Transaction authorization from Know Your Customer (KYC) information in online banking

Transaction Authorization from Know Your Customer (KYC) Information in Online Banking

Prakash Chandra Mondal,[1,*] Rupam Deb,[2] and Mohammad Nurul Huda[1]

[1]Department of Computer Science and Engineering, United International University
Dhaka, Bangladesh

[2]School of Information and Communication Technology, Griffith University
Brisbane, Australia

[*]prakash.cse2009@gmail.com

Abstract— **Online banking is getting popularity due to location independence, 24/7 services and responsiveness. Financial services through the internet are running under various threats like phishing, pharming (cyber attack intended to redirect a website's traffic to another fake site), malware, Man-In-The-Middle (MITM) attack and the evolving sophistication of compromise techniques. One time password (OTP) in online banking system alleviate the risk and make it secure. In various methods of OTP and Mobile Transaction Authentication Number (mTAN), device can be lost or stolen, delivery in delay etc. Compliance with Anti-Money Laundering (AML), Know Your Customer (KYC) and sanctions requirements continues to be a key focus area for Financial Institution (FIs) management, and firms must ensure they are following appropriate compliance procedures to meet the increasing regulatory demands [1, 2]. Addressing existing limitation of OTP, this paper proposes Challenge Question (CQ) from dynamic KYC database for transaction authorization before committing any financial transaction from online banking application. Analysis and simulation results show that the proposed method provides equal control as existing OTP/mTAN.**

***Index Terms*—Two factor authentication (2FA); Know your customer (KYC); online banking authentication method; internet banking; online banking; Transaction authorization;**

I. INTRODUCTION

Online banking is an alluring way of doing business as well as all banking activity independent/irrespective of location. This awesome facility also incurred a highest point of risk as it is using public network over the world. The main endeavour of the FIs is to provide a consistent and secure process of authentication to their users minimizing potential avenues of attack, especially attack vectors beyond the control of either the user or the FIs.

However, authentication method for internet banking is still pursuing to ensure highest level of security. Existing strong authentication method is sometimes a nuisance to the real users who are operating their regular business using internet based financial system. Current activity of any of the users has a linear relationship with users many past usage patterns such as geo-location, nature of regular transaction, range of regular transaction, time of regular transaction, hardware to perform transaction, frequency of transaction, purpose of regular transaction, bio-metric behaviour and many other non bio-metric behaviours.

In this research paper, we introduced KYC information verification in place of one time password (OTP) while performing transaction in order to verify the user more intensively. In that case KYC must be privatized with widespread dynamic user input. The application affluent KYC from the dynamic update from the user interaction through the application on the other hand user can add more confidential information or random question with answer to the KYC database to make the authentication process stronger and more secure. We will also consider ranking on the KYC information for CQ which will be asked to the user after performing a transaction. The CQ will be assigned to ask the user based on the risk factors assessment result. One or more CQ may be asked to the user based on the risk assessment outcome. High rated CQ will be asked to the user when the risk assessment result is higher and low rated CQ will be asked when the risk assessment result is lower.

The rest of the paper is organized as follows. Section II overviews the related work. Description of our proposed model is introduced in Section III. Section IV discusses the result and compares with other method of OTP. Finally, Section V concludes the paper and presents future work.

II. RELATED WORK

In recent couple of decades, many authentication methods have been developed. There are a variety of technologies and methodologies which can be used to authenticate transaction of the customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs) [4][5][8], USB plug-ins or other types of “tokens”, transaction profile scripts, biometric identification, and others. The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution’s risk assessment process [3][10]. Mohamed Hamdy Eldefrawy, Khaled Alghathbar and Muhammad Khurram Khan, 2011 [5] present a novel two-factor authentication scheme whereby a user’s device produces multiples OTPs from an initial seed using the proposed production scheme. The initial seed is produced by the communications partners’ unique parameters. Applying the many from one function to a certain seed removes the requirement of sending SMS-based OTPs to users, and reduces the restrictions caused by the SMS system. Security risks associated with current Mobile Transaction Authentication Number (mTAN) System are discussed and some modifications in existing system are proposed for using mTAN in a more secure way by Waqar Ahmad Khan, Ghalib Asadullah Shah, Yasir Saleem and Amjad Farooq, 2016 [6]. Alain Hiltgen, Thorsten Kramp and Thomas Weigold, 2005 [7] presents two challenges/responses for Internet banking authentication solutions, one based on short-time passwords and one certificate-based, and relate them to the taxonomy of credential stealing and channel breaking attacks. They further outline how these solutions can be easily extended for non-

repudiation (i.e., transaction signing), should more sophisticated content manipulation attacks become a real problem. Providing foolproof security for financial applications is a rigorous activity. Security architect needs to consider various design considerations to make the applications bullet proof.

Some of the factors [4] considered by the Business Signatures solution are:

Credential Risk: User does not have the correct password and other personal identification data expected.

Transaction Risk: User is trying to make a payment over a threshold amount or change passwords or other personal security information.

Location Risk: The user is not coming from an approved or previously authenticated Internet location with an expected Browser Profile and Computer Profile.

Behavioural Risk: The user coming at an unusual time of day, performing a transaction involving an unusual payee, or unusual amount is given and does not match with users' past behaviour.

III. Proposed Model

The main endeavour of the model is to identify the real online banking user from his/her KYC database information. In this model of financial transaction through online we propose single login using user ID and password with CQ for transaction authorization from customer KYC information database before committing a financial transaction. The purpose of CQ is to authorize a transaction in place of OTP. The CQ's are selected to authorize a transaction based on the risk assessment of the user who has initiated the transaction. Those CQs carry higher grade which contains private information of the customer. In this method CQs are chosen from a collection of CQ where the level of the CQ is defined by the risk factors calculation result.

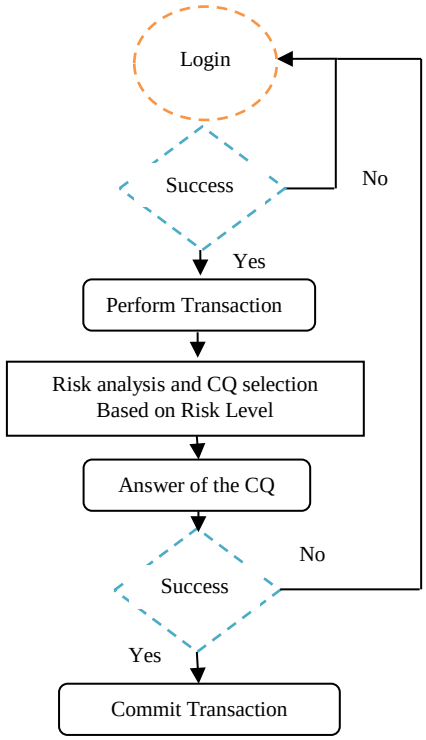

Fig. 1 Transaction authorization model using CQ from KYC database

Risk factors are calculated considering Credential Risk, Behavioral Risk, Transaction Risk and Location Risk. The process works in two stages. First, Risk factor calculating and selecting CQ for transaction authorization and final stage is sending the selected CQs to the customer through mail or SMS before authentication of a transaction.

The brief idea of the model is depicted in the Fig. 1. In the figure the initial step is single factor authentication called login using user ID and password. Analyze transaction performers risk level and select CQ. In the final state verify the transaction performer based on the CQ response. This CQ is the replacement of OTP/mTAN or some other existing 2FA authentication models.

A. *Risk Assessment*

Risk and threat in online transaction depends on various factors. The prime goal of the FIs is to permit right user to access to financial network and restrict others. In this context, we analyse previous activities of the user and calculate similarity between previous and present introducing multiple techniques and algorithms.

1) *Behavioural Risk*:

We have considered there types of behavioural biometrics to assess behavioural risk as users' regular tendency to traverse url path over web application, Users' accessing time, users' taken time interval between the two quickest transaction.

User behaviour is assessed in this scope by computing the probability of the current access time from the previous access times historical log. Activities of the user in the financial application can be collected from the recording of different kind of user activities during his/her uses. For this simulation we have used live activities log from a client's web based application [12] where hour wise access time for a particular user depicts in Fig. 2. Time dependency of the user access has been partitioned hourly basis for each hour in 24 hours.

Number of access of a particular user is C_h, where

$C_h = \sum_{t=h-1}^{t=h+1} a^{t \pm \nabla t}$ and h represents current hour

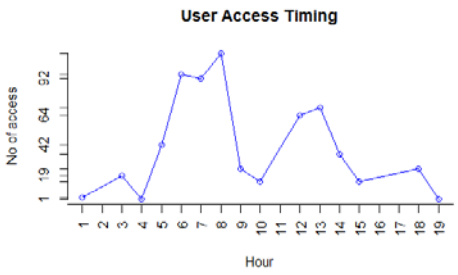

Fig. 2 Historical access time for a user plotted using R studio

From the above behavioural access time data, it has been determined the probability of uses the application in the current time. The probability result determines the selection of CQ which will be assigned to ask for transaction authorization before finally commiting a financial transaction. The probability of the current time from the historical timing of a particular user is calculated using Hidden Markov Model (HMM) (1).

$P(x, \pi) = P(x_1, \ldots, x_N, \pi_1, \ldots\ldots, \pi_N) = P(x_N | \pi_N)\, P(\pi_N | \pi_{N-1}) \ldots\ldots P(x_2 | \pi_2)\, P(\pi_2 | \pi_1)\, P(x_1 | \pi_1)\, P(\pi_1) = P(\pi_1)\, P(x_1 | \pi_1) \prod_{N=2}^{N} P(X_N | \pi_N)\, P(\pi_N | \pi_{N-1})$ (1)

CQ level will be assigned based on the derived probability result. Less probability indicate suspicious or fake user on the

other hand high probability means trusted and real user. Suspicious user is checked by high rated CQ and vice versa.

In this assessment process we measure least time difference between two consecutive transactions from a dataset [12] of a live website. We get user activities time records from the user activities log and assessed over 15 least intervals from the collection, which is figured out in the Fig. 3 bar chart. Fraudsters always try to commit transaction within a short time or using some automated script. Using this evaluation we considered short time intervals between the transactions which will prevent to run script and quick transactions. On the other consideration we assessed user's regular short time intervals between the transactions which will match with user's regular behaviour of transaction to indentify real user.

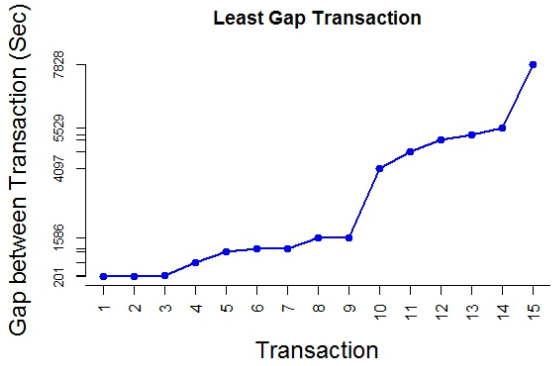

Fig. 3 Least time interval among consecutive quickest transactions plotted by R studio

Any unnatural time space between the transactions will be treated as high risk transaction. If two transactions referred within little time space (30 seconds or less based on the application response time) that will temporarily blocked the transaction and notify the user as it may be generated by fraudster or malicious scripting. In other case if any transaction occurs in less than minimum time interval of users previous activities will result to face a high rated CQ during transaction.

2) Credential Risk

In case of credential risk this paper proposes a strong authentication method as all kinds of credential risk are vital and seldom used i.e personal information changing, failure to provide correct details. This criteria match between the provided input and KYC database existing data. User failure to provide correct answer to the KYC information will be treated as suspicious and high rated CQ will be assigned for further verification.

3) Transactional Risk

Transactional risk assessed based on the KYC profile data limit and regular transaction domain. When user exceeds regular transaction maximum value or is inferior to regular transaction minimum value then it will be treated as suspicious transaction and high rated CQ will be applied during the transaction. In case of user exceeding the transaction profile (TP) upper limit the transaction will block the account temporarily without asking for CQ and any other MFA. From the World Bank dataset [18] to detecting suspicious transaction we calculate standard deviation STD=$\sqrt{\frac{\sum(X-\bar{X})^2}{n}}$, maximums and minimums of the last 30 to 100 transactional data.

Hence, MIN-STD > Suspicious transaction amount > MAX+STD.

4) Location Risk

Location risk has been determined by translating the ip address to geo-location. User will be asked different time to keep record of his/her upcoming movement into the system. The system will compare with the given information and current location prior to committing a transaction. In addition to that hardware address used by the user will be compared with the current hardware (desktop, laptop, mobile, tab etc.). If the hardware used for the transaction is different from all previous hardware/devices the CQ will be harder based on the non similarity.

B. Assigning the CQ from the risk analysis

More personalized information will be high grading and more public questions will be graded as low value. Based on the risk factor taxonomy the challenge question will be carried to the user for further verification during login or prior to the transaction. The TABLE I. describes some of the samples of grading method of the CQ. Frequently Ask Question (FAQ) for the user will pop-up to the user during his work though the application and will update the answer accordingly.

TABLE I. SAMPLE CQ WITH GRADING

Sample Challenge Question(CQ)	***Rating(1-5)***
One of your childhood friends picture with name?	5
Which color you like best?	5
How often you go to abroad?	1
How many devices do you use for online transaction?	5
Usually when do you use the online transaction?	3
What is upper limit of your regular transactions?	3
What is the purpose of online transaction?	1
What is your highest educational degree?	3
What is your profession?	3
Which fruit you like best?	5
Which meal you enjoy more?	5
Your Passport No/Ration Card/ Aadhar Card/Driving License	5
Your Permanent Account Number (PAN) Card	5
Your NID/ TIN/VAT ID Number	5
Your Marriage date?	5
Your spouse born in?	3
User question and answer entry	5
Your first job in? / Your family name?	1
Birthday of your spouse?	3
The Drink you like best? (FAQ)	5
Are you going abroad in coming month? (FAQ)	5
What is your first/last educational institute name?	5

The outcome of the risk analysis select the grade of the CQ as described in the TABLE II.

TABLE II. CQ SELECTION PROCEDURE

Challenge Question	***CQ Level 1***	***CQ Level 2***	***CQ Level 3***
Geo-location change	NO	NO	YES
Transaction device Change	NO	YES	NO
Changing nature of transaction	YES	NO	NO
Changing regular transaction purpose	YES	NO	NO
Exceeding regular transaction frequency	NO	YES	NO
Exceeding regular transaction limit	NO	NO	YES
Exceeding profile transaction limit	Temporarily Blocked and notify		
New user	YES	NO	NO
Exceeding general transaction timing	NO	YES	YES
Transaction excceds TP limit	Temporarily Blocked and notify		
First failure login attempt	NO	NO	YES

Challenge Question	*CQ Level 1*	*CQ Level 2*	*CQ Level 3*
Second failure login attempt	NO	YES	YES
Third failure login attempt	YES	YES	YES
Forth failure login attempt	Temporarily Blocked and notify		

CQ sends to the customer's email or SMS to the mobile shows in the Fig. 4.

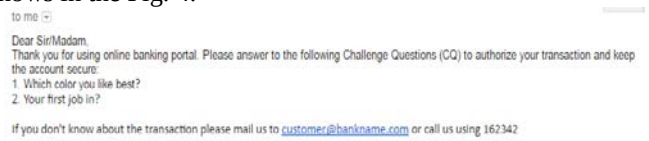

Fig. 4 Transaction authorization CQ to the customer email

Answer to the CQ sends via SMS or email should enter into the online banking portal for authorization a transaction.

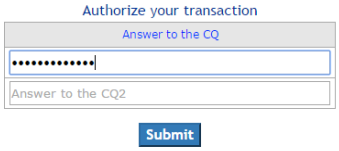

Fig. 5 Answer to the CQ from email of SMS

IV. Result and Comparative Analysis

This paper proposes an alternative method of authorize/signing for financial transaction through the internet. It is a method to minimize financial fraud forgery on online financial network. The main challenge to avoid fraudulent activity in the financial network is keep the system away from unauthorized person. The proposed method presented here includes sensitive personal information called KYC information to verify the actual owner of the account for online financial activity. It considers all the known and upcoming possible way to theft information and unauthorized entry into the online financial system. The dimension to the risk of the hacking and information stealing is unlimited and tendency for these illegal operations evolving time to time; the method proposed a way to extend the KYC database as required by risk assessment in a certain intervals. As the FIs already preserved customers KYC so, it is effective and fruitful to continue reuse of KYC data for authentication purpose rather than using additional cost involved mechanism.

By this approach the evolving security threat will be minimized in a significant stage, moreover the model performance is preserved and improved eventually in each user activities. Authentication measures are a dynamically assigned procedure to restrict transaction from the unauthorized user. In this process it is recommended to user CQ in lieu of OPT/mTAN described in TABLE I. CQ is graded in various level of standard from 1 to 5 with an independent mechanism based on the heuristic result of the risk.

In this paper we used users' own attributes to indentify a real user and a verfication method by using his/her own attributes from KYC database information. KYC is the most secrete and private information to identify a particular account holder in the FIs moreover simulation shows mitigated all possible ways of compromizing the system. We can state that the proposed system will ensure equal security as existing OTP/mTAN.

CQ generate from the separate message server and send to the users mobile or using email in that case man-in-the-middle (MITM) attack prevent by the system itself as users input taken from to web interface to verify later in the verification module. Comparison of traditioanl model and proposed model dipicted shown in the TABLE III.

TABLE III. Comparison security properties traditional scheme and our proposed model [4]

Attacks	**OTP/mTAN**	**KYC based CQ**
Evesdropping attack	✓	✓
Replay attack	✓	✓
Dictionary attack	✓	✓
Brute force attack	⌂	✓
Man-in-the-middle attack	X	✓
User impersonation attack	✓	✓

Notation: √ Satisfied ⌂ Partially Satisfied × Not Satisfied

V. Conclusions

In this paper, we propose dynamic KYC based transaction authorization method to ensure secure and flawless financial access to the actual account holder of the online bank. Analysis and simulation results show that the proposed method provides equal control as existing OTP authorization minimizing some dynamic risk of being stolen and delay delivery of SMS. Our proposed method is costless and does hurdle to carry an additional hardware. As there is no chance of key theft this method can be used anywhere from private or public computer. Our method will ensure dynamic security by tackling most of the vulnerabilities in internet based financial transaction.

References

[1] Know your customer (KYC) laws by country. [Wikipedia] Available: https://en.wikipedia.org/wiki/Know_your_customer

[2] FATF, GAFI. "Guidance on the risk-based approach to combating money laundering and terrorist financing," June 2007.

[3] FFIEC Guidance: Authentication in an internet banking environment, federal financial institutions examination council (FFIEC), Retrieved February 4, 2006.

[4] Wen-Bin Hsieh, Jenq-Shiou Leu, "Design of a time and location based one-time password authentication scheme," 2011 7th International Wireless Communications and Mobile Computing Conference (IWCMC), pp 201-206, 4-8 July 2011.

[5] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Khurram Khan, "OTP-based two-factor authentication using mobile phones," Eighth International Conference on Information Technology: New Generations (ITNG), pp. 327-331, 2011.

[6] Waqar Ahmad Khan, Ghalib Asadullah Shah, Yasir Saleem and Amjad Farooq, "Modified mobile transaction authentication number system for 2-layer security," Intelligent Systems Engineering (ICISE) International Conference, 15-17 Jan 2016.

[7] Alain Hiltgen, Thorsten Kramp, Thomas Weigold, "Secure internet banking authentication," IEEE Security & Privacy, vol.4, no. 2, pp. 21-29, March/April 2006.

[8] Shailesh Kumar Shivakumar, Babu Krishnamurthy, "Advanced security design for financial applications, External Document," White paper of Infosys 2016.

[9] Syeda Farha Shazmeen, Shyam Prasad "A practical approach for secure internet banking based on cryptography," International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012.

[10] Lior Golan, Amir Orad, Naftali Bennett, "System and method for risk based authentication," U.S. Patent US 20050097320 A1, May 5, 2005.

[11] World Bank dataset Available:https://finances.worldbank.org/Financial-Intermediary-Funds/Financial-Intermediary-Funds-Cash-Transfers/h4s8-nwev

[12] Data Set from clients live website Available: http://reporting4results.com/actiontracker/login.php