An Effective Protocol to Resist Password Stealing Attacks and Fake accounts in Social Sites

R.Danu[1], A.Raviraman[2], R.Gurumoorthy[3], G.Guber Sambath[4]

[1]*Assistant Professor, Sri Manakula Vinayagar Engineering College, Pondicherry-605104, India*
[2, 3, 4] *Dept. Of Information Technology, Sri Manakula Vinayagar Engineering College, Pondicherry-605104, India*

[1]danu_ramachandran@yahoo.co.in
[2]raman392@gmail.com
[3]rgurumoorthy.it@gmail.com
[4]gubersambath@gmail.com

Abstract – The internet plays a major part in our day to day activity and it provides various information on basis of their needs and work. But we need to consider the pros and cons of the internet. There are many advantages of the Internet that show you the importance of this new medium. One of the most negative aspects of the impact of the internet on our daily life is, that it alters the social behaviour, habits and abilities of people which includes the anti social activities and identity thefts. The identity theft is an emerging and a major threat in the current trend in the internet world. The proposed system involves the secured registration process. The main objective of our system is to provide a secured portal during the user registration process in any social sites. The user's information is validated for their originality in this secured portal using the Aadhaar ID and the Central Identity Data Repository (CIDR).We also provide a resistant protocol to encounter the password stealing attacks with the aid of oPass Methodology. This system minimizes the users from creating accounts in various social sites with fake details or identities. It includes a secured registration phase, login phase and recovery phase.

Keywords: User Authenticaiton, Password reuse attacks, Password stealing Attacks

I. INTRODUCTION

The main aim of our proposed system is to minimize the online fraudulent activities that occurs frequently. First the user has to be authenticated for his/her originality, for that purpose we use a Smart ID (Aadhaar ID) to establish the identity of the users online. The Aadhaar ID contains all the personal information of the individual and also documents such as Voter ID, Ration card and Biometrics such as Face, Iris, and Fingers. The user's data is verified because in the current system the user creates an account in much easier way by providing information as they wish and it may not even belong to person who exists in the country or world.

There is a big influence of technique on our daily life. Much of the legal discussion around the social sites today focuses on a key concern: fraud. The Identity theft Although many users are voluntarily tweeting and posting on their daily lives, this sometimes occurs involuntarily. In growing numbers, people find themselves exposed to fraudulent behavior, with others impersonating them on various sites through fake accounts.

The fake social media accounts can cause drastic effects In the social networking environment. That can happen to anyone, the adverse effects of fake accounts results leads to,

i) Indulging a schoolboy who twitters on behalf of the school director,
ii) A fan who twitters on behalf of the artist, and
iii) A student who twitters on behalf of the Prime Minister.

Another aspect of our project is to produce a system in to resist the password stealing attacks and the password reuse attacks. In this project the user is given with a long-term password by the help of which the user generates the OTP for the current login session. The generated OTP is valid only for that current session and thus this Pin (OTP) is of no use for the next session.

Our System includes the following advantages over the existing system

Phishing Protection:

Adversaries often launch phishing attacks to steal users' passwords by cheating users when they connect to forged websites. Our project allows a secured way of login by which the user's password are kept safe.The Users who adopt oPass are guaranteed to withstand phishing attacks.

Secure Registration and Recovery:

In our system, the registration is carried out in a secured way to validate the user's information for their originality using Aadhaar ID.Once the user wants to register in a new website then a secured portal is made available to the user. This portal is carried out in https protocol to avoid various possilbe attacks.Recovery phase is designed to deal with cases where a user loses his cellphone or in the case of change of mobile number by using the Enrollment number of the Aadhaar card.

Password reuse attacks prevention:

The password reuse attacks and the weak password attacks can be overcome by OTP. The OTP is the credential that is used to get access to their accounts. The OTP is obtained through the mobile. By the help of the OTP each login of the user appears to be unique since OTP for every session is unique.

Cellphone Protection:

An adversary can steal users' cell-phones and try to pass through user authentication. However, the cellphones are protected by a long-term password.

II. BACKGROUND

The proposed system is made more secured with the help of the following background functionalities which are listed as follows:

A.Aadhaar ID

The Aadhaar ID is used to unique identity to indentify an individual online. This Aadhaar ID is issued by the Unique Identification Authority of India (UIDAI). The Aadhaar ID is not a proof for Indian citizenship rather it is only an authentication entity used to uniquely identify an individual online.The Aadhaar ID is similar to that of the Social Seccurity Number (SSN) which is used in United states for various authenticated services.

The Aadhaar ID in our system plays a vital role in authenticating the users for their originality during the time of registration into the sites. The Aadhaar ID is requested from the user during the registration process.The Aadhaar system stores the user's information in the Central identities Data Repository (CIDR). This service is used by various sites during the registration phase as a service form the UIDAI (uidai.gov.in) in a secured portal as in the case of banking transaction.

B.One-TimePassword(OTP) using HMAC-SHA512

OTP provides the user a unique login each time when he/she login to their accounts. OTP is generated using hash function HMAC-SHA512. OTP is generated only after the successful submission of the valid Username and Long-term Password (LTP) by the. The pupose of longterm password is to protect users from the password reuse attacks. The LTP gives access to the OTP generation and transaction of the respective OTP to the user's Mobile that is specified during the time of registration. OTP protects the system from phishing attacks and the password reuse attacks.

The LTP and the user's Aadhaar ID is given as input to the hash function which prevents the DNS spoofing attack .

C.SMS

The SMS is used to deliver the login credential to the user in a safe manner and to ensure that the user is the original requestor for the OTP and also to check whether the mobile number is concerned to that specific user during the verification process in the registration phase.

III. RESEARCH PROPOSAL

In this section, we present our system the is resistant against the password stealing attacks and the creation of accounts with fake identies.

A.Overview

Unlike the generic registration and login process in the various web sites the proposed system has the following phases:

i) Authenticated Registration Phase
ii) Login phase
iii.) Recovery Phase

In the existing system there are various mechanisms for restricting and eliminating the fake accounts which takes place after the account has been created (i.e. post-registration), but in the proposed system the user validation process takes place during the account registration by which we can limit the users form registering into various sites with false details or with another person's identity. For the verification process the key element used is Smart ID (Aadhaar ID) which contains the personal information about the user and the same ID is requested from the user during account registration process in various sites. Our system also provides a protocol that is resistant to password stealing attacks and password reuse attacks. In our system the user is allowed to created his/her own email ID and a Long-term Password (LTP). After the successful submission of the email ID and the LTP the user gets the OTP to his Mobile.The user has to enter the OTP that is given by the server to his/her mobile number to access the respective account. This OTP hold good only for that current session, so even if it is stolen the OTP won't work for a different session. And also the LTP can be used for any number of accounts in various websites.

The overall architecture of the system is given as follows:

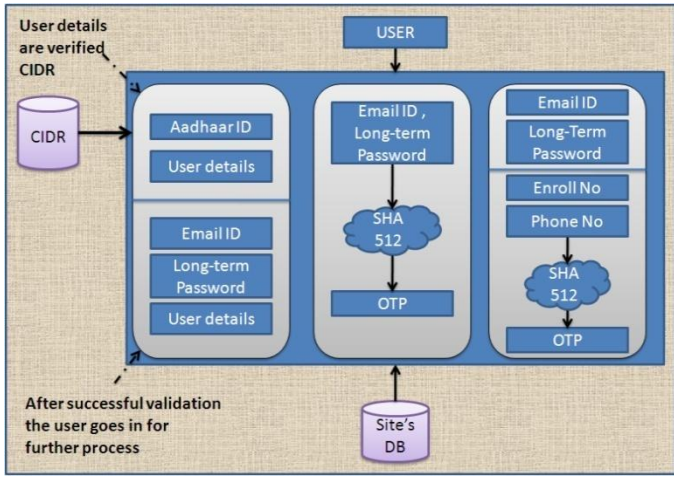

Figure 1: Overall Architecture

B. Authenticated Registration Phase

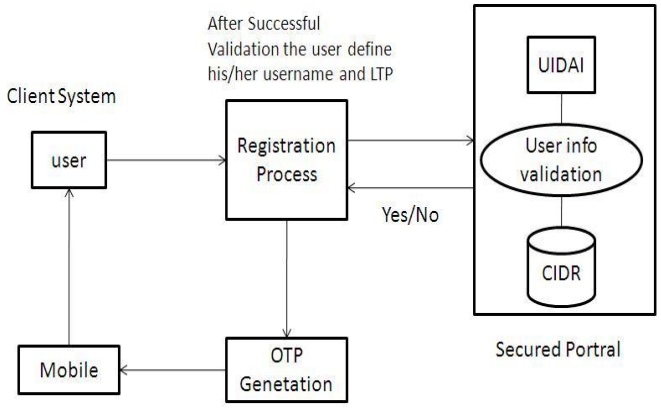

Figure 2: Registration Process

Figure:1 depicts the work flow of the authenticated registration process in our system

The aim of this phase is to limit the users from creating accounts with Fake Identities and False details. For a new user, when he/she goes in for registration the sites invokes a service from the UIDAI (Unique IDentification Authority of India) in secured portal. In this secured portal the user provides his/her Aadhaar ID and personal details (username, DOB, Mobile Number etc.). The user information are validated using the Adhaar ID with the help of the CIDR (Central Identity Data Repository) which stores the Aadhaar information (Managed by UIDAI). Only after the successful verification process the user is allowed to create his/her email ID and LTP.

C. Login Phase

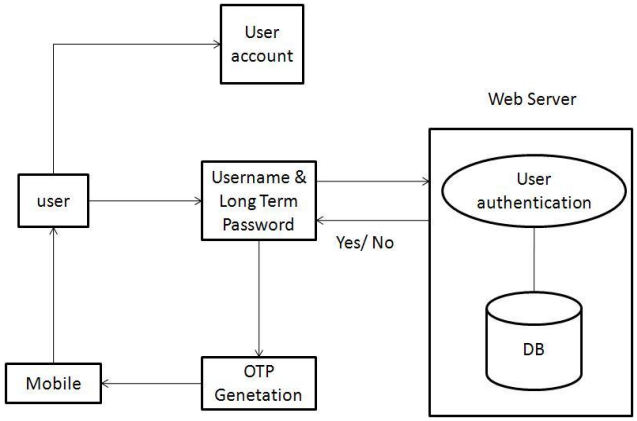

Figure 3: Login Process

The login phase begins when the user sends a request to the server through browser. This login Phase is secured one because of the One-Time Password (OTP) that is generated during each login. With the help of the OTP each login is uniquely provided to the user. The purpose of OTP in the Login Phase is to eliminate the password stealing attacks and other Phishing attacks.

The protocol starts when user wishes to log into her favorite web server (already registered). However, begins the login procedure by accessing the desired website via a browser . Once the user gets to the login Page, the user continues to enter the email ID and the Long-term Password in the required fields. After the successful validation of the email id and the Long-term Password the server starts to generates the OTP for that respective login .

The OTP is generated in a secured manner, which involves the hashing process. After the successful verification of the email id and the long-terrn password the server fetches the Aadhaar ID information of that user from the database and it is provided along with the Long-term Password to the hash function HMAC512 as input. The above inputs are given to the hash function which produces the hash value (512 bit) with the random key value generated in each instance of the hash function. The purpose of fetching the user's information in the process of OTP generation is to make sure that the system is resistant to the DNS spoofing attacks.

The Mobile computes a secret credential by the following operation:

SHA-512	Bits
Output Size	512
Block Size	1024
Maximum message size	2^{128} -1
Iterations	80
Operations	+, AND, OR
Performance	99 MiB/s

1 MiB = 2^{20} bytes = 1024 kibibytes = 1048576 bytes

Sample input:
abc

Sample output:
e3bcf148cf4aba61ad59042dcca53e018f685cdc009f5e9f23
9e6f83de6dcc4d8ef0c714721b596627b7d8f9e2edb6c093
298f95589c47ba82e439e1ae519f41

D. Recovery Phase:

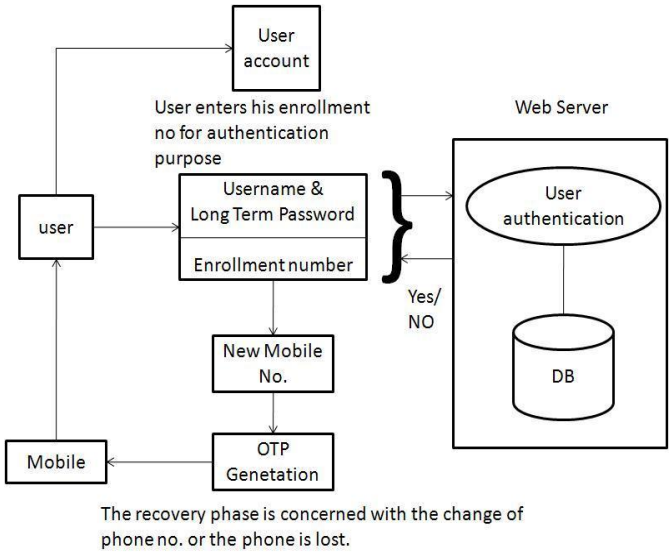

Figure 4: Recovery Phase

IV. CONCLUSION

This project has developed with the use of Aadhaar ID and with the help of the mobile Phone which makes the system resistant from the major attacks such as,

- Password Reuse Attacks.
- Password Stealing Attacks.
- Fake Identities.
- DNS Spoofing.

The purpose of this paper is to reduce the malicious activities that are caused by fake accounts and identity thefts. The future work of this system is carried out using the Biometrics (Face, Iris, Fingers) of the individuals that are available in the Aadhaar system. With the help of the Biometric devices these biometric information can be used for more secured authentication.

REFERENCES

[1] Tackling Twitter and Facebook Fakes –ID Theft in Social Media,
World Communication Regulation Act Report ,BNA (Bureau of National Affiars)

[2] oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks, *Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin.*

[3] Bump in the Ether: A Framework for Securing Sensitive User Input,
Jonathan M. McCune, Adrian Perrig, Michael K. Reiter.

[4] Reducing the Trusted Computing Base for Applications on Commodity Systems,
Jonathan M. McCune.

[5] Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers, *Mohammad Mannan, and P.C. van Oorschot.*

[6] SessionMagnifier: A Simple Approach to Secure and Convenient Kiosk Browsing, *11th Int. Conf. Ubiquitous Computing*, 2009, pp. 125–134, ACM.

Chuan Yue , HainingWang.

[7] Phoolproof Phishing Prevention,
Bryan Parno, Cynthia Kuo, Adrian Perrig

[8] M. Wu,S.Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in *DIMACS Workshop Usable Privacy Security Software*, Citeseer, 2004.

