MACHINE LEARNING BASED SECURITY SYSTEM FOR OFFICE PREMISES

Rutuja Patil, Adarsh Charak, Utkarsha Bhad, Sachin Deshmukh

Rutuja Patil Undergraduate Student JSPM's RSCOE, Maharashtra, INDIA Pune – 411033
Sachin Deshmukh Undergraduate Student JSPM's RSCOE, Maharashtra, INDIA Pune – 411033
Utkarsha Bhad Undergraduate Student JSPM's RSCOE, Maharashtra, INDIA Pune – 411033
Adarsh Charak Undergraduate Student JSPM's RSCOE, Maharashtra, INDIA Pune – 411033
[3]Example: Prof. Vinodkumar Bhutanal, Dept. of Computer Engineering, JSPM'S RSCOE, Maharashtra, India

---***---

Abstract -

Safety plays a major role in today's world. User-authentication can be defined as a procedure used to verify the identity of the user , authentication is an essential term I n the digital world so as to protect the client's/user's critical data stored online or offline. Various mechanisms are gradually evolving to authenticate users in various scenarios. At offices and work places as well, this user authentication is of utmost importance in order to avoid any mal-practices if any as well as to maintain individual work privacy in the organization. This project aims at developing a user authentication system for offices based on their company generated login ID and passwords, One-Time-Password (OTP) generation and face recognition. The system also has features such as auto-saving data to server and auto-logout

Key Words: **AutoSaved, Auto-logout, Face recognition, Login ID and passwords credentials, One-Time-Password (OTP).**

1. INTRODUCTION

Now-a-days we have various tools for protecting system from malicious activity such as proxy servers, firewalls, security software, and so on. Still the data privacy cannot be assured, and hence we have to come up with a software or a tool which has negligible chances of getting attacked. We aim in providing 4 step security so that the data is not accessed illegally. This approach gives more security by restricting unauthorized access and auto logout feature. We can guarantee integrity and confidentiality. One strong pillar that is one-time password makes it more difficult to get illegal access to data.

The authentication, confidentiality and privacy of data is needed in today's world. IOT that is the internet of things is evolving widely. The IoT architecture is just modified version of some existing data communication tools. Due to the vulnerabilities of the Internet, security and privacy issues should be considered and resolved before the IOT is globally deployed. Direct interaction of smart devices within the immediate living space of humans intimidates new security vulnerabilities. Research has been led in developing customized tools for computer security to establish confidentiality, integrity and availability. In case of any kind of security failure, our system provides the users data fully data security and assurance of privacy. The aim is to prevention system that is adaptive and receptive to new threats and provides more control of owner on the data stored on system by restricting the access to particular user for specific file with limited rights. The idea behind it to create software that will protect the data from all kinds of attacks and maintain entire confidentiality of the data.

2. LITERATURE REVIEW

There has been a use of three tire architecture in paper "Effective Authentication For Restricing Unauthorized User", [1] for providing security to the system. Those tiers are Facial recognition, Fingerprint Scanning and OTP. All these tiers give a great strength to security of system. Incase if there is an attack on system, the measures are provided so as to not leak the important data from the system. By using AES 512 all the data is encrypted which can only be decrypted by a specific key.

Security and protection of personal data online/offline is very critical as data is becoming critical and smartphones are vulnerable to illegal unauthorized access. User-authentication allows legitimate person to ask the data. Mobiles are made secured by using the methodology of biometric authentication using user's physical traits. The survey provides an overview of the current state-of-the-art approaches for continuous user authentication using behavioral biometrics captured by smartphones' embedded sensors, including insights and open challenges for adoption, usability, and performance.

Biometric User-authentication of a user by using their own unique traits is the most easiest and common way to identify a person. In [3], a multimodal-biometric-user-verification system with similar twin shows the fingerprint, face and lip classification model using Support Vector Machine.

Paper – 'Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare data;

[4] it analyses the results of using both fingerprints as well as online signatures. Here the signatures are verified using the dynamic time warping methodology. The weighted sum rule is applied for the process of biometric fusion (signatures and fingerprints). Deep learning classifier is proposed in this work for multi-biometrics authentication. When a biometric authentication request is submitted to improve the authentication performance, the proposed user-authentication system uses deep-learning to automatically select an accurate matching image.

Now-a-days we can see the concept of cloud evolving having benefits like high performance, accessibility, better storing capacity etc. Storage has become a huge issue for users having large data, cloud provides a solution of unlimited storage to a user. Yet cloud has various vulnerabilities and users do not wish to compromise security. So the aim is to figure out and address the security issues by using cross validation strategy.

User-Authentication is always done at the start of the program, but in order to understand the genuineness of the user the authentication must be continuously going on. In [6], Suhail Javed Quraishi and Sarabjeet Singh Bedi proposed the usage of key-stroke used as biometric characteristic for continuously authenticating the user. Authentication using biometric uses basically three stages such as the enrollment stage, the verification stage, and the identification stage. Identification stage marks the user as an authenticated user only if the input pattern is matched with the profile pattern or else the system will automatically logout. There is no restriction on input data during enrolment, verification, and identification stage. The technique used to classify the authenticated user's input from others is Unsupervised One-class Support Vector. This User-authentication system can be used in areas like in non-proctored online-examination, Intrusion and Fraud Detecting Systems, etc.

Paper "A Robust e-Invigilation - System Employing Multimodal Biometric Authentication", presents the development of robust, flexible, transparent and continuous authentication mechanism for e-assessments. There has been a significant growth of students/users using e-learnings and e-assessments. The major concern is that they might cheat using these resources in their exams. So in order to reduce the chances of cheating in online examinations, biometrics of the student can be used to check whether the legitimate student is attempting the exam the system gives a continuous user-identification by using biometrics;: an eye tracker is used to record the student's eye movement; and, the speech -recognition is used to detect communication from student's end. The focus of [7] particularly is on the development 3D Facial-Authentication. Experiments have also been conducted in order to test these biometrics to see whether the student is cheating During the experiment, participants' biometric-data, eye-movement, and head-movements have been collected using a software.

As of today, computers are protected with various security software, proxy servers, firewalls, still the data inside the computer has vulnerabilities. We aim in providing 4 step security so that the data is not accessed illegally. This approach gives more security by restricting unauthorized access and auto logout feature. We can guarantee integrity and confidentiality. One strong pillar that is one-time password makes it more difficult to get illegal access to data.

Paper "Effective Authentication for Avoiding Unauthorized User Access", presented a evolved Role Based Access Control model by modifying previous role based access control in Structure Query Language. This model evaluates & executes security policies that contain access conditions against the dynamic nature of data. The goal is to create or use a mechanism for forward looking, assertive and flexible security-features to regulate access to data in the data storage. This is easily achieved by integrating roles & authenticated access rules and implemented through effective audit trail.

Paper [10] presented a state of art about biometric hand, different techniques used. Biometric is essentially used to avoid risks of password easy to find or Stoll; with as slogan save Time and Attendance. The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.. Biometrics is recognizing a person based on his physical unique characteristics like fingerprint, iris recognition, face recognition etc. This methodology provides us more uniqueness and security. As these characteristics cannot be faked, the chances of the computer system having biometrics getting accessed illegally are negligible. Traditionally the biometrics meant signatures, keys and passwords. Biometrics is defined as 'Life Measure' in Greek dictionary. Biometrics is a very useful method which is widely used in criminal identification and prison security. These can be used to protect the ATMs, phones, systems, smartcards etc. Thus, Biometric is a widely evolving technology which is very efficient for user authentication and security.

Objectives :

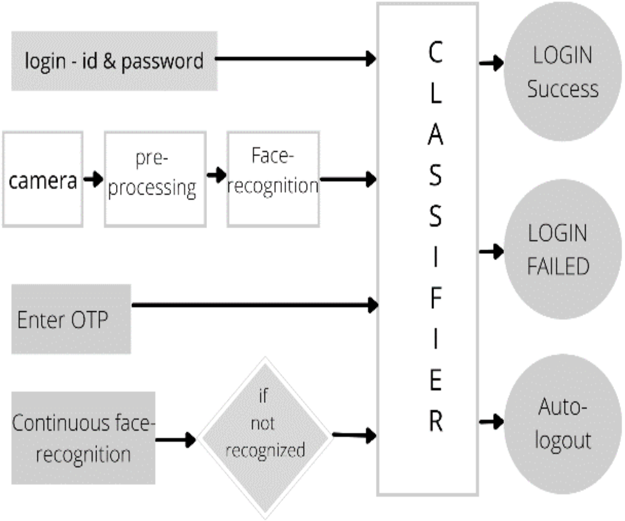
1.Effective Authentication for Avoiding Unauthorized User Access.

2. Effective Authentication for Restricting Unauthorized User.

3. Evaluation of 3D facial confirmation.

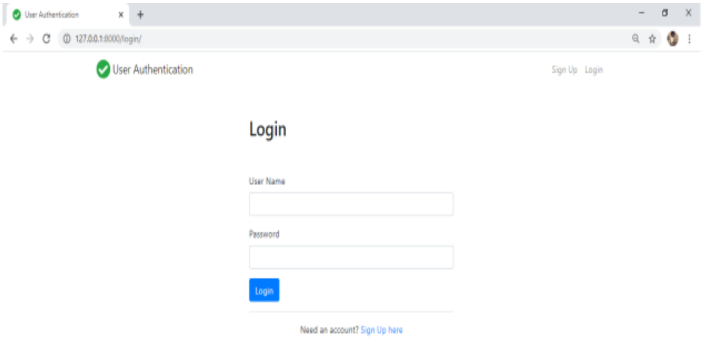
3. RELATED WORK

Module 1 – Proposed Framework



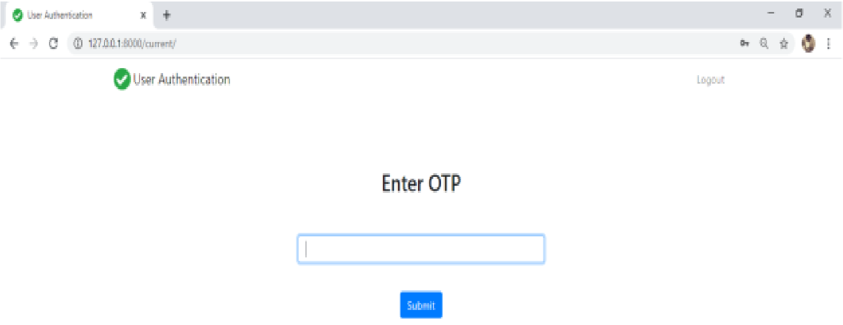
A face acknowledgment framework is a PC application for naturally recognizing or checking an individual from an advanced picture or a video outline from a video source. Highlights like face acknowledgment and One-Time Password (OTP) are utilized for the improvement of safety of records and protection of clients. Face acknowledgment innovation assists the machine with recognizing every single client particularly. Proposed framework comprises of a four-venture secure verification process for working representatives in their separate associations.

Module 2 – Login



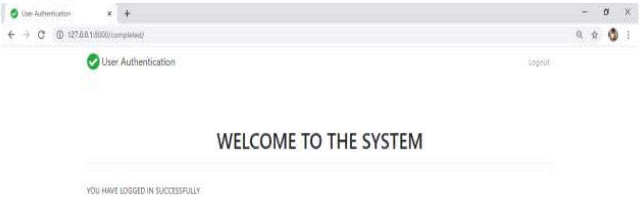
Firstly, the client/user needs to enter the login Id and secret key which are unique provided by the organization. When that coordinates with the data set, the next phase is to create the OTP on the enlisted phone number. If the user is failed to provide the OTP, further access to the system is denied. If the OTP is accurate, the user is directed to the next phase.

Module 3 - OTP and Face Recognition



Enter OTP

Whenever this is done, next comes the face recognition and acknowledgment. With the assistance of webcams present with every single system, the face before cam is distinguished. A live picture is caught consequently through a webcam introduced on the gadget, which is contrasted and the picture put away in the data set. Assuming this picture matches, client can get the admittance to work that specific framework. Haar Cascade Classifier is utilized to execute face acknowledgment. An extra component of autosave and auto-logout is likewise remembered for this framework. Assume the representative ends up passing around their work area because of certain reasons, the webcam will be ceaselessly recognizing and catching the pictures if any.



WELCOME TO THE SYSTEM

YOU HAVE LOGGED IN SUCCESSFULLY

In case an obscure face picture other than that framework client, is caught by the webcam, the entire work/information will be consequently saved to the organization's server and the framework will naturally logout, so that, the obscure client can't make any controls in the client's work. The autosave highlight assists the client to re-proceed with the work with framing the point he/she had left it. Thus, an extremely effective, protected and dependable framework is created.

Module 4 – Algorithms

1. Haar Cascade Algorithm
2. Making Integral Pictures
3. Adaboost coaching and cascading classifiers

4. RESEARCH GAP ANALYSIS

By referring several related works, the following challenges associated with the existing framework-

1. Haar Cascade Algorithm may fail to recognize the face if the face is manipulated by wearing sunglasses or tilting head towards any side.
2. For training the model, manual intervention is required.
3. The existing system works only on Windows OS.

5. CONCLUSIONS

We have used 4 steps for giving the accurate security and authentication purpose. These steps include – 1.credentials for logging in 2. Facial recognition using HAAR-CASCADE 3.One Time Password and 4. Auto-Logout. These are the four pillars of our system which give proper authentication and security.. This approach gives more security by restricting unauthorized access and auto logout feature. We can guarantee integrity and confidentiality. One strong pillar that is one-time password makes it more difficult to get illegal access to data

REFERENCES

1. Patil, A., Rana, D., Vichare, S., & Raut, C. (2018). Effective Authentication for Restricing Unauthorized User. 2018 International Conference on Smart City and Emerging Technology (ICSCET). doi:10.1109/icscet.2018.8537323

2. IEEE INTERNET OF THINGS JOURNAL (IOTJ) 21 Sensor-based; Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey Mohammed Abuhamad, AhmedAbusnaina, DaeHunNyang, and DavidMohaisen arXiv:2001.08578v210 on May 2020

3. Multimodal-Biometric-User-Verification-System with Similar Twin using SVM 2 B.Lakshmi priya, M.PushpaRani International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, march 2020

4. Multi-Biometric User-Authentication Technique Using Deep Learning Classifier for Securing of Healthcare Data Dr. GandhimathiAmirthalingam1 , Harrin Thangavel1 Volume 8, No.4, July – August-2019

5. Cloud-Security: To Prevent Unauthorized Access Using an Eeficient Key-Management Authentication Algorithm S.NaveenKumar1, K.1Nirmala2 International Journal of Engineering & Technology, (IJET) - ; 7 (1.1) 2018

   On the key-strokes as Continuous User Biometric Authentication Mr.SuhailQuraishi, SarabjeetsinghBedi at International Journal of Engineering and Advanced Technology IJEAT ISSN: 2249 – 8958,, August-2019