iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3703

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Secured Login with Networking

Yogita Bagul[1], Asmita Targe[2], Kartik Bhavsar[3], Jaya Mali[4]
[1, 2, 3, 4] *Department of Computer Engineering, MET's Institute of Engineering*

Abstract: ***Real Time Secured Login module is designed for managing the applications efficiently over the internet. The Real Time Secured Login module will trace IP address, location of user and time of login. This information will be stored in database and login notification will be sent to user.***
In Real Time Secured Login module, whenever user will sign up, an unique id will be generated for user. Whenever user will login into his account, the location of user, time of login and IP address will be stored into the database. Along with these, login notification will be sent to the user through mail for security purpose. After login, the career guidance will be provided to the user according to their area of interest. This module has been designed for students and industry purpose.
Keywords: Web based, Server and Client Oriented, Email, IP-Address, Network based.

I. INTRODUCTION

The rapid development of Internet-based applications and services has made websites a crucial part of our lives. More and more users are using online office services instead of desktop office software, online social services to engage in social activities, online information boards to post their business products, and online shopping to do their purchasing. However, the security and privacy problems have also grown along with these newer and open Internet applications.
In order to use the online services and applications, users typically need to create accounts including usernames and passwords. The username-based identity and the related password problems because of online user behaviors have been a focus of research studies for quite some time.
User authentication is very crucial for the computers as well as network system security. Most of the login strategies share a common problem that's they authenticate at user just at the initial login session and then don't re authenticate the owners until the end user logs out. In this particular case virtually anyone can use the system materials if the initial user doesn't effectively logout. And so, for resolving this particular issue, the system must continuously monitor and also authenticate the end user after the original login session. To be able to do this objective, we want to develop strong, dependable also as user-friendly techniques for the constant user authentication.
In networking system, since most of the activities exist on internet and user authentication is the most essential component within the field of Security. Computer users are asked to create, preserve and remind an increasing number of passwords for host accounts, email servers. Most users choose easy to remember passwords (i.e. weak passwords) even if they know that these passwords might be unsafe. Another decisive problem is that users tend to reuse same passwords across a variety of websites.
The Main aim of our module is to provide activity details performed on user's account mainly the login details through the mail. In registration, user gives his all details with his Aadhar Card Number and then system will use that Aadhar Card Number as a User's unique id. In this module we will also add the user's reviews as a feedback.
One time password (OTP) systems provide a mechanism for logging onto a network or a service using a unique password which can be used only once, as the name suggest. This prevents some forms of identity theft by making sure that captured username/password cannot be used second time. Typically user logon name stays same, and one time password changes with each login. One time passwords are a form of so-called strong authentication, provides much improved protection to on-line banking accounts, corporate networks and other systems containing sensitive data. a one-time password (OTP) strategy, to protect network access and end users digital identities. This adds an extra level of security and it will be extremely challenging for an attacker to access unauthorized data, networks or online accounts.

II. LITERATURE SURVEY

Who Are You? A Statistical Approach to Measuring User Authenticity by David Mandell Freeman, Sakshi Jain, Markus D¨urmuth, Battista Biggio and Giorgio Giacinto[1],This system does the classification of login attempts into good attempts and bad or suspicious attempts and it is derived from user's past login history.
A Survey on User Identity Verification for Secure Login Session by Swati Borude, Pratiksha Chokhar, Neha Bhosale, Ashwini Palve,Prof.M.N.Kale[2],This system provides user verification periodically during login time.

©IJRASET (UGC Approved Journal): All Rights are Reserved

Two factor authentication for secured login in support of effective information preservations and network security by S. Vaithyasubramanian, A. Christy and D. Saravanan[3],This system provides both alphaneumeric password and graphical password as a gateway for authentication.

Design and Analysis of Continuous and Transparent User Identity Verification for Secure Internet Service by Dr. Ch. Venkatramana Reddy, Dr. Vijay Reddy Madireddy[4],This system uses multimodal biometric traits.

Soft Biometric Traits for Personal Recognition Systems by Anil K. Jain1, Sarat C. Dass, and Karthik Nandakumari[5], This system uses soft biometric traits(age, weight, gender) for user login verification.

Multimodal Biometric System: A Feature Level Fusion Approach by K. Geetha, V.R Xadhakrishnan[6],This system combines two biometric traits means two feature sets are combined into one feature set.

Password less Authentication Using Keystroke Dynamics: A Survey by Jhalak Modi, Hardik G. Upadhyay, Mitesh Thakor[7],This system uses keystroke dynamics means it measures user's typing pattern.

A Survey on One Time Password by Mirza Tanzila Maqsood, Pooja Shinde[8],This system uses a unique password which can be used only once.

Secure Image Based One Time Password by Neha Vishwakarma, Kopal Gangrade [9],OTP is generated in the form of images.

Security and Privacy Risks of Using E-mail Address as an Identity by Lei Jin, Hassan Takabi, James B.D. Joshi[10], System asks the questions to user about his/her email address.

III. SYSTEM ARCHITECTURE

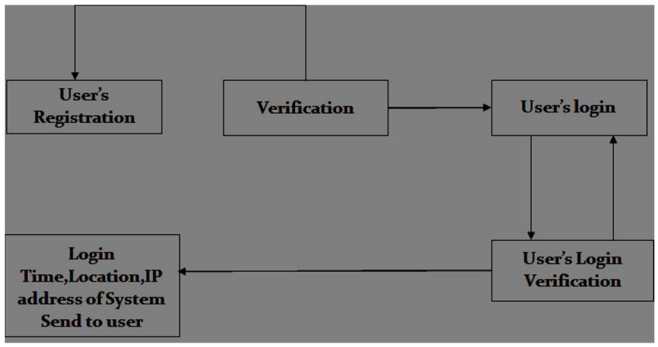


Figure-1: System Architecture

First block here shows user registration. When user wants to register or sign up he/she will be given a form on the html page. User will enter his aadhar number, email address and any other details required. Aadhar number will be the unique key used in the database to store an user. When user submits the registration form a request is sent to the server with aadhar no and email address. Server will check if the user is already registered or not in the system and gives an appropriate response like user is already registered. If user is not registered already then server will send an OTP (One Time Pin) to the given email address using the SMTP server. User will enter that OTP in the registration form and submit it. Then user is saved in the database with given aadhar number and email address and other details.

Second is user login. When user tries to login, aadhar number is sent to the server and server then checks if the given aadhar is registered or not. If it is registered then it will send an OTP to the given email address of the user. User will enter the OTP and proceed with the login process. After the login is successful, server will send the location, login time and IP of the user to the given email address. Server will determine the IP and location through the request which is sent from the browser client to the server. This information is sent to the email address and it is also stored in the database as a log of the user login activity.

IV. METHODOLOGY

Here user first register his/her details to the website. These details are checked in the database .If the information given is already available in the database then the message is displayed that the account is already existing or if the complete details are new then the user is registered. (A verification link is send to user's registered email id and then after when the user checks on the link then his/her account status will be active and the user will be authenticated and then he/she will be able to login).

For Login username and password will be accepted from the user and if the user is registered, then the user will be able to login. If the user entered wrong username and password the message will be displayed that the username and password are invalid. If account does not exist then the message would be displayed that the account is not exist. After login the mail will be send to the user

©IJRASET (UGC Approved Journal): All Rights are Reserved

and that mail containing details like user's login time, IP address of the system, browser used, operating system, geophysical location including its latitude and longitude.

For account recovery, One Time Password (OTP) will be send on user's registered mobile number or registered email id and also if OTP is not received by the user then it will be sent again and if the OTP is received and checked by the user then he/she will be able to change his/her password and the password will get updated and then user can login with the username and updated password.

V. RESULTS AND DISCUSSION

Provide better security to user's account. User will get all the login information. Can be used in any website where user's security is most important. Can be used in website where user have to create implement Security.

VI. CONCLUSION

In this paper we are providing login information to the user about his/her login activities. This login information contains location of user, IP address of the system, login time, geophysical location and Browser Details. All these information will be send to the user through user's email id to get acknowledgement and get known about his/her web activities.

VII. ACKNOWLEDGMENT

We would like to thank Prof. Vaishali Khandave, MET's Institute of Engineering, Nashik for her expert guidance and valuable contribution for the betterment of the project.

REFERENCES

[1] David Mandell Freeman, Sakshi Jain, Markus D¨urmuth, Battista Biggio and Giorgio Giacinto[1]-" Who Are You? A Statistical Approach to Measuring User Authenticity", NDSS '16, 21-24 February 2016, San Diego, CA, USA Copyright 2016 Internet Society, ISBN 1-891562-41-X http://dx.doi.org/10.14722/ndss.2016.23240

[2] Swati Borude, Pratiksha Chokhar, Neha Bhosale, Ashwini Palve, Prof. M.N.Kale, "A Survey on User Identity Verification for Secure Login Session", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7,Issue 3,March 2017

[3] S. Vaithyasubramanian, A. Christy and D. Saravanan, "Two factor authentication for secured login in support of effective information preservations and network security", ARPN Journal of Engineering and Applied Sciences and Technology, Volume 5, Special Issue 11, May 2016

[4] Dr. Ch. Venkatramana Reddy, Dr. Vijay Reddy Madireddy, "Design and Analysis of Continuous and Transparent User Identity Verification for Secure Internet Service", International Journal of Innovative Research in Science, Engineering.

[5] Anil K. Jain1, Sarat C. Dass, and Karthik Nandakumar1, "Soft Biometric Traits for Personal Recognition Systems", Proceedings of International Conference on Biometric Authentication, LNCS 3072,pp. 731-738, Hong Kong, July 2004.

[6] K.Geetha, V.Radhakrishnan, " Multimodal Biometric System: A Feature Level Fusion Approach ", International Journal of Computer Applications (0975 – 8887) Volume 71– No.4, May 2013.

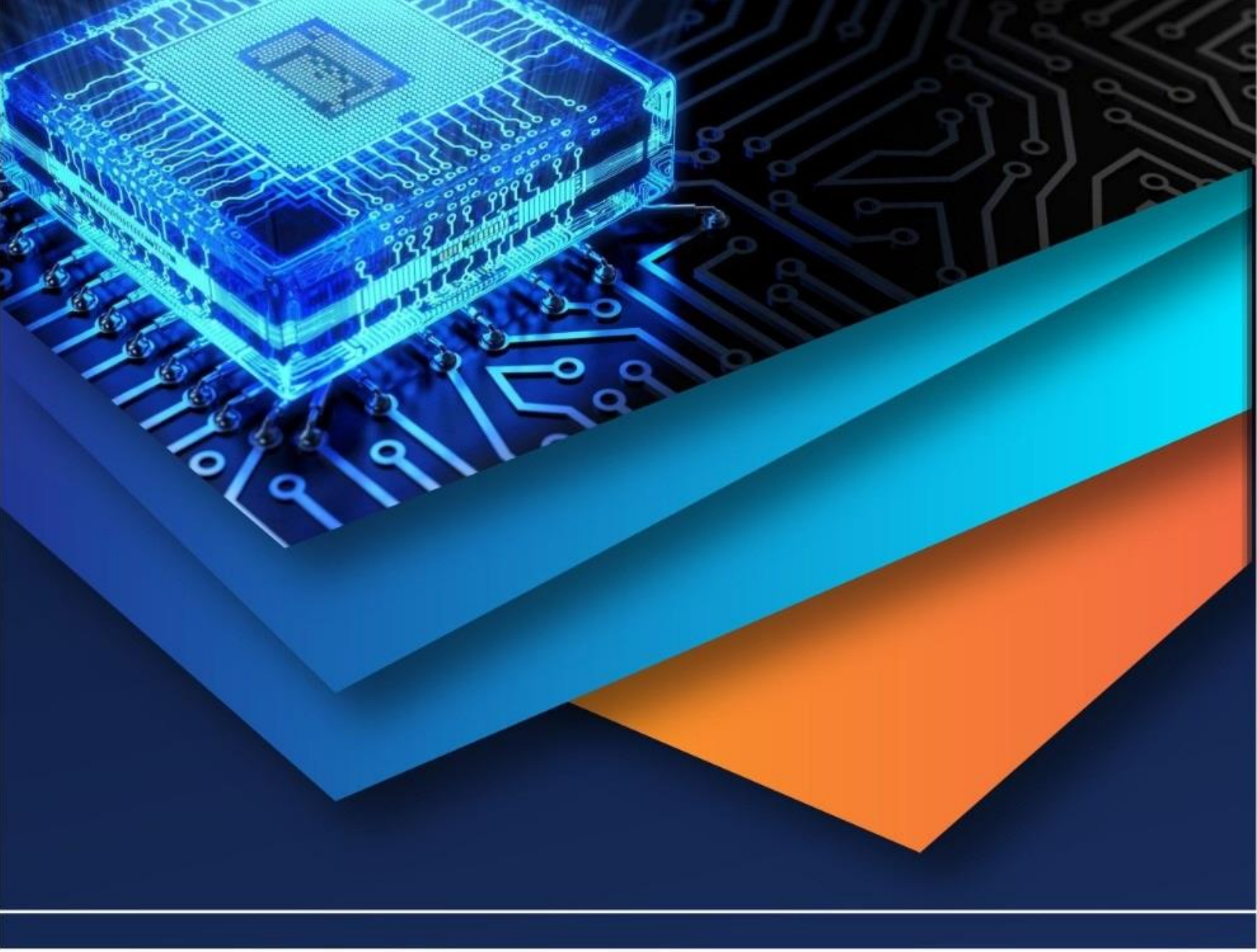
[7] Jhalak Modi,Hardik G. Upadhyay, Mitesh Thakor, "Password less Authentication Using Keystroke Dynamics: A Survey", International Journal of Innovative Research in Computer and Communication engineering, Vol. 2, Issue 11, November 2014.

[8] Mirza Tanzila Maqsood, Pooja Shinde, "A Survey on One Time Password ", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index. Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611.

[9] Neha Vishwakarma, Kopal Gangrade, "Secure Image Based One Time Password ", International Journal of New Innovations in Engineering and Technology.

[10] Lei Jin, Hassan Takabi, James B.D. Joshi, "Security and Privacy Risks of Using E-mail Address as an Identity", US National Science Foundation award IIS-0545912.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)