Two Factor Authentications in Internet Banking

Mr. Vinayak Gandhi[1] Mr. Rohit Jadhav[2] Mr. Chetan Mane[3] Mr. Mangesh Gosavi[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Rajendra Mane College of Engineering and Technology, Ambav, Mumbai University

Abstract— Two factor authentications in internet banking system describes a method of implementing connectionless two factor authentication using mobile phones in the field of Internet Banking. The proposed method guarantees that authenticating to services, such as online banking transactions is done in a very secure manner. The proposed system involves using mobile phones a token for One Time Password generation (OTP). The generated One Time Password is valid for only a short user defined period of time and is generated by some random algorithm and verified using Secured Cryptographic Algorithm. Additionally, an SMS-based mechanism and tracking user behavior method is implemented as there is large area of concern in security. In this system implementation we have also focused on the security which is provided to the user during the online banking transactions. Thus the proposed system is also adding the extra layer of security at the point where you enter information online. The service helps to prevent unauthorized access to users account before it happens by confirming your identity by providing additional security messages.

Key words: OTP (One Time Password)

I. INTRODUCTION

A. *Two-Factor Authentication*

Two-factor authentication provides a significant increase in security over the traditional username/password combination. The two factors of two factor authentication are: something you know and something you have. In the single-factor world of authentication, the password was the "something you know" part. The additional factor, "something you have", is the key component. The something you have component can either be tokens, smart cards, pin/tan's, and biometrics (to be discussed later). Tokens display a set of numbers on a small screen. Usually, the set of numbers (OTP) changes every minute. This number then is joined with the user's password, or pin number to create a passcode. A correct passcode then authenticates the user to access the secure resources. Smart Cards are used in combination with a Smart Card reader. The user will insert the card and the card sends an encrypted message to the website or, the reader displays a unique code that the user will enter.

B. *Pros and Cons of Two-Factor Authentication*

While two-factor authentication may seem like the perfect cure-all for securing networks and resources, there are many security holes that this type of authentication will not protect against. Fake websites provide would-be hackers a way of getting personal information from individuals. The 'store-front' looks authentic, and the user ends up entering information like credit card numbers, social security numbers and bank account information directly into the hands of an identify thief. Two-factor authentication can not protect someone against this type of man-in-the-middle attack. Another type of security breech is if the would-be hacker already has access the computer itself. Then when the user accesses either company or internet resources, the attacker then attempts to piggyback on the transmission and either perform fraudulent transactions, or access secure resources. Trojan horse attacks like this one also cannot be prevented with two-factor authentication.

II. LITERATURE REVIEW

Research has been made on 'two factor authentication using BESTOKEN' where R. Groom (author) [1] has mentioned about using a smart phone as token for the authentication. This involves implementing both connection oriented as well as connectionless authentication system. System focuses on creation of the OTP on server side and sending it to the clients.

Two factor authentication has widely used in banking section today. The bank of America is providing the two factor authentication to it millions of users providing them hardware tokens described by D. Ilett [2]. While tokens provide much safer environment to users, it can be costly to most of the organizations. The banks have to also be ready for token replacement if a token breaks or get stolen.

Mannan and van Oorschot describe MP-Auth [4]: another system that uses a trusted mobile device such as a smart-phone to enter the password. The device encrypts the password using the end server's public key before passing it to the untrusted terminal. MP-Auth also requires channel between the trusted device and the untrusted machine. The public keys of the sites to be accessed are once again loaded onto the user's device, which prevents the untrusted machine from mounting a (MITM) attack.

We propose a mobile (smart phone) based software token that need to be install on the device. Our system reduces the work on server side by providing user an OTP generation application, which can be used whenever user wants to perform secure online tasks, reducing the extra telecommunication charges. Two factor authentication systems in internet banking focuses more on the algorithms like AES-DES, RSA algorithms that are used for encryption and decryption process. In active attacks like Man in the middle attack the attacker is providing the fake websites forcing the user to enter the private information. Hence to minimize all possible damages the one time passwords that are generated are encrypted and sent over the internet to the server side minimizing the MITM attacks. The additional and important part included in this system is monitoring users behaviour so that minimizing the possibilities of hacking the users sessions of transactions. Therefore considering all possible attacks this system aims towards reducing the adjustments to be done by the user and providing safe and secure online transactions.

III. PROPOSED SYSTEM

The Two factor authentication system in Internet Banking mainly aims towards the security during the banking transactions done by the user. It also focuses on the handling and creation of One Time Password (OTP) application on the user's device (smart phones). The other valuable part in our system is the Behaviour tracking method and session handling where based on the user's previous transaction history the behaviour of the user is recorded. If server detects the abnormal pattern while handling the user his account then server will send the message to validate the user from his device (smart phone).

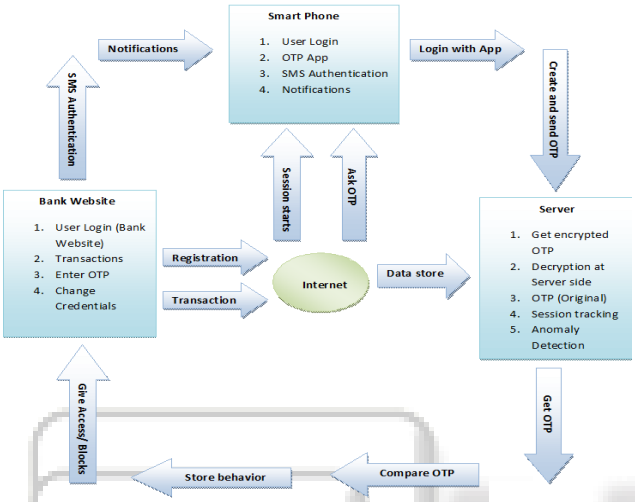

Fig. 1: Architecture of Two factor Authentication System

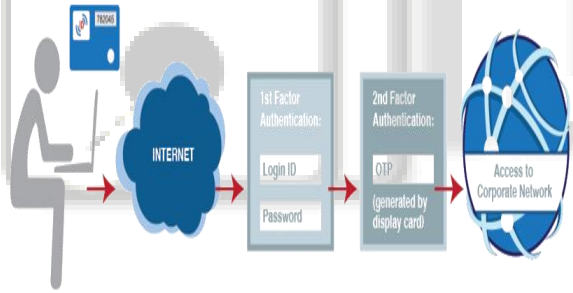

Fig. 2: Actual Authentication Process

IV. IMPLEMENTATION DETAILS

A. Algorithms

1) Advanced Encryption Standard (AES) Algorithm

The OTP generated on application is encrypted and send to the server where it gets decrypted. We used here Advanced Encryption standard algorithm (AES) to encrypt OTP, providing an extra secure way for sending the secret data.

The operations of Algorithm can easily be broken down to the following functions:

1) ADD ROUND KEY
2) BYTE SUB
3) SHIFT ROW
4) MIX COLUMN

B. Modules

1) Design of E-Banking Website

E-Banking website is designed to show how user can perform different operations on website. It also focuses on providing extra security while performing transactions by generating OTP in application and entering it on the website. E-Banking website also tracks the behaviour of the user like which links and pages currently user is accessing.

2) Generation Of OTP On Application

The OTP is generated using Random Algorithm. In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it's very important to develop a secure OTP generation algorithm which will run on user's mobile phone. Several factors can be used by the OTP algorithm to generate a password which is difficult-to-guess. Users seem to be willing to use simple factors such as their mobile number and a PIN for services. The OTP is valid for some user defined period of time.

3) Encryption Using AES

The OTP generated on application is encrypted and send to the server where it gets decrypted. We used here Advanced Encryption standard algorithm (AES) to encrypt OTP.

4) Session And Behaviour Tracking

Behaviour tracking takes advantage of this fact combined with knowledge of online banking fraud attacks and general online behaviour to determine if a specific online session is legal or has high risk of being fraudulent.

Here is how the process of anomaly detection is divided and the solutions used to detect suspicious activity for each individual user:

1) Create and update a model/pattern of expected behavior for each individual user.
2) Maintain every online banking session for each individual account holder.
3) Analyze all individual account behavior during an online banking session from login to logout — how user access his account, how user manage his accounts, the types of transactions user is included in, the frequency of activities, what kinds of activities take place during the same session and much more.
4) By comparing individual or groups of activities in this online session to identify the patterns of normal behavior, determine if the session is legal or unexpected, or suspicious.
5) SMS-Based Authentication System

The SMS authentication system gets activated after abnormal or suspicious behaviour is detected. When user performs any activity which was not previously done by that user then SMS message is sent to the user and administrator. It tells user to verify his identity and administrator to take necessary actions after abnormal behaviour is detected.

V. APPLICATION

Two factor authentication using smart phone in internet banking being a current topic of interest. It provides its services in various fields of online tasks and transactions such as online banking, e-shopping, ATM transactions (tokens) and many other online applications. It also has the potential to be further used in Social linking applications. An efficient two factor authentication system has the ability to provide various services related to security and is beneficial for user.

VI. CONCLUSION AND FUTURE SCOPE

This system focuses on the implementation of two-factor authentication methods using mobile phones. It provides an

overview of the various parts of the system and the capabilities of the system. The proposed system is implemented to encourage the user to perform the tasks (transactions) very securely. Storing and monitoring the users behaviour is one of the main working areas of this system. The system has several factors like use of secure algorithms that makes it very difficult to hack.

The only thing constant in this world is change. There is always room for improvement or change in any software and our system is no exception. GUI implementation can be put to a wider scope. Also, its processing tie can be taken into focus while implementation.

ACKNOWLEDGMENT

We would like to express our sincere gratitude towards our guide, Prof. Gosavi M.K., for the help, guidance and encouragement, he provided during the BE Project. This work would have not been possible without his valuable time, patience and motivation. We thank him for making our stint thoroughly pleasant and enriching. It was great learning and an honour being his students. We are deeply indebted to Prof. Naik L. S. (Head of Department) and Prof. Gamare P.S. (Project Coordinator) and the entire team in the Computer Department. They supported us with scientific guidance, advice and encouragement, they were always helpful and enthusiastic and this inspired us in our work. We take the privilege to express our sincere thanks to Dr. Bhagwat M. M. our Principal for providing the encouragement and much support throughout our work.

REFERENCES

[1] R. Groom, "Two Factor Authentication using BESTOKENpro USB TOKEN." Available at http://bizsecurity.about.com/od/mobilesecurity/a/twofactor.html
[2] D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers," 2005. Available at http://www.silicon.com/financialservices/0,3800010322,39153981,00.html
[3] Florencio, D.,Herley, C.: A large scale study of web password habits. In:Proceedings of the International conference on World Wide Web (WWW 2007), pp.657-666 (2007).
[4] Mannan, M., Van Oorschot, P.C.:Using a personal device to strengthen password authentication from untrusted computer, technical report TR-07-11(March 2007), http://www.scs.carleton.ca/research/tech_reports/
[5] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," inInside Risks 178, Communications of the ACM, 48(4), April 2005.
[6] FadiAloul, Syed Zahidi, Two factor authentication in internet banking, Proceedings of the IEEE International Conference on Computer Systems and Applications, pg. 641-644, 2009.
[7] Anders Moen Hagalisletto, Arne Riiber, Using the mobile phone in two-factor authentication, Proceedings of the 1st International Workshop on Security for Spontaneous Interaction, IWSSI 2007, Innsbruck, Austria, 2007.

