Authentication using Robust Primary PIN (Personal Identification Number), Multifactor Authentication for Credit Card Swipe and Online Transactions Security

S.Vaithyasubramanian
Department of Mathematics
Sathyabama Institute of Science and Technology
Chennai, India

***Abstract*—In view of effectiveness, ease of access and profitability, the advancement in e-Commerce is an immense step in forward. The development is went with further unusual vulnerabilities to worry. The significant issue all through the world in credit card management is credit card fraud. Because of extortion and fraudsters persistently look for better approaches to confer unlawful activities the organizations, users and establishment finds tremendous loss yearly. In the common Credit Card extortion process, fraudulent transaction will be distinguished only after the transaction is finished. In recent Studies, the security of Credit Card Transaction from unauthorized admittance or usage are addressed by diverse access control methods. This paper illustrates a new scheme of Authentication using Primary PIN and Multifactor authentication to secure credit card transactions.**

***Keywords*—Credit card fraud; online transaction; card swipe transaction; Personal Index Number (PIN); Card Verification Value (CVV); One Time Password (OTP); Primary Personal Index Number; security**

I. Introduction

In the present eventful and digital world with the advancement in electronic commerce it is convenient for customers to buy goods and utilities by sitting in front of computers. Nowadays customers are buying their essentials and desired commodities through various online sellers. For the payment mostly they use credit cards or online transactions. The increase in usage of credit card transactions manage to pay for added chance for offenders to steal credit card credentials and as a result executing fraudulent. At the point when banks lose cash in view of Credit Card misrepresentation, cardholders pay for the greater part of that misfortune through higher loan fees, higher expenses and decreased advantages. Henceforth, it is in both the service provider banks and the cardholders hand to diminish ill-conceived utilization of charge cards by early extortion location [1, 2].

In the most recent years credit card payment has grown-up rapidly. The Popular and Common mode of payment for any mode of purchase are mostly by credit card. Issue with making business through online is the transaction can be made without the presence of the cardholder or card. It is in this manner unimaginable for the vendor to ensure the consumer is the authenticated cardholder or not. In spite of this enormous popularity the cards are not free of risk. e-Commerce turned today's trade either entire or part of their business popular and to reach peoples economical and reliable. User-friendliness, better efficiency, manageability and services allows the customers to use credit card for purchases regardless of location, time and credit amount over the desk [3, 4].

The most acknowledged mode of shopping at shops and in online over the world in this day is by credit card transaction. It give cashless at the time of transaction and appropriate approach to do shopping online, paying bills and performing other related responsibilities. Subsequently danger of misrepresentation, fraud transaction utilizing credit cards has additionally been expanding. To discover fraudulent with respect to misfortune in these transactions is very difficult. In regular day to day existence credit cards are utilized for acquiring merchandise and enterprises utilizing the online or physical card for offline trade. In card based purchase, the cardholder shows their card to a dealer and authenticate with PIN for making payment. To make fraud in this kind of acquisitions, the person doing fraud has to steal the Credit Card or Card Credentials. The card number, PIN and expiry date are the data attackers need to do online fraud. If the legitimate user does not understand the loss of card, it can lead to important financial loss to the credit card providers and also to the user. Owing to non-availability of credit card transactions dataset and deficient in fraud detection techniques, effective security is a major concern in this domain. Organisations and consumers under no circumstances disclose their standard or transaction data [5, 6].

Comprehensive Study, analysis using various methodology has been proposed but still this problem persist and leads to search of better preventive solution rather than a corrective. Available unstable, unauthentic data set and data size leads to study in imperfection. It will be better to prevent credit card fraud rather before it happens and detected, to address this a new Primary PIN validation and Multifactor based authentication process is proposed in this paper. Review on various proposed methodology and study on credit card frauds is discussed in Sections 2 and 3. Sections 4 and 5 describes the

proposed methodology and implementation process, in Section 6 factors influencing Primary PIN and analysis on usage of Primary PIN is discussed. Section 7 describes advantages, limitations and recommendations.

II. Literature Review

Abdullah (2004) discussed the consequences of identity theft, as a result of it their study emphasizes how users and bankers faces different type of threats and losses [7]. Mannan and Oorschot (2008) discussed about identity theft and consequence of that how credit card frauds are happening, in view of this they prescribes the security measures by regulating 4 variants. They are providing Identity number to user with approval code, transaction with or without chip cards, altering database in a way that only authorized party can get access with secret key, centralized verification in users perspective [8]. Furiah and Braheem (2009) discussed various study on techniques to detect online credit card frauds. The study includes factors influencing credit card fraud, techniques such as supervised and unsupervised learning, importance of address verification services, card verification value and users reliable email authentication. Based on their review and comparative analysis they come up with suggestion for prevention that trustable email server will be the best solution [9]. Hsu T (2011) proposed a technique to detect online credit card fraud using machine learning technique. For study, online transaction data of AliExpress retail service was examined and the result has shown accuracy rate of 97% [10]. Rahman and Anwar (2014) did survey on Islamic banking division of Malaysia with detailed 146 question and answer analysis between bank officers and managers. Their analysis suggest that to prevent and to protect against frauds there is a need of highly secured Password system and protected firewalls [11]. Tselykh A and Petukhov D (2015) implemented cloud web server based fraud detecting service to reduce and to identify frauds. The proposed system is cost effective, utilizing defined protocols and ML algorithm they were able to detect frauds [12]. Alkhasov et al., (2015) presented in what ways credit card frauds will happen and how bearer can be victim for frauds to various techniques like phishing, skimming to say a few. Using Clustering technique, Correlation between bank and user data and applying multiple regression model they predicted fraud investigation [13]. Santiago G.P et al., (2015) studied credit card transaction fraud in online services. For study, they considered the payment dataset of Latin American services. Findings and analysis on frauds were done by supervised learning algorithm Support vector machine. They concluded with, it is difficult to identify such credit card fraud as their rate of detection deviated much from the fraud rate [14]. Correia I (2015) explored the fuzziness of transaction data set and utilised IBM open source proactive technology online to detect online frauds. Various parameters such as policy and fraud types were discussed and taken into account for classification. Feedzai three years dataset has been analysed and has shown existence of 80% illegitimate transactions [15]. Zareapoor M and Shamsolmoali (2015) studied various credit card fraud detection techniques such as SVM, KNN algorithm, Naive Bayesian and proposed algorithm based on decision tree - bagging ensemble classifier to detect credit card fraud. The data set from Japan and China were considered for analysis and they were able to predict accuracy in detecting frauds in less time. They carried analysis by classifying the data set into four groups and data set carried 2.8% fraudulent [16]. Van Hardeveld G. J et al., (2016) proposed online tutorial methods to find out credit card fraud but fails to detect abnormality. In their crime script analysis they discuss various factors like common carding path carried by launders and possible measures against them [17]. Kamaruddin and Vadlamani Ravi (2016) discussed the problem experienced by banking sectors and credit card holders in the observation of credit card fraud. They implemented data processing technique by using particle swarm optimization and neural networks to detect credit card frauds. For analysis ccfraud data set containing 94 Lakhs transaction details with fraudulent 5.96% were utilized and they were able to predict 89% accuracy of prediction [18]. Artikis A et al., (2017) proposed machine learning technique with event learning in identifying fraud prototypes in credit card administration. Dataset from SPEEDD consisting of 100 Lakhs transaction were evaluated with the help of 4 fraud analysis experts. By their proposed system they were able to identify 24 fraud incidences and comparing with inferences based logical programming their system performed better [19]. Correia I et al., (2017) developed a model for European SPEEDD project to detect credit card frauds. For fraud detection, user interface is classified in two modules UI1 and UI2 where UI1 detect fraud while UI2 emphasis on transactions. The parameters for UI2 phase includes variations in transaction, expiry of cards and flash attacks [20]. Sohony I et.al, (2018) proposed credit card fraud detection by using neural network. To resist these types of fraud feasible solutions are prevention and detection techniques. To achieve better performance they implemented ensemble machine learning technique, in their examination normal instances are predicted by random forest and abnormal instances were detected by neural network [21]. Abakarim Y et al., (2018) proposed a deep learning neural network algorithm to detect credit card frauds. Analysis on classification of authenticate and unauthorized transaction is carried by neural network's auto encoder. Two days Data set of European cards during 2012 is analysed and the proposed method has shown good precision rate compared with various methods such as regression and classification methods [22]. Graves et al., (2018) proposed probabilistic model in determining credit card fraud, according to their study once data breach happens it is better to reissue a new card. Analysis has been carried out by Monte Carlo algorithm [23]. Tran et al., (2018) explored the problem of credit card fraud with the advance of abnormality detection procedure, European dataset has been analysed using support vector machine and attained optimal result in detecting frauds. In the same hand they arrived at less false identification results [24].

These various study on Credit card fraud suggests that though various significant methodology are available and applicable in detecting frauds in addition it needs better improvement. More precise non-disclosure of attack data by customers and service providers and non-availability of adequate data structures this more complicate. For security enhancement and by improving the existing authentication

system this paper is proposed with Primary PIN and Multifactor authentication system

III. Credit Card Fraud: Statistics

Despite the fact that unavailability of data on credit card fraud exist financial analysis websites / resources like Forbes, Wallet hub, zdnet publish statistical report on identity theft, data breaches, loss due to credit or debit card fraud every year. These statistical analysis shows how users are affected by these kind of frauds. From the analysis it is clear that year by year how fraud rate has been increased. All these services do analysis, suggest users to change PIN often and to implement multifactor authentication. Statistical report on credit card fraud, data breaches and identity theft is tabulated in Table I.

TABLE I. Sample Statistical Report on Credit Card Fraud

Source	Location	Year	Incidents / Statistics
Forbes [25]	World Wide	2012	Mexico - 25%; Netherland - 8% Canada - 19%; China - 24%
UK cards association [26]	UK	2012	14% increase between 2011 and 2012; 27% Abroad
Wallet hub [27]	Overall	2013	40 million accounts affected due to card data breach
Credit cards [28]	Worldwide	2014	1540 data breaches
Ftc.gov [29]	USA	2014	17% credit card fraud; 39% identity Theft
Zdnet [30]	India	2015	534 - Phishing websites 342 - outside India
Assocham [31]	India	2015	300,000 Cyber crimes
Le-vpn [32]	USA	2015	47% of worlds credit card fraud Most by Phishing and Spyware
	France	2015	Three hundred thousand families suffered from fraud
Wallet hub [27]	Overall	2016	Credit card Fraud Mexico - 56% Most affected Hungary - 9% Least affected
Fool [33]	USA	2017	8.1 billion dollars loss; 133131 number of credit card reports
Shift processing [34]	USA	2018	38.6 % credit card fraud losses, Around 16 hundred thousands
Finextra [35]	UK	2018	22% credit card fraud

IV. Proposed Methodology

E-commerce technology enhanced humankind with cashless purchase in both online and offline purchases. Purchase through credit card services had become common in these days. Users who prefer these kind of services first acquire credit card, provided by numerous service providers. Once they receive the card they can opt purchases either by directly swiping or tapping the card in a shop or through online shopping. To authenticate whether they are the legitimate user, they will be provided with CVV or PIN for authorization and also by OTP verification sent to their registered mobile by service provider.

Advantages of using credit card services are cashless purchase, ease access and credit purchase i.e. we pay for you now you pay later. On the other hand, credit card fraud made loss of integrity, loss of money to both user and service provider and identity theft. Through skimming devices, phishing websites, fake websites, shoulder surfing and malwares, credit card frauds are carried out. So many research and methods have been proposed, evolved to overcome this issue. As an alternative in this paper authentication using Multifactor and Primary PIN validation process is proposed.

The proposed methodology is represented as working architecture and shown in Fig. 1. Once the user collects the card as a mandatory user will be requested to generate Primary PIN, along with PIN provided by service provider. Initial customer database of each user will be created, containing information about their location, preferred location of purchases, favourite shops, items and their desired information about purchases. On each purchase the parameters or features will be compared and verified for users, when it matches then only approval gateway will be processed. For online transaction, users need to provide card verification value (CVV). If CVV matches then PIN. If PIN matches then validation through OTP sent to users registered mobile. If the features or parameter doesn't matches user will be prompted to use Primary PIN. If primary PIN matches then access for providing CVV, PIN and OTP will be granted. If Primary PIN doesn't matches access will be declined with alert message to users registered mobile no. Similar methodology will be followed for swipe based purchases. In each purchases the database of the user will get updated and verified in subsequent purchases either online or offline. At the time of suspect of unauthenticated transaction, validation will be directed to use Primary Pin instead of regular PIN. In addition to regular PIN here user needs to remember Primary PIN. As multifactor authentication process the proposed methodology

enhances the security of credit card based transaction whichever online or offline. In existing methodologies the transaction gateway won't ask for all CVV, PIN and OTP. For validation either OTP with CVV or PIN. But in our proposed methodology it requires all authentication factors which user knows and user gets.

V. Implementation Process

On each Transaction, transaction history database of each users will be updated. In comparison and analysis phase users each transaction will be observed for authenticity, In case if features doesn't matched as an unsecured transaction the user will be asked to go for continual transaction with Primary PIN validation. If Primary PIN validation succeeds after multifactor authentication user gets approval. Else transaction will be declined by stating unauthenticated user.

For Online Transaction:

Step1: User Enters Card details
Step2: Comparison and analysis with Features/Parameters of users Transaction history database. If Parameter matches proceed to step 3 else Step 6.
Step3: Enter CVV If CVV matches next step.
Step4: Enter PIN If PIN matches next step.
Step5: Enter OTP sent to users Registered Mobile. If OTP matches Approval.
Step6: Enter Primary PIN known only to the authenticated customer.
Step7: If Primary PIN matches proceed to Step3. Inclusion of transaction history in Database.
Step8: If Primary PIN does not matches Transaction decline. Alert and message to user registered mobile number.

For card swipe Transaction:

Step1: User Swipes Card.
Step2: Comparison and analysis with Features/Parameters of users Transaction history database. If Parameter matches proceed to step 3 else Step 5.
Step3: Enter PIN If PIN matches next step.
Step4: Enter OTP sent to users Registered Mobile. If OTP matches Approval.
Step5: Enter Primary PIN known only to the authenticated customer.
Step6: If Primary PIN matches proceed to Step3. Inclusion of transaction history in Database.
Step7: If Primary PIN does not matches Transaction decline. Alert and message to user registered mobile number.

VI. Features Influencing and Study on Primary PIN

The proposed method is focused on prevention of credit card fraud by implementing Primary PIN and Multifactor Authentication. As in the comparison and analysis phase each transaction is to be compared with users transaction history, various features of purchases are gathered and stored in the customer database. The features or parameters influences Primary PIN usage in Comparison phase are given in Table II and in each transactions customers history database will be updated. To validate the proposed methodology a study was conducted on 500 respondents about execution of Primary PIN during transaction variance at comparison phase and implementation of multifactor authentication. Since the proposed methodology require users to remember PIN provided by service provider and Primary PIN which they generated, analysis on users remembrance also carried out. From the analysis represented in Fig. 2 it is clear that Primary PIN and multifactor authentication has got good welcome among the respondents.

TABLE II. Users Transaction History database and Features influences for Primary PIN

Online Transaction	Card Swipe Transaction
Product Category	Places /Area & Zone of the Purchase
Recipient Delivery Name & Address	Shops by category
IP Address, Usage	Probable Day & Probable Timings
Authentication failure	Probable Events & Occasion
Types of Transaction	Amount of transaction
Value purchase against regular purchase	Authentication failure
Sites used / Service Provider	National & International usage
National & International usage	Linked Mobile Number
Linked Mobile Number & Mail ID	
Credential Entry Time	
OTP matching and Number of Attempts	
Merchant / Vendor details	

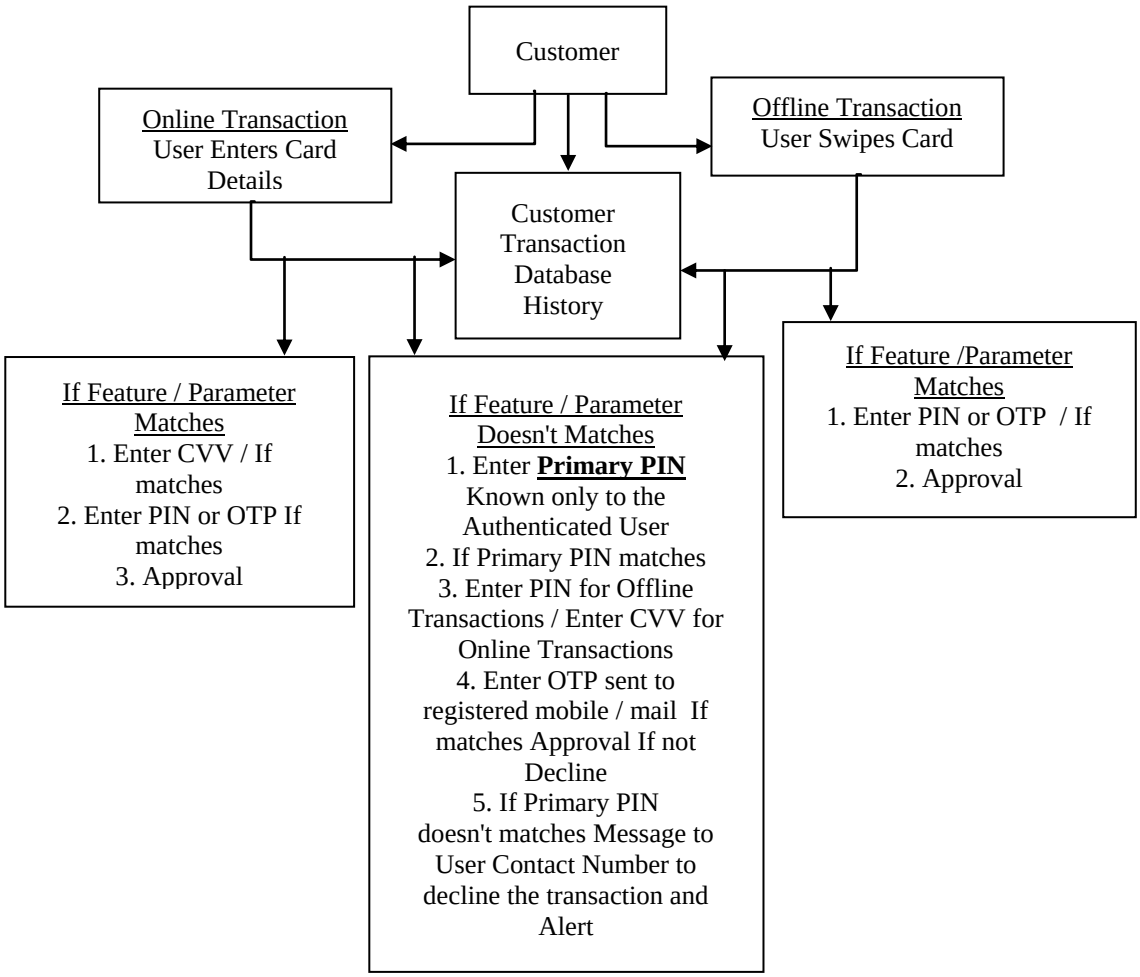

Fig 1. Proposed Multifactor and Primary PIN Authentication Process Architecture.

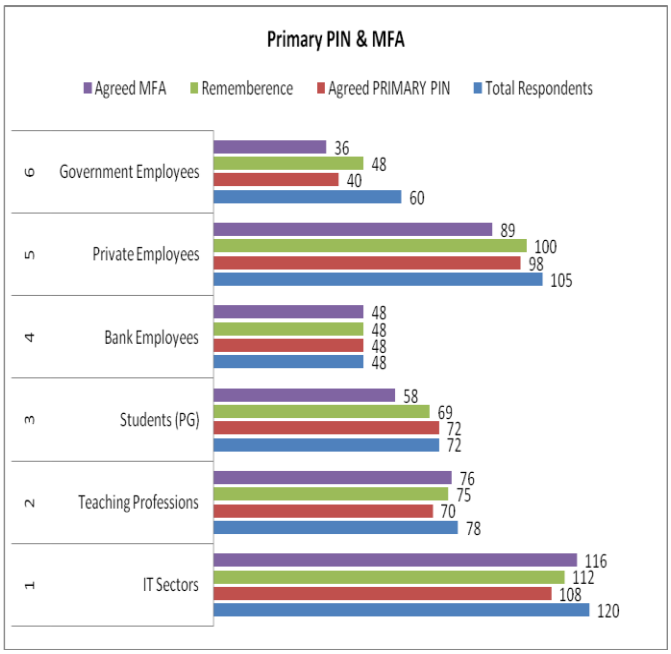

Fig 2. Preference and Remembrance of Primary PIN and MFA.

VII. Advantages, Limitations and Recommendations

Survey from the respondents shows higher priority towards the proposed methodology, despite the fact that it has advantages, limitations of applying the same is to be discussed. Advantages and Limitations along with recommendations are tabulated in Table III.

TABLE III. Advantages, Limitations and Recommendations of the Proposed Methodology

ADVANTAGES	LIMITATIONS	RECOMMENDATIONS
Secured Transaction Customer Satisfaction Fraud diminution Multifactor Authentication Cost effective Trust on sellers	Remembrance Ability Time Complexity Database Maintenance Database Storage	Regular Password Change, Alert Registration, Using 3D Secure PIN, Additional security layer using Biometric authentication. No link between Normal PIN and Secondary PIN. Avoid Multiple Card. Multifactor Authentication.

VIII. Conclusion and Future Work

New way to prevent from Credit Card fraud in either way of transaction by swipe or through online is proposed using Primary PIN in this paper. The proposed system based on Primary PIN and Multifactor authentication prevents the credit card users from secure users' funds. In mismatch situations users will be given alert to use for the Primary PIN to prevent from credit card fraud. The goal of the proposed methodology is to maintain security, integrity, availability and privacy of information entrusted to the system. Sample survey analysis on Primary PIN preference, remembrance ability and usage of multifactor authentication shows the strength of the proposed methodology. To a Greater extent further research on user studies based on user's usage whether user friendly or not, PIN remembrance and service provider aspects are essential. And further this method can be studied in net banking and ATM transaction with sufficient modification so as to overcome ATM threats. In future biometric authentication can be included as an additional validation process to enhance more security.

Reference

[1] Gold, S. (2014). "The evolution of payment card fraud. Computer Fraud & Security", Vol. 3, Pp. 12-17.

[2] Yan Li Z and Jia Z. (2012). "Research on data pre-processing in credit card consuming behaviour mining". Energy Procedia, Vol.17, Pp.638-643.

[3] Delamaire L, Abdou H and Pointon J. (2009). "Credit card fraud and detection techniques: a review". Banks and Bank systems, Vol. 4,Issue 2, Pp. 57-68.

[4] Carneiro N, Figueira G and Costa M. (2017). "A data mining based system for credit-card fraud detection in e-tail". Decision Support Systems, Vol. 95, Pp. 91-101.

[5] Ranjeeta Jha, Abhaya, Vijay Kumar Jha. (2014). "A Review on Credit Card Fraud detection Techniques". International Journal of Engineering Research & Technology, Vol. 3 Issue 4, Pp. 524-528.

[6] Sivakumar N and Balasubramanian R. (2015). "Fraud detection in credit card transactions: classification, risks and prevention techniques". International Journal of Computer Science and Information Technologies, Vol. 6, Issues 2, Pp 1379-1386.

[7] Abdullah A K. (2004). "Protecting your good name: identity theft and its prevention". In Proceedings of the 1st annual conference on Information security curriculum development, Pp. 102-106.

[8] Mannan M and Van Oorschot P. C. (2008). "Localization of credential information to address increasingly inevitable data breaches". In Proceedings of the 2008 New Security Paradigms Workshop, Pp.13-21.

[9] Al Furiah S and Al Braheem L.(2009). "Comprehensive study on methods of fraud prevention in credit card e-payment system". In Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services, ACM, Pp.592-598.

[10] Hsu T. (2011). "Real-time risk control system for CNP (card not present)". In Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, ACM, Pp.783-783.

[11] Rahman R. A and Anwar I. S. K. (2014). "Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks". Procedia-Social and Behavioural Sciences, Vol. 145, Pp. 97-102.

[12] Tselykh A and Petukhov D. (2015). "Web service for detecting credit card fraud in near real-time". In Proceedings of the 8th International Conference on Security of Information and Networks, ACM, Pp.114-117.

[13] Alkhasov S. S, Tselykh A. N and Tselykh A. A. (2015). "Application of cluster analysis for the assessment of the share of fraud victims among bank card holders". In Proceedings of the 8th International Conference on Security of Information and Networks, Pp.103-106.

[14] Santiago G. P, Pereira A and Hirata Jr. R. (2015). "A modelling approach for credit card fraud detection in electronic payment services". In Proceedings of the 30th Annual ACM Symposium on Applied Computing, ACM, Pp.2328-2331.

[15] Correia I, Fournier F and Skarbovsky I. (2015). "The uncertain case of credit card fraud detection". In Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems, ACM, Pp.181-192.

[16] Zareapoor M and Shamsolmoali P. (2015). "Application of credit card fraud detection: Based on bagging ensemble classifier". Procedia computer science, Vol.48, Pp. 679-685.

[17] Van Hardeveld G. J, Webber C and O'Hara K. (2016). "Discovering credit card fraud methods in online tutorials". In Proceedings of the 1st international workshop on online safety, trust and fraud prevention, ACM, Pp. 1.

[18] Kamaruddin S and Ravi V. (2016). "Credit card fraud detection using big data analytics: use of PSOAANN based one-class classification". In Proceedings of the International Conference on Informatics and Analytics, Pp. 1-8.

[19] Artikis A, Katzouris N, Correia I, Baber C, Morar N, Skarbovsky I and Paliouras G. (2017). "A prototype for credit card fraud management: Industry paper". In Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems, ACM, Pp. 249-260.

[20] Correia I, Artikis A, Katzouris N, Baber C, Morar N, Skarbovsky I and Paliouras G. (2017). "Demonstration of a Prototype for Credit Card Fraud Management". In Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems, ACM, Pp.335-338.

[21] Sohony I, Pratap R, and Nambiar U.(2018). "Ensemble learning for credit card fraud detection". In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data, ACM, Pp.289-294.

[22] Abakarim Y, Lahby M and Attioui A. (2018). "An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning". In Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications, ACM, Pp.30.

[23] Graves J. T, Acquisti A and Christin N. (2018). "Should Credit Card Issuers Reissue Cards in Response to a Data Breach? Uncertainty and Transparency in Metrics for Data Security Policymaking". ACM Transactions on Internet Technology-TOIT, Vol. 18, Issue 4, Pp.1-19.

[24] Tran P. H, Tran K. P, Huong T. T, Heuchenne C, HienTran P and Le T. M. H. (2018). "Real time data-driven approaches for credit card fraud detection". In Proceedings of the 2018 International Conference on E-Business and Applications, Pp. 6-9.

[25] https://www.forbes.com/sites/halahtouryalai/2012/10/22/countries-with-the-most-card-fraud-u-s-and-mexico/#701217864708.

[26] http://www.theukcardsassociation.org.uk/wm_documents/3533%20Fraud%20The%20Facts%20FINAL.pdf.

[27] https://wallethub.com/edu/cc/credit-debit-card-fraud-statistics/25725/

[28] http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[29] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

[30] http://www.zdnet.com/article/online-banking-and-plastic-card-related-fraud-in-india-increases-35-percent/

[31] https://www.assocham.org/newsdetail.php?id=4821.

[32] https://www.le-vpn.com/how-to-avoid-increasing-online-credit-card-fraud/

[33] https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/

[34] https://shiftprocessing.com/credit-card-fraud-statistics/

[35] https://www.finextra.com/pressarticle/76482/credit-card-fraud-index-41-billion-stolen-as-a-result-of-credit-card-fraud-in-the-uk-in-past-year.