usability and security of NFC's different operating modes in mobile devices. *Elektrotechnik & Informationstechnik.* 2013; 130(7): 201-206.

[12] SY Dauda, J Lee. Technology adoption: A conjoint analysis of consumers′ preference on future online banking services. *Information Systems.* 2015; 53: 1-15.

[13] T Allan, J Zhan. *Towards Fraud Detection Methodologies*. 5th International Conference on Future Information Technology. Busan, South Korea. 2010: 1-6.

[14] Y Wang, C Hahn, K Sutrave. *Mobile payment security, threats, and challenges*. Second International Conference on Mobile and Secure Services (MobiSecServ). Gainesville, FL, USA. 2016: 1-5.

[15] NJ King, PW Jessen. Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones–Part I. *Computer Law & Security Review.* 2010; 26(5): 455-478.

[16] P Vishwakarma, AK Tripathy, S Vemuru. A Hybrid Security Framework For Near Field Communication Driven Mobile Payment Model. *International Journal of Computer Science and Information Security.* 2016; 14(12): 337-348.

[17] Vishwakarma PP, Tripathy AK, Vemuru S. The Fact-Finding Security Examination in NFC-enabled Mobile Payment System. *International Journal of Electrical and Computer Engineering (IJECE).* 2018; 8(3): 1774-1780.

[18] Vishwakarma PP, Tripathy AK, Vemuru S. A Layered Approach to Fraud Analytics for NFC-Enabled Mobile Payment System. In: Negi A, Bhatnagar R, Parida L. *editors.* Distributed Computing and Internet Technology. ICDCIT 2018. Lecture Notes in Computer Science, Springer. 2018; 10722.

[19] J West and M Bhattacharya. Intelligent financial fraud detection: A comprehensive review. *Computers & Security.* 2016; 57: 47-66.

[20] A Demiriz, B Ekizoğlu. *Using location aware business rules for preventing retail banking frauds*. First International Conference on Anti-Cybercrime (ICACC). Riyadh, Saudi Arabia. 2015: 1-6.

[21] D Preuveneers, BavoGoosens, W Joosen. *Enhanced fraud detection as a service supporting merchant-specific runtime customization*. Proceedings of the Symposium on Applied Computing. ACM, Marrakech, Morocco. 2017: 72-76.

[22] J Han, M Kamber. Data Mining Concepts and Techniques. Second Edition. San Francisco, CA: Morgan Kaufmann. 2006.

[23] F Benmakrouha, C Hespel, E Monnier. *An algorithm for rule selection on fuzzy rule-based systems applied to the treatment of diabetics and detection of fraud in electronic payment*. International Conference on Fuzzy Systems. Barcelona, Spain. 2010: 1-5.

[24] A Charleonnan. *Credit card fraud detection using RUS and MRN algorithms*. Management and Innovation Technology International Conference (MITicon). Bang-San, Thailand. 2016: 73-76.

[25] A Adukkathayar, GS Krishnan, R Chinchole. *Secure multifactor authentication payment system using NFC*. 10th International Conference on Computer Science & Education (ICCSE). Cambridge, UK. 2015: 349-354.

[26] C Kier, G Madlmayr, A Nawratil, M Schafferer, C Schanes, T Grechenig. *Mobile Payment Fraud: A Practical View on the Technical Architecture and Starting Points for Forensic Analysis of New Attack Scenarios.* Ninth International Conference on IT Security Incident Management & IT Forensics. Magdeburg, Germany. 2015: 68-76.
[27] AC Kim, S Kim, WH Park, DH Lee. Fraud and financial crime detection model using malware forensics. *Multimedia Tools and Applications.* 2014; 68(2): 479-496.
[28] S Almuairf, P Veeraraghavan, N Chilamkurti, DS Park. Anonymous proximity mobile payment (APMP). *Peer-to-Peer Networking and Applications.* 2014; 7(4): 620-627.
[29] J Sänger, N Hänsch, B Glass, Z Benenson, R Landwirth, MA Sasse. *Look before You Leap: Improving the Users' Ability to Detect Fraud in Electronic Marketplaces*. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. San Jose, California, USA. 2016: 3870-3882.
[30] GE Teng, CZ He, J Xiao, XY Jiang. Customer credit scoring based on HMM/GMDH hybrid model. *Knowledge and Information Systems.* 2013; 36(3): 731-747.