The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1396 - 1406

Fuzzy Authentication System for Online Transaction Fraud Detection Using Geo Location

Jaydip Kumar[1*] Karam Veer Singh [2] Vipin Saxena[3]

[1,2,3]Department of Computer Science, BabasahebBhimraoAmbedkar University, Lucknow (UP) India, 226025.

Emails: jaydipkumar2001@gmail.com , kvsingh.bhu@gmail.com, profvipinsaxena@gmail.com

ORCID ID: [*]https://orcid.org/0000-0001-9350-8775, [2]https://orcid.org/0000-0003-1935-0011, [3]https://orcid.org/0000-0003-1035-1704

Abstract

In the current days, there is an extensive use of online transaction of information from one place to another place and daily, it is incrementing as an exponential growth. Simultaneously, online activities are also performed by the hackers and thus incrementing the online fraud. Therefore, the present research work is an attempt to minimize online fraudulent activities especially for the financial sectors by implementing the different authentication and authorization schemes at the different levels. In the present work authentication scheme has been proposed by implementing the secure One Time Password (OTP) transmission and Personal Identification Number (PIN) which are based on Global Positioning System (GPS) where transaction is performed then GPS has collected the location details from where the transaction has performed and the location of phone in which OTP is received. The concept of distance has calculated with the both GPS locations and used as a authentication factor. Client Financial Control Application (CFCA) is also responsible for authentication for the online transaction which ables to allow or deny transaction based on account status and fuzzy rule based expert system is used to authenticate the distance, transaction time and other parameters while transaction is performed. The main objective of this paper is to provide security for online transactions and to keep track for online fraudulent transaction.

Keywords: Authentication and Authorization, Distance Based Fraud, Fuzzy Based Authentication, GPS locations, Online Fraud, Online Transaction.

Introduction

In the digital era, many of the people are transacting the currency in the form of digital from one place to another place through the high speed internet services. The use of paper currency has been minimized and online transaction of currency is increasing exponentially. Due to presence of hackers on high speed internet services, the digital transfer of currency is unsafe and for the secure transfer of currency, many of banks are using broad based Wisdom Web of Things (W2T) technology which can be used for detecting the online fraud in the banking system. In this technology information is collected from credit card transaction data, online banking transaction data, customer's information and other types of transactional information. The Rivest, Shamir and Adleman (RSA) digital system is also used for secure online transaction[1]. The cracking by hackers of RSA digital system is still not reported in the literature but hackers have hacked the other types of algorithms which are used in the transaction of digital currency, hence it is a big challenge for the financial transaction to stay safe and also to avoid frauds. Due to this many of financial and other institutions have introduced the different kinds of authentication schemes like OTP, one and two types authentication, etc. which are not able to provide complete security.

Day by day, online frauds are increasing called as eye catching frauds. It is very risky for the customer to transfer bulk digital currency from one end to other end due to various services across the internet. Various researchers have also proposed different kinds of fraud detection schemes. But due

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1396 - 1406
to low latency rate, most of the people are not able to report fraud transactions to the financial and other institutions instantly after occurrence of fraud. This makes losses to the customers and recovery rate by the cyber police is very low. It is observed from the literature that the online frauds are twelve times higher than the use of physical card fraud because online transaction of digital currency do not require any physical cards and personal transactions illegally and it can be collected through physical or clone websites, collision attacks, malicious insiders and many more.

Anomalies and misuses of currency detection scheme are being used by the scientists and engineers for fraud detection. In these techniques, large database related to incoming and outgoing transactions are collected and there after it is very easy to detect the fraud after applying the kinds of schemes. These schemes are based upon the fraud detection and also to obtain the fraud patterns in the near future. The supervised learning techniques like neural networks, decision trees, support vector machines and logistic regression are also used to obtain fraud patterns. But these are used for existing fraud patterns and kinds of fraud detection which are not previously happened.

It also lacks the acceptance and rejections of transaction therefore, it is necessary to crack strong fraud detection techniques. Due to evolution of the e-commerce website related to sales and purchases of various items. It is major concerned that fraud must be detected at the time of transaction. For example, various fake e-commerce websites are available on the social media platform like facebook etc., customers don't have idea about the e-commerce websites and move towards the payment gateway for the payment of items to be performed, but after long time, aware of e-commerce don't supply the desired items then customers come to know that the website is fake, hence only option at that time to register cyber First Information Report (FIR) in the cyber police station which takes long time for investigation and customers suffer. Hence, it is obvious that fraud must be detected before the transactions of digital currency. It is also added from the literature that online fraudsters are continuously developing new techniques for online fraud. Therefore, it is necessary to financial and other organizations to develop robust system for fraud detection and there is need to make strong detection techniques which could detect the fraud activities at the time of transaction to avoid future miss happening[2].

In view of above, the proposed work is related to develop highly secure transaction technique for online detection of fraud in the digital era. The presented scheme shall detect the fraudster before proceeding towards the final step of transactions.

Related Work

For fraud detection and analysis of the credit or debit card for online transactions, different supervised learning techniques such as neural networks, decision trees, support vector machines and logistic regression have been proposed by scientist and engineers in the literature. Let us describe some of the important research work related to the present work.

Money laundering is a new problem for the financial and other organizations. Financial institution and other organizations encountered numerous issues related to the internet banking fraud. The internet banking increased the affordability and benefits while ordering the online products, but it also increased the number of hackers. An optimal risk threshold algorithm has been proposed for determination of risk for each user. Individual behavior transaction detection and combination of the behavior and optimal risk threshold generate the behavior benchmark which is used to construct the multidimensional hypersphere model[3]. The large number of transactions with the online banking and e-commerce are performed every day. It is required an efficient and fast fraud detection technique to identify the fraud. Most of the techniques detect the fraud based on the previous pattern. Fraud detection within the short time span is very difficult and needs advanced detection technique. An Adaptive Neuro-fuzzy inference system is proposed which is self-learning predictive system. This

was the combination of neural networks with fuzzy inference and able to detect newly arrived fraud techniques[4]. The banking systems are trying to minimize the fraud transaction and reduce the huge loss of banks. Many advanced detection techniques have been applied for fraud detection but have no effective results on prevention and detection. A Hidden Markov Model (HMM) was proposed for detection of fraud and ensured that the transaction was genuine or not[5].

The billions of dollars are losing every year due to the online fraud transactions. The fraud prevention techniques still need to be improved. A rudimentary fraud detection model was proposed that utilize transaction behaviors. This model collects information of transactions such as time, amount, geographical location and calculates the statistical values and patterns with the probability of fraud[6]. The huge increment of online transaction was forced by the worldwide banking sectors and to avoid fraudulent transaction rule-based system was designed. The static nature of the rule-based system was bypassed by the newly arrived attacks. Researches designed adaptive fraud detection systems using machine learning and deep learning, but still these are not trustable. A profile-based fraud detection model was introduced and made temporal and spatial analysis over the data[7].

Transactional fraud can be done by different ways such as physical fraud, online fraud, spamming and phishing. The fraud detection in banking sector is mostly based on the data mining techniques and based on their past experience and probability. Different data mining techniques and modified model were proposed for fraud detection[8]. Machine learning is also a part of Artificial Intelligence system which has the ability to automatically learn and get the knowledge itself without manually programmed. Mostly online fraud detection scheme has used the machine learning concepts for prediction of fraud. A method was proposed to maximize the correctly flagging for identification of fraudulent transactions but also minimize the cost of wrong predictions[9].

Billions of losses are performing every year by the financial frauds. Information related to the real transactions is very beneficial for predicting the fraud in the transactions. Statistical and machine learning model was also proposed for detecting online fraud. A comparison was performed between the algorithms and finds the genetic algorithm which offers better discriminative power and compared with original features[10]. Many different popular organizations such as Alibaba, Amazon and Paypal invest billions of dollars for the safe transactions. To avoid the fraud, machine learning and data mining techniques are already in use but still facing same problems. A model was proposed for e-commerce fraud detection with the combination of manual and automatic classifications[11]. From the last few years, every organization such as e-commerce systems or banking system upgraded their security systems to protect online frauds. But all existing approaches were not provided sufficient in-depth security model against the elusive attacks. A decision support system was developed for banking fraud analysis against the elusive attacks. And build a model for entire system with the comparison of user-centric and system-centric. In this regard, proof-of-concept attack tool was used for mimicry attacks[12].

Online shopping is already running well but it was get more populated during the COVID-19 pandemic. Due to huge increment in online transactions, credit or debit card detected high risk payment system. A cost-effective fraud detection upgraded system was proposed which is used to detect Card-Not-Present (CNP) fraud transactions[13]. In the high increment in the fraud rate many researchers were presented with the different machine learning methods for detection and prediction of online fraud transactions. A novel fraud detection model was developed for streaming transaction data and extracts the behavioral patterns using the sliding window strategy. Different classification techniques were used for better prediction rate[14]. To prevent the online transaction fraud different financial transaction related organizations have implemented various authentication and authorization techniques at different levels. Anti-fraud techniques are facing different challenges under the trending new situations. A modified deep forest framework based on the Bagging Balance Method (BBM) was

proposed for detection of online fraud. The proposed model improved 10% compared with random forest and 5% improvement compared with original deep forest model[15]. Behavior Profile (BP) is an important way of detecting fraud based on historical transactions records, behavior of the transaction is genuine or not. Markov chain model is used for representing the behavior profile of users, which is effective for those users whose transaction behaviors is stable or not. Logical Graph of Behavior Profile (LGBP) model was proposed which was total order-based model and computed the path-based transition probability from one attribute to another, and also defined information entropy-based diversity coefficient and state transition probability matrix for capturing the temporal features of user. Consequently, a Behavior Profile (BP) has proposed for every user for verification of all incoming transactions which are genuine or not[16]. Let us define some of the important techniques are explained below briefly.

1.Advanced Encryption Standard (AES)

It is an extended version of Data Encryption Scheme (DES) which was developed in the year 2001 and it supports the data upto 128 bits with any combination and support of key length as 128, 192, and 256 bits and corresponding to these key length, AES is named as AES-128, AES-192 and AES-256[17] respectively. It has N rounds depending upon AES key length with string rounds as AES-128, AES-192 and AES-256 are 10, 12, and 14 respectively. It also consists of N-1 rounds based on different transformation techniques like SubBytes, ShiftRows, MixColumn and AddRoundKey and the last round contains three techniques like SubByte, ShiftRow, and AddRoundKey[18].

2.GPS Positioning

It is a Global Positioning System (GPS) which was developed by U. S. department of Defense based upon space positioning, timing and navigation system with the satellite positioning system for geo-location for efficient movement with the combination of twenty four orbits satellites. These satellites are placed in six different orbit paths in space and each path consists of four satellites[19].

3.Haversine formula

It was introduced by Jamez Andrew in the year 1805 based on the spherical earth taken as elliptical and based upon the spherical trigonometric function by considering the distance between two points and sides which creates spherical triangle, however the complete formula is given below[20].

$\Delta long = (long2 + long1)cos\frac{(lat1+lat2)}{2}$ 1

$\Delta lat = (lat2 - lat1)$ 2

$S=\sin2\left(\frac{\Delta lat}{2}\right)+\cos(lat1)\cos(lat2)\sin2\left(\frac{\Delta long}{2}\right)$3

$d = \sqrt{(S)}R(4)$

Where R is the radius of the earth in kilometer (km), Δlat is the amount of changes in latitude in km, $\Delta long$ is the magnitude of change in longitude in km and d is the calculated distance in km.

4.Fuzzy Techniques

Fuzzy set theory was first invented by the Zadeh[21] from the University of California. It is a approach for variable processing which allows for multiple possible truth values to be processed through the same variables. In the fuzzy set theory, every element of set has a degree of membership. The degree of membership function has described between the interval [0, 1].

In the fuzzy set theory, the Triangular Fuzzy Number (TFN) is used to provide the cyber security for online services[22]. In the TFN, the p, q, and r are representing the smallest possible values and mean value represents the largest possible value. In TFN, $\mu_{\tilde{N}}$ is the membership function which is shown below in Fig.1.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1396 - 1406

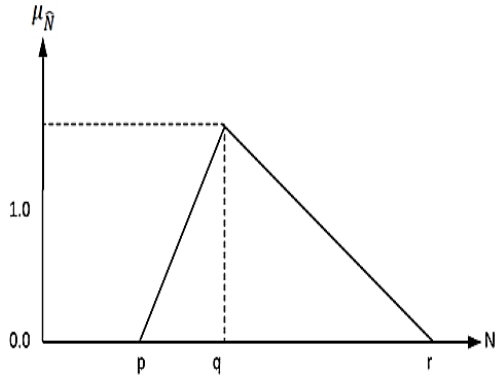

Figure 1.Representation of Triangular Fuzzy Number

The formula for membership function is given below.

$$\mu_{\hat{N}} = \begin{cases} 0 & a < 1 \\ \frac{a-p}{q-p} & 1 \le a \le q \\ \frac{r-a}{r-q} & q \le a \le r \\ 0 & a > 1 \end{cases} \quad (5)$$

So, the Triangular Fuzzy Number is $\hat{N} = (p, q, r)$. Due to the wide field of TFN, some basic operations on triangular fuzzy numbers are given below.

Let $\hat{R} = (a, b, c)$ and $\hat{S} = (d, e, f)$ are two triangular fuzzy numbers.

$\hat{R} + \hat{S} = (a + d, b + e, c + f)$ 6

$\hat{R} - \hat{S} = (a - d, b - e, c - f)$ 7

$\hat{R} \times \hat{S} = \big(min(a \times d, a \times f, c \times d, c \times f), b \times e, max(a \times d, a \times f, c \times d, c \times f)\big)$8

$\frac{\hat{R}}{\hat{S}} = \left(min\left(\frac{a}{d}, \frac{a}{f}, \frac{c}{d}, \frac{c}{f}\right), \frac{b}{e}, max\left(\frac{a}{d}, \frac{a}{f}, \frac{c}{d}, \frac{c}{f}\right)\right)$(9)

Proposed Methodology

Due to evolution of high speed internet connectivity and transactions growth of e-commerce website, many authorized users are transacting the currency across the online mode. Most of people have the debit/credit cards and other payment options like paytm etc. Due to increase of these, cyber frauds are increasing day by day. For the financial and other organization, the following types of problems arise at the time of transaction of digital currency:

A. Stealing of Bank Account information by sending phishing techniques;
B. Cloning of Credit/Debit cards for performing illegal transactions of currency;
C. Hacking of currency transfer at the time of transactions;
D. Sometimes physical debit/credit cards are not required for transactions only its number, and other information can be put while steeling the digital currency.

In the present work, hybrid authentication scheme is applied at the time of online transaction of digital currency. In the first step of authentication scheme, card holder name, card number, card expiry and CVV number are required as it is done. In the present scenario of transfer of digital currency, further, OTP or PIN is used for second level of authentication but by the use of these two levels of authentication. Online fraud related to transfer of digital currency cannot be avoided; therefore there is need of the third authentication scheme. In the proposed work geo-graphical location of the user is considered in which the distance between the user and the server is computed. If the computed distance is within the specified limit then online transaction of digital currency is placed otherwise it

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1396 - 1406
can decline the transfer. For this purpose Client Finance Control Application (CFCA) is used. The distance between two devices can be computed by Haversine formula as shown in the equation. For this propose concept of fuzzy technique is also used. The Various algorithms for securing the online transfer of digital currency are described below in brief.

Authentication

In the online payment system, the authentication is the process of recognizing the user's identity while transaction is processed. It is the first step while starting the process. Different authentication processes require different types of credentials to ascertain any user's identity.

The pseudo codes for authentic transfer of digital currency are described below in brief which include first and second levels of authentication procedure including the computation of geo-graphical location of the user.

CFCA Authentication

For CFCA authentication, the pseudo code is given below:

IFCFCA_Login== True
IFSet_Status=Active
THEN Account accept transaction for 30 min
ELSESet_Status=Inactive
THEN Account decline transactions till status will Active
ELSECFCA_login=Failed

In the above pseudo code, the CFCA application manages the user's account. If any user wants to proceed online currency transfer then there is need to first login to CFCA application using userid and password. If successfully logged_in then user can manage account and set account status as "Active" or "Inactive" which is shown in Fig. 2 and Fig.3. The account status is active then account accepted all the online transactions. If the account status is inactive, it rejects all the online transactions related to concerned account.

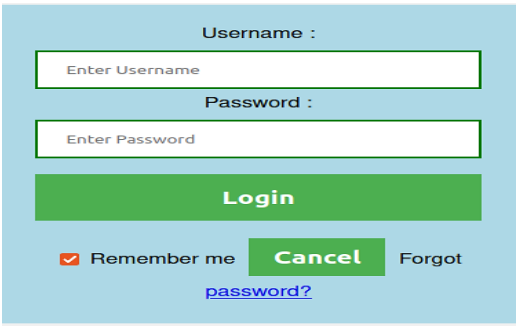

Figure 2. CFCA login Window

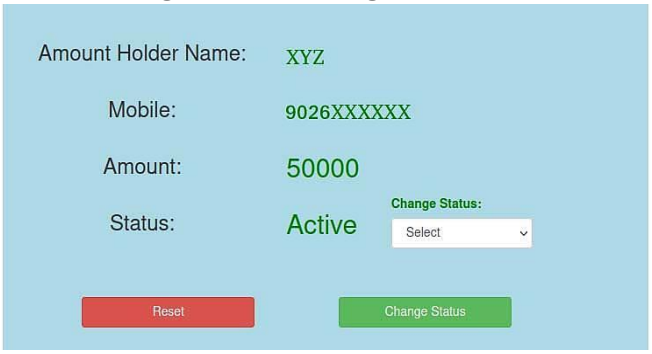

Figure 3. Representation of CFCA Control Panel

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1396 - 1406

OTP Authentication

For OTP authentication pseudo code is given below:

IF OTP_Login== True
IF Txn== Allowed
THEN Send user location
ELSE Txn== Declined
THEN User's location not sends
ELSE OTP_Login==Failed

The OTP authentication is essential part of online transactions. In the present work, the OTP has encrypted using AES algorithm with the user's id as a key while transaction is processed. At the user's device, user needs to login through CFCA credentials. If the login is successful, then the user can allow or reject transaction from the OTP received device. This is shown below in Fig. 4.

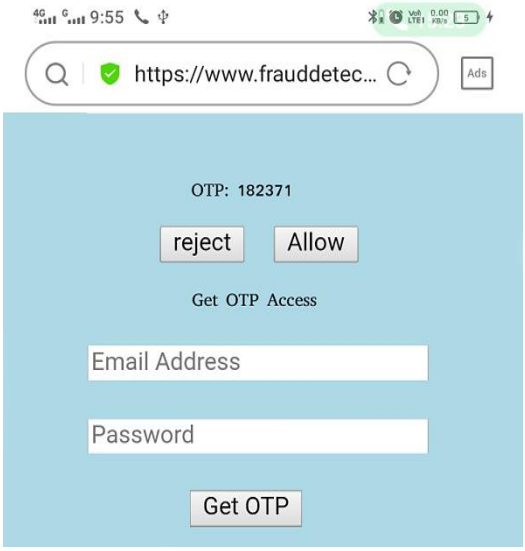

Figure 4. OTP Authentication

Fuzzy Rule Based Authentication

Fuzzy Rule Based authentication uses the human intelligent to solve the real world problem. It is normally represented in the form of rules or users data in the computer system. These rules and data are depending upon the problem to solve it. In the modern intelligent system, rule based expert system plays a very important role with its rules. Let us consider the following.

L_1= Location of transactional device.
L_2= Location of Mobile
K = Maximum Distance
D = haversine(L_1, L_2)
OTP=OTP_Matched ()
A_{sts}=isAccountActive()
A_{mnt}=isAmountAvailable()
D_{max}= Maximum Allowed Distance
T = Transaction Computation Time
T_{max_limit}=Maximum transaction time limit
$T_{xnallow}$=Transaction_Allowed_by_Mobile()
RT=TransactionReject()
PT=ProcessTransaction()

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1396 - 1406
IF (OTP == True) AND ($T_{xnallow}$== True) THEN
IF (D ≤ K) AND (T ≤ T_{max_limit}) THEN
IF(A_{sts}== True) AND (A_{mnt}==True) THEN PT
ELSE RT
ELSE RT
ELSE RT

The above rule-based authentication is implemented for the proposed system. In this system if any user processed online transactions, the financial institution server verifies the OTP. If OTP is matched and transaction allowed by OTP received device then, the server computes the distance through haversine formula between both devices using latitude and longitude. At the same time, server fetched the maxmum transaction per day limit. In the next step server checked calculated distance D ≤ K and T ≤ $T_{max\_limit,}$ where K is distance range defined by financial institution, and T is number of transactions per day. At the final stage of transaction, the server verifies the account status and available amount, if the transaction satisfies the defined condition, the transaction successfully completed otherwise reject the transaction.

Fuzzy Based One Time Password (OTP) Generation

The fuzzy One Time Password (OTP) system is designed by fuzzy rules and the Linear Congruence method. The Linear Congruence method is used for Pseudo Random Number Generator (PRNG). Triangular membership function is used to fuzzyfy the fuzzy input set as low, medium and high. The pseudo code for fuzzy OTP generation is given below and fuzzy inputs and outputs are given in Fig. 5 and Fig. 6 respectively.

Pseudo Code for Fuzzy OTP Generator

Step1:F_i= fuzzy input set
Step2: Find M[low], M[medium] and M[high] using triangular membership function based on F_i
Step3: Define fuzzy rules based on output of triangular membership function.
Step4: Compute P=crisp_value(M)
Step5:R[]=PRNG(P)
Step6: For i in range R
Y=int(i)ss
X+=str(r.randint(1,Y))
otp=X

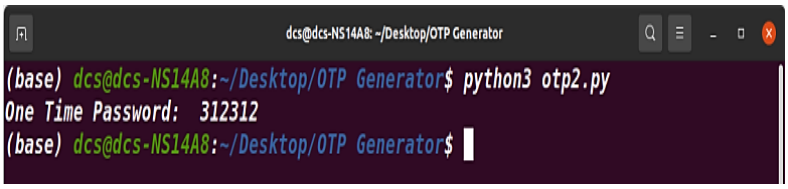

Figure 5.Representation of Fuzzy based OTP

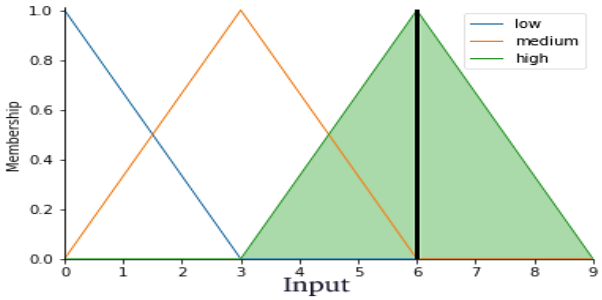

Figure 6. Fuzzy Membership Input

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1396 - 1406

Result and Discussion

The result of the proposed algorithm has been evaluated from the different parameters such as distance of both device, transaction execution time, and the CFCA status. For performance and accuracy evaluation of the proposed algorithm[23]has used four different parameters for measuring the algorithms such as True-Positive (T_p), True-Negative (T_N), False-Positive (F_p) and False-Negative (F_N). After performing 188 transactions and evaluated of the proposed algorithm to maximize the T_p and $T_{N,}$ and minimize the F_N and $F_{P.}$ According to the performance metrics from Table 1 and Table 2 the fraud detection rate 99.21%, hit rate 98.43%, false positive Rate 1.063% and false negative rate 0.531%.

Table 1.transactions on each category

S.No.	Parameter	Number of Transactions
1	T_p	126
2	T_N	59
3	F_P	2
4	F_N	1

Table 2. Performance of the proposed algorithms

S.No.	Performance metrics	Performance (%)
1	Detection Rate	99.21
2	Hit Rate	98.43
3	False Positive Rate	1.063
4	False Negative Rate	0.531

Concluding Remarks

The online shopping is the need of every human in present days and online transaction is the essential component to fulfill the purpose of online shopping. As per related work the numbers of online fraud transactions are exponentially increasing. To deal with these online fraud transactions banking sector has provided different level of fraud detections techniques. In this paper the author have proposed a new scheme for the detection and prevention prior to perform the transactions. The proposed scheme uses different level of security to provide secure transactions. In the first level CFCA application is used to control the client's account, in the second level OTP is encrypted using AES encryption technique and client can reject or accept the transaction from the OTP received device and the last level uses distance of the both devices is calculated using GPS triangulation. The proposed scheme is implemented and analyzed using different parameters such as distance, execution time, and account status using these parameters the proposed algorithm has been maximize the fraud detection rate.

Authors' contributions:

J. K. contributed to the design and implementation of the research, K.V.S analyzedthe results and done writing of the manuscript. V.S. performed the computation sand verified the analytical methods. All authors discussed the result sand contributed to the final manuscript.

Reference

[1] Kumar J, Saxena V. Cloud Data Security through BB84 Protocol and Genetic Algorithm. Baghdad Sci. J. 2022 Dec 5; 19(6 (Suppl.)):1445-.doi: https://doi.org/10.21123/bsj.2022.7281

[2] AL-Mayyahi MA, Hosseini Seno SA. A Security and Privacy Aware Computing Approach on Data Sharing in Cloud Environment. Baghdad Sci. J. 2022 Dec 12;19.Doi:https://dx.doi.org/10.21123/bsj.2022.

[3] Chen L, Zhang Z, Liu Q, Yang L, Meng Y, Wang P. A method for online transaction fraud detection based on individual behavior. InProceedings of the ACM Turing Celebration Conference-China 2019 May 17 (pp. 1-8).doi: https://doi.org/10.1145/3321408.3326647
[4] Veeraiah, D., Mohanty, R., Kundu, S., Dhabliya, D., Tiwari, M., Jamal, S. S., & Halifa, A. (2022). Detection of malicious cloud bandwidth consumption in cloud computing using machine learning techniques. Computational Intelligence and Neuroscience, 2022 doi:10.1155/2022/4003403
[5] Alarfaj FK, Malik I, Khan HU, Almusallam N, Ramzan M, Ahmed M. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access. 2022 Apr 12;10:39700-15.DOI: 10.1109/ACCESS.2022.3166891
[6] Kim J, Jung H, Kim W. Sequential Pattern Mining Approach for Personalized Fraudulent Transaction Detection in Online Banking. Sustainability. 2022 Aug 8;14(15):9791.doi:https://doi.org/10.3390/su14159791
[7] Cherif A, Badhib A, Ammar H, Alshehri S, Kalkatawi M, Imine A. Credit card fraud detection in the era of disruptive technologies: A systematic review. Journal of King Saud University-Computer and Information Sciences. 2022 Dec 5.doi:https://doi.org/10.1016/j.jksuci.2022.11.008
[8] Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences. 2022 Aug 11.doi:https://doi.org/10.1016/j.jksuci.2022.08.003
[9] Bello AM, Mohammed A, Javan H. Effects of Forensic Audit on Fraud Detection in the Nigerian Banking Sector. African Journal of Management and Business Research. 2022 Jun 30;4(1):10-8.https://publications.afropolitanjournals.com/index.php/ajmbr/article/view/143
[10] J. Solanki, S. Sejwal, D. Mehrotra, and S. K. Chowdhary. A step forward in fraud detection system using machine learning.J. Crit. Rev. 2020; 7(12): 413–425.doi: 10.31838/jcr.07.12.76.
[11] Seera M, Lim CP, Kumar A, Dhamotharan L, Tan KH. An intelligent payment card fraud detection system. Annals of operations research. 2021 Jun 8:1-23.https://doi.org/10.1007/s10479-021-04149-2
[12] Xiuguo W, Shengyong D. An analysis on financial statement fraud detection for Chinese listed companies using deep learning. IEEE Access. 2022 Feb 22;10:22516-32.Doi:10.1109/ACCESS.2022.3153478
[13] Carminati M, Polino M, Continella A, Lanzi A, Maggi F, Zanero S. Security evaluation of a banking fraud analysis system. ACM Transactions on Privacy and Security (TOPS). 2018 Apr 16;21(3):1-31.https://doi.org/10.1145/3178370
[14] Mekterović I, Karan M, Pintar D, Brkić L. Credit card fraud detection in card-not-present transactions: Where to invest?. Applied Sciences. 2021 Jul 23;11(15):6766.https://doi.org/10.3390/app11156766
[15] Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Procedia computer science. 2019 Jan 1;165:631-41.https://doi.org/10.1016/j.procs.2020.01.057
[16] Huang M, Lizhi WA, Zhang Z. Improved Deep Forest Mode for Detection of Fraudulent Online Transaction. Computing & Informatics. 2020 Sep 1;39(5).doi: 10.31577/cai 2020 5 1082
[17] Zheng L, Liu G, Yan C, Jiang C. Transaction fraud detection based on total order relation and behavior diversity. IEEE Transactions on Computational Social Systems. 2018 Aug 7;5(3):796-806.DOI: 10.1109/TCSS.2018.2856910
[18] Venu, S., Kotti, J., Pankajam, A., Dhabliya, D., Rao, G. N., Bansal, R., . . . Sammy, F. (2022). Secure big data processing in multihoming networks with AI-enabled IoT. Wireless Communications and Mobile Computing, 2022 doi:10.1155/2022/3893875
[19] Singh G. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications. 2013 Jan 1;67(19).Doi:10.5120/11507-7224
[20] Kumar J, Saxena V. Hybridization of Cryptography for Security of Cloud Data. International Journal of Future Generation Communication and Networking. 2020;13(4):4007-14.http://sersc.org/journals/index.php/IJFGCN/article/view/34754
[21] Hegarty CJ. The global positioning system (GPS). Springer Handbook of Global Navigation Satellite Systems. 2017:197-218.DOI: 10.1007/978-3-319-42928-1_7

[22] Jimoh OD, Ajao LA, Adeleke OO, Kolo SS. A vehicle tracking system using greedy forwarding algorithms for public transportation in urban arterial. IEEE Access. 2020 Oct 15;8:191706-25.DOI: 10.1109/ACCESS.2020.3031488

[23] Gholamizadeh K, Zarei E, Omidvar M, Yazdi M. Fuzzy sets theory and human reliability: review, applications, and contributions. Linguistic methods under fuzzy information in system safety and reliability analysis. 2022 Mar 11:91-137.DOI: 10.1007/978-3-030-93352-4_5

[24] Makani R, Reddy BV. Designing of fuzzy logic-based intrusion detection system (fids) for detection of blackhole attack in aodv for manets. InCyber Security and Digital Forensics: Proceedings of ICCSDF 2021 2022 (pp. 113-128). Springer Singapore.DOI: 10.1007/978-981-16-3961-6_11

[25] Khattri V, Singh DK. Implementation of an additional factor for secure authentication in online transactions. Journal of Organizational Computing and Electronic Commerce. 2019 Oct 2;29(4):258-73. https://doi.org/10.1080/10919392.2019.1633123