Two Factor Authentications using Smart Phone 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 specific algorithms like TOTP 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

Today security concerns are on the rise in all areas such as banks, governmental applications, military organization, educational institutions, etc. There are several issues when it comes to security concerns in these widely spread and varying industries with one common factor being passwords. Most systems today depend on static passwords to verify the user's identity. But these passwords come with major security concerns. A common user can use easy to guess passwords, can use same password for multiple accounts in online and social networking area. However, hackers have many options of using techniques to steal these passwords such as snooping, sniffing, MITM and guessing, etc. Some strategies have been proposed for using the passwords. Some of which are very difficult to use and others might not meet the companies or organizations security concerns. Two factor authentication using devices such as tokens have been proposed to solve the password problem and are seen to be difficult to hack. Two factor authentications also have disadvantages which include the cost of purchasing, issuing, and managing the tokens. From the user's point of view, using two-factor authentication system for multiple systems requires carrying multiple tokens/cards (hardware tokens) which are likely to get lost or stolen. Now in the world of smart phones a mobile can be used to do many useful things. The research has been made evolving the use of mobile phones (smart phones) as a token given the advancement in hardware and software industries for many authentication systems. Several mobile banking services available take advantage of the improving capabilities of mobile devices. From being able to receive information on account balances in the form of SMS messages to using WAP and Java together with GPRS to allow fund transfers between accounts, stock trading, and some banking related transactions. Installing the applications provided by the company's panel to get more benefits from the services like online fund transfer, news services and receiving the notifications in no time. Consequently, using the mobile phone as a *token* will make it easier for the customers to deal with multiple two factor authentication systems; in addition it will reduce the cost of manufacturing, distributing, and maintaining millions of tokens. In this paper, we propose and develop a complete two factor authentication system using mobile phones (smart phones) instead of tokens or cards and also provide security for user's authentications on mobile device i.e. pattern locks (passwords) also maintaining log of each individual's activities on server. The system consists of a server connected to GSM modem and a mobile phone client running on an android application. User has the choice to create his own OTP whenever he wants to do the transactions. The approach used here is an SMS-based approach that is also easy to use and secure, but more expensive. OTP generation on the client's side is the main aim of system making it more secure as there may not be the same information available for attacker on the other end.

II. LITERATURE REVIEW

1) 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.
2) 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.
3) 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.
4) 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 behavior 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 Anomaly Detection 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).

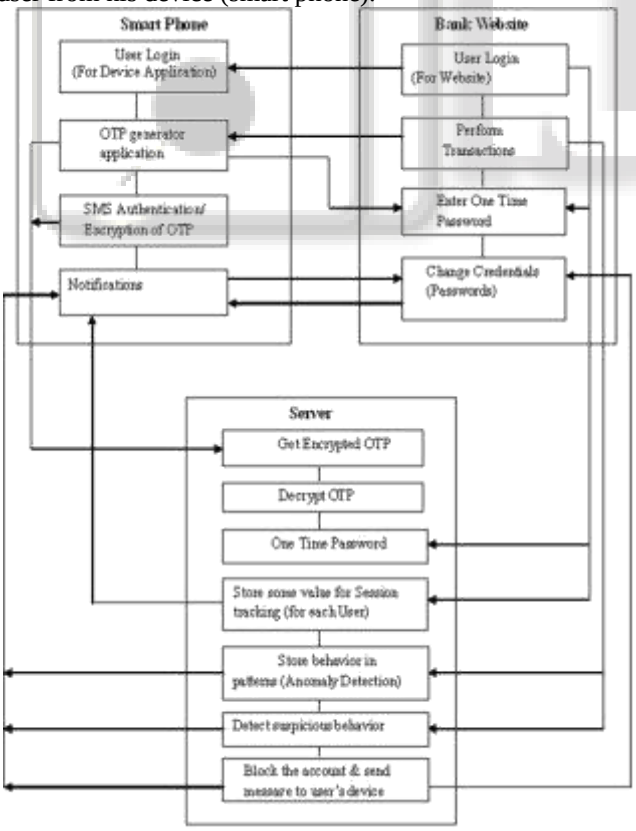

Fig. 1: Architecture of Two factor authentication system.

Fig. 2: Actual authentication process.

IV. IMPLEMENTATION DETAILS

A. *Algorithms*

1) Time-based One Time Password (TOTP) Algorithm:

TOTP algorithm is specifically implemented for One Time Passwords (OTP) generation. OTP generation is done with the help of hash function.

2) AES-DES Hybrid Algorithm:

Instead of using one single Encryption algorithm we are using here the combination of AES and DES algorithms called as Hybrid Algorithm, providing an extra secure way for sending the secret data.

The basic idea of the proposed hybrid algorithm is to integrate AES into each iteration of the fiestal network of DES. Mathematically, each round of the model can be expressed as:

$$L_n = R_{n-1} \quad (1)$$

$$R_n = \text{AES}\,(L_{n-1} \text{ XOR } R_{n-1} \text{ XOR } K_n) \quad (2)$$

The above set of equations is repeated over each of the 10 rounds.

The input block of 256 bit data is split into two halves, the left and right. For each round n, XOR function is carried out.

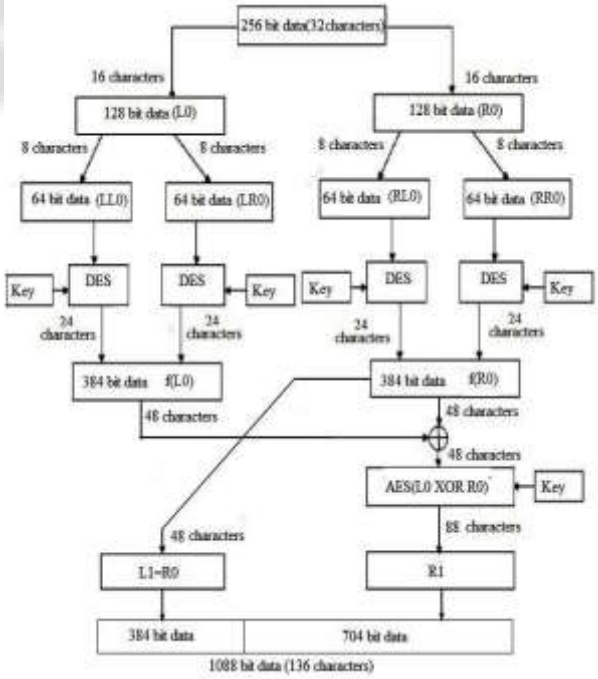

Fig 3: Hybrid Encryption Flow

3) Clustering techniques/K-Means:

This algorithm is best suited for Anomaly detection. Clustering techniques (algorithms) such as k-means, hierarchical clustering is used for identifying or storing the user's behaviour in the form of patterns.

k-Means Clustering is an algorithm that attempt to find groups in the data (Alpaydin 139). In pseudo code, it is shown by Alpaydin (139) to follow this procedure:

Initialize $\mathbf{m}_i$, i = 1,…,k, for example, to k random $\mathbf{x}^t$
Repeat
  For all $\mathbf{x}^t$ in X
    $b_i^t \leftarrow 1$ if $\| \mathbf{x}^t - \mathbf{m}_i \| = \min_j \| \mathbf{x}^t - \mathbf{m}_j \|$
    $b_i^t \leftarrow 0$ otherwise
  For all $\mathbf{m}_i$, i = 1,…,k
    $\mathbf{m}_i \leftarrow$ sum over t ($b_i^t \mathbf{x}^t$) / sum over t (b_i^t)
Until $\mathbf{m}_i$ converge

The vector **m** contains a reference to the sample mean of each cluster. **x** refers to each of our examples, and **b** contains our "estimated [class] labels" (Alpaydin, 137).

B. Modules

1) Connection-Less Authentication System

A onetime password (OTP) is generated on the user's mobile device without any interference of the server. The mobile phone will act as a token and use certain algorithm using hash functions to generate a one-time password locally. The server will have all the required factors including the One's unique to each mobile phone in order to receive the same password at the server side and compare it to the password submitted by the client on the bank's website. The client may submit the password online. A program (application) must be installed on the client's mobile phone to generate the OTP.

2) SMS-Based Authentication System

In order for the server to verify the identity of the user, the mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns rights to do the transactions based on the randomly generated OTP to the mobile phone. The user will then have a given amount of time to use the OTP before it expires. Note that this method will require both the client and server to pay for the charges of sending the SMS message.

3) One Time Password (OTP) Algorithm:

The OTP generation is done using TOTP algorithm using Hash function. 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 difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services. Note that these factors must exist on both the mobile phone and server.

4) Hybrid Algorithm implementation

Instead of using one single Encryption algorithm we are using here the combination of AES and DES algorithms called as Hybrid Algorithm, providing an extra secure way of transmission of the secrete data from client to server and vice versa.

5) Anomaly Detection and Session tracking

The anomaly detection approach focuses on the individual user. Different users quite naturally have different online banking behaviour from each other. Each user has a unique online banking identity. Anomaly detection 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.

V. Application

Two factor authentication using smart phone in internet banking being a current topic of interest, it is still in its research phase. 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 multiple 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-I. 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. Bhagawat 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.

