A Secured Way to Enhance Online Banking Transaction

Maleeha Khan, Vinjam Likitha, G. Vijay Kumar

Abstract: ***The need for security in online banking is popular due to various cybercrimes emerging in recent years. As of now existed framework contains numerous sorts of strategies like One Time Password (OTP), Biometric Authentication, Mobile Transaction Authentication Number (mTAN) and some more. So, based on the various cyberattack issues taking place while committing financial transaction we proposed the idea of introducing challenge questions (CQ) to provide security at the time of transaction. This paper aims at intensifying a secured transaction in online banking wherein we add a security layer to the existing OTP methodology which contains challenge questions (CQ) from Know Your Customer database. After successful login of account we have to answer the CQ and then enter the OTP for final transaction.This methodology provides a secured way to transfer money from our accounts and make it secure.***

Keywords—Security, Know Your Customer, Challenge Question, Online Banking, One Time Password.

I. INTRODUCTION

As in the level of security the transactions frauds are increasing day by day. The need for highly secure identification and personal verification information systems are becoming extremely important especially in the banking and finance sector. As there are more number of technologies in todays internet banking like phishing, fake emails and phone calls imitating to be sent from banks, trojan horse programs to capture user ids and passwords so it is very important and urgent need to enhance the internet banking security system.Internet banking is an appealing method for working together just as doing all financial movement autonomous of area. Anyway validation strategy for web based money related framework is as yet seeking after to guarantee largest amount of security. The most outstanding feature of online banking is its convenience. Online banking provides the ability to carry out banking transactions in comfort of their homes or offices.

Know your customer as the name implies banks are required by regulators to know whom they are dealing with those methodology deals with some regulators for a natural person they need to know:

Identity**:** All the details listed on the identification document such as full name, date and place of birth, nationality, residential address etc.

Revised Manuscript Received on April, 07, 2019.

Maleeha Khan, Department, of ECM, Koneru Lakshmaiah, Education, Foundation, Vaddeswarm, A.P, India.

Vinjam Likitha, Department, of ECM, Koneru Lakshmaiah, Education, Foundation, Vaddeswarm, A.P, India.

Dr. G. Vijay Kumar, Department, of ECM, Koneru, Lakshmaiah ,Education, Foundation, Vaddeswarm, A.P, India.

Political Status**:** Whether the client or his/her relative is holding on to any prominent political appointment.

Criminal Links**:** Whether the client is linked to any financial crime, terrorism or sanctions.

Source of Fund**:** The source of fund has to be legal.

Expected Volume Of Transaction**:** If there is an exceptionally large amount of money involved in the transaction the bank need to ensure that the source of fund is legal.These are the requirements of the KYC process and includes following steps:

ClientOnBoarding**:** The bank establishes a relationship with the client and collect all the documents for identification.

Screening: The client will be checked against a database for name matches other sanctioned persons. If there are no matches they can carry on with their business relationships,if there are matches,the compilence officers will begin their painful process of verifying whether the matches are real or false.If it is false match then its not verified else they will need to decide what to do with the client now that there is a match with the database. If the client is a criminal or terrorist linked they probably they need to freeze the amount and submit a report to the authorities. Another form of this method is to monitor the transactions and figure out unusual transactions. If the transaction is out of the norm, the bank need to verify that nothing fishy is going on.*Repeat Screening*: The screening process will repeat periodically as the client status and the database may change over time.

II. RELATED WORK

There is classification of headways and systems financial institutions (FIs) can use to affirm exchange of the clients. These classifications use many kinds of methodologies such as user passwords, Id numbers (PINs), One-time passwords [4][5][9]. Usage of various types of tokens or USB plugins, trade profile substance, biometric recognizing confirmation and various more. The measurement of risk shifts with each technique used and its results should depend upon the eventual outcomes of the cash related establishment's danger assessment process[4][11].Security issues related with current Mobile Trade Authentication Number (mTAN) System are discussed and few modifications in the existed structure are proposed for using mTAN in a certainly secure way by Waqar Ahmad Khan,2016[6].Tejendra Pal Sing Brar states in his paper that Online Banking is an emerging technology which comprises various capabilities as well as potential problems, the users are tentative to use the system.

Usage of Online Banking has brought many concerns from different perspectives in the form of government, businesses, banks, individuals and technology[7].

III. PROBLEM DEFINITION

The main venture of the model is to distinguish the authentic user in online banking from the information available from the KYC database information. It thinks about all the known and future conceivable approach to burglary data and unapproved passage into the online cash related framework we propose dynamic KYC based exchange approval strategy wherein we need to respond to the test questions and afterward enter the OTP for further last exchange to assure security and grant access to the user holding an account in the bank.The purpose of CQ is to authorize a transaction along with the existing system of OTP to make the transactions more secure. The CQ's selection is based on the risk analysis done by the user who has initiated the transaction. The Challenge Questions contains questions to answer. The method what we proposed will ensure dynamic security by tackling most of the vulnerabilities in online banking transactions.

The CQ contains inquiries to be answered. Our strategy will guarantee dynamic security by handling the greater part of the vulnerabilities in web based cash related exchanges.

IV. METHODOLOGY

Hazard factors are determined considering various types of risks which namely include Credential, Behavioural, Transaction as well as Location risks.The procedure works in two steps firstly, calculating the risk factor and selecting the CQ for approval of transaction and after answering the CQ and the second phase starts with OTP sending.

Risk Assessment: Hazard and danger in online banking relies upon different variables the prime goal of FIs is to enable legal access for online banking and checking those with the past strategies for the customer and make sense of the closeness among the past and present techniques.

Credential Risk: In case of credential risk a wide range of certification chance are crucial and only from time to time utilized i.e individual data changing , neglected to give right subtleties. This criteria arrange between gave information and KYC data base existing information client fail to give right reaction to the KYC information will be taken as suspicious and high assessed CQ will be figured out for further check.

Transactional Risk: It is based on the limitation of the transaction provided which will be treated as suspicious in case of maximum as well as minimum value after which high CQ will be applied during the transaction.

Location Risk: It is based on the geographic location to figure out the threat by understanding the IP address of the location which request to maintain the record in the system where the CQ sends to the user's email or SMS to the flexible reaction.

The main idea of providing security while a transaction is taking place is to ensure a safe and secure transaction. From the block diagram as shown the process begins wherein initially the user has to login with his/her account number and enter the password where the access is granted. Later, after successful login of the account then selection of transaction process takes place such as transferring of funds, online shopping, and many more. After the Selection of transaction the user has to answer the challenge questions(CQ) as it a one layer of security what we have added to the existed system of OTP. Then, after successful answering of the CQ an OTP is send to the mail id or mobile number of the user. So, in final transaction of online banking the user should enter the OTP for the successful banking. This kind of methodology helps the user to keep his/her account secured without any cyber crimes taking place while he is performing transaction.

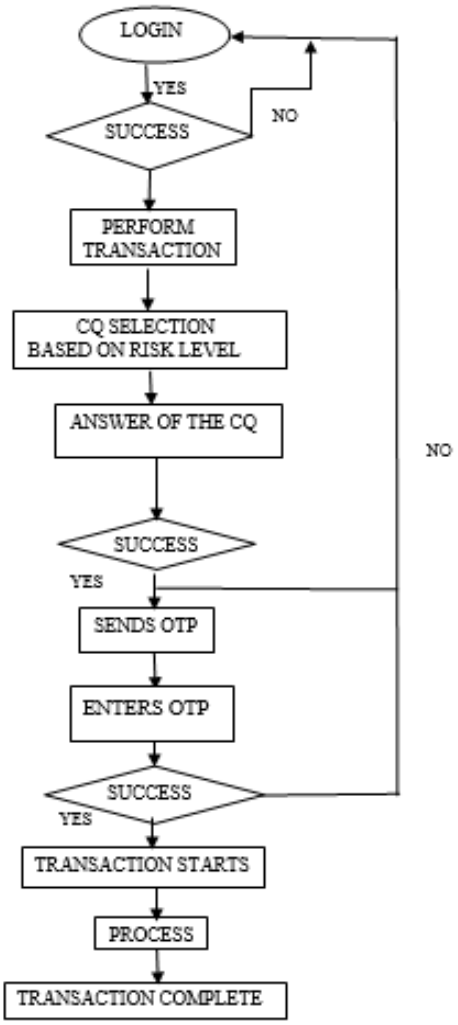

Fig.1.Block Diagram For Online Transaction

V. RESULTS AND COMPARITIVE ANALYSIS

This paper proposes an elective technique for approve/marking for online banking through the web. It is a technique to limit financial frauds on online banking issues. The fundamental test to overcome the frauds in online banking is fend off the framework from unapproved individual. The proposed technique introduced here incorporates delicate individual data called KYC data to check the genuine user of the record for online banking facility. It thinks about all the known and forthcoming conceivable approach to burglary data and unapproved section into the online banking framework.By this methodology, the advancing security danger can be limited altogether. In addition, the model execution is protected and improved in the end in every client action. Validation measures are powerfully relegated to make the framework increasingly dependable and keep the unapproved client out of the entire procedure.In this technique we use users' own attributes to identify the user details and verify from the KYC database information. KYC provides information of the user for checking out the identity and granting access to the account. From both the tables below shown we get the comparison of the methodologies used and their rates by which they attacked by the hackers and the time complexity measured.

ATTACKS	TRADITIONAL SCHEME	CQ and OTP
Evesdropping attack	✓	✓
Brute Force attack	□	✓
Dictionary attack	✓	✓
Replay attack	✓	✓
Man in middle attack	×	✓
User impersonation attack	✓	✓

TABLE I. COMPARISON OF THE EXISTED AND PROPOSED SYSTEM

Methodologies Used	Chance of Attacks	Time Complexity
One Time Password	High	High
Email Confirmation	Medium	Medium
Fingerprint Sensing	High	Medium
Face Detection	Medium	High
Voice Detection	High	Medium
Challenge Questions With OTP	Low	Medium

TABLE II. COMPARISON BASED ON THE ATTACKS AND TIME COMPLEXITY

VI. CONCLUSION

Security plays an important role in online banking as there are many ways to secure online transaction. As there are in number of ways to secure the unauthorized access in online banking through various techniques. So, we introduced the CQ as it plays a main role while performing transaction it reduces the risk of the system to get hacked from unknown sources resulting in cyber crimes to the existed OTP methodology for further security purpose. This methodology used in online banking is quite costless and does not carry any additional hardware. Our methodology will guarantee dynamic security issues by overcoming the threats emerging in online banking.

REFRENCES

1. Wikipedia, "Know your customer (KYC) Laws by country".
2. Transaction Authorization from Know Your Customer Information in Online Banking, 9th International Conference on Electrical and Computer Engineering.
3. Know your customer (KYC) laws by country. https://en.wikipedia.org/wiki/Know_your_customer.
4. FFIEC Guidance: Authentication in an internet banking environment (FFIEC), Retrieved February 4, 2006.
5. "Design of a time and location based one-time password authentication scheme," Wen-Bin Hsieh et.al, 2011 7th (IWCMC), pp 201-206, 4-8 July 2011.
6. "Modified mobile transaction authentication number system for 2-layer security," Waqar Ahmad Khan et.al, Intelligent Systems Engineering (ICISE) International Conference, 15-17 Jan 2016.
7. "Vulnerabilities in e-banking: A study of various security aspects in e-banking", Tejinder Pal Singh Brar et.al, International Journal of Computing & Business Research, ISSN (Online): 2229-6166 (FFIEC), "Authentication in an Internet Banking Environment," Retrieved February 4, 2006.
8. "Design of a time and location based one-time password authentication scheme," Wen-Bin Hsieh et.al, 2011 7th International Wireless Communications and Mobile Computing Conference (IWCMC), 4-8 July 2011] .
9. "Advanced security design for financial applications, External Document," Shailesh Kumar et.al, White paper of Infosys 2016. John Trader-(2014) 'Impact of Biometrics in Banking'-IEEE Transaction-Vol 54.
10. 'An identity Authentication System using Fingerprint' Anil K. Jain et.al, IEEE Transaction-Vol 86 No. 10 1998.
11. "System and method for risk based authentication," Lior Golan et.al, U.S. Patent US 20050097320 A1, May 5, 2005.
12. Available:https://finances.worldbank.org/Financial-IntermediaryFunds/Financial-Intermediary-Funds-Cash-Transfers/h4s8-nwev, World Bank dataset.
13. "Online Banking Security Flaws: A Study", Rajpreet Kaur Jassal et.al, International Journal of Advanced Research in Computer Science Engineering, Volume-03, Issue-08, ISSN-2277 128X , August 2013.
14. "Security Issues in E-Banking Services in Indian Scenario", Mr. Shakir Shaik et.al, Asian Journal of Management Sciences, Volume-02, Issue-03, pp.(28-30). ISSN: 2348-0351, March 29, 2014.
15. "Internet banking authentication methods in Nigeria Commercial Banks," O.B. Lawal et.al, African Journal of Computing &ICT, Vol 6. No. 1, March 2013.