IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

Secured Third-Party Authentication System

Digvijaysing Rajput[1], Mahesh Gaikwad[2], Tejas Nikumb[3], Suved Chougule[4], Prof. Sagar S. Mane[5]
Students, Department of Computer Engineering[1,2,3,4]
Guide, Department of Computer Engineering[5]
NBN Sinhgad School of Engineering, Pune, Maharashtra, India

Abstract: *Nowadays, most of the applications are using the traditional method of username and password system and focusing on how to make passwords more secured using encryption methods, but because of daily new vulnerabilities & its limitations, currently many businesses are moving towards a new way of Third-party authorization systems. So, we are presenting the solution as Secured Third-Party Authentication System using Biometric Face Recognization, which will make the Login & Signup Process more secure & easier to use.*

Keywords: Third-Party Authentication, Transport Layer Security (TLS), Privacy, Machine Learning, Face Recognition.

I. INTRODUCTION

Nowadays Internet is a crucial part of our day-to-day life, but it was started in the 1960s, just as a way for government researchers to share their information. In 1960s, Computers were heavy, large, and Immobile so in the early days, to access any information of the computer, they needed to go there physically or have magnetic computer tapes sent to the user.

The Internet was launched on 1 Jan 1983, before the Internet, there was no other way for computers to interact. After Internet, a new protocol was developed & established as TCP/IP Protocol. It allowed different computers to communicate with other devices on different networks.

Like Computers, passwords are nothing new. Unique keywords have been used around for centuries. The Roman military also used unique keywords to distinguish their friend & foe as it was an effortless way to protect their information.

In 1961, A Compatible Time-Sharing System (CTSS) was developed by MIT that all researchers can easily access. But they were using a common mainframe, so to keep individuals' data secure, they used a personal digital key (Word) & so was the concept of a password was developed.

Nowadays, every business owner wants to have an online platform like a website or mobile app. But the traditional username and password system become hectic for users as well as developers. As more and more services are going on online, typing a long, complicated, strong password can be frustrating for users because they also need to create a different password for different applications & remember them. Developers also face problems securing that password. So, developers are now moving toward Third-Party Authentication systems.

II. LITERATURE SURVEY

Sr No	Title	Methodology	Developed For	Limitations
1.	Web Application Vulnerabilities: Exploitation and Prevention. (2020)	For this work, the DAMN vulnerable machine is used different tools are used on the machine if vulnerabilities are found it reported	New vulnerabilities come day to day users need to be aware of the new threats they are possessed with.	This paper only describes the vulnerabilities and exploits them on real-time DVWA machines but did not focus on upcoming solutions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

2.	The Combination of RSA key with the One Time Pad for Enhance Scheme of 2-Factors Authentication. (2020)	RSA process, in the generation of a security key, is needed so that the number will not be traced then the number given is encrypted first and decrypted back when needed.	RSA algorithm has the benefit of resisting brute force & statistical attacks. So, it's not easy for the attacker to access the password.	RSA process has a slow speed of encryption & Decryption because it has multiple number generation & hackers also found some security weakness in RSA keys
3.	Towards Integrated Methods of Detections & Description for a Face Authentication System. (2020)	They used SSD Neural network with a pretrained COCO database & ImageNet database to get results.	They attempt to develop an ML algorithm that can identify faces even when they are present in groups.	Low Accuracy because they do not train different types of Faces data to ML algorithm. Used pretrained data.
4.	Discussing an Alternative Login Method with their Advantages & Disadvantages. (2018)	Biometric auth uses multiple methods such as Voice Recognition, Fingerprint Scanning, Facial Recognition, Lip Scanning.	In the constant tug-of-war of the cyber security world, traditional User ID & Password is not sufficient, so a new approach is needed.	Face Recognition is analyzed using old algorithms, Paper focuses on Lip Scanning but If a user has chapped or peeling lips, the system may develop errors.
5.	Face & Gender Recognition System based on Convolutional Neural networks (2019)	The wide 1D pixel vector is made of the 2-D face picture in compact main elements of the space function for facial recognition by the vgg16.	Developed for predicting gender and Face recognition by using vgg16, faceresnet.	It's a prolonged process but the accuracy of the result is high.
6.	Study on Face Recognition Techniques (2020)	Face Detection Based on The Combination of Haar-like Features & The Adaboost.	To Analyse the performance of both algorithms by comparing them.	The skin colour model-based algorithm detects some false positives & also Ada-boost has a slow training speed & it's also sensitive to noise.

III. System Architecture

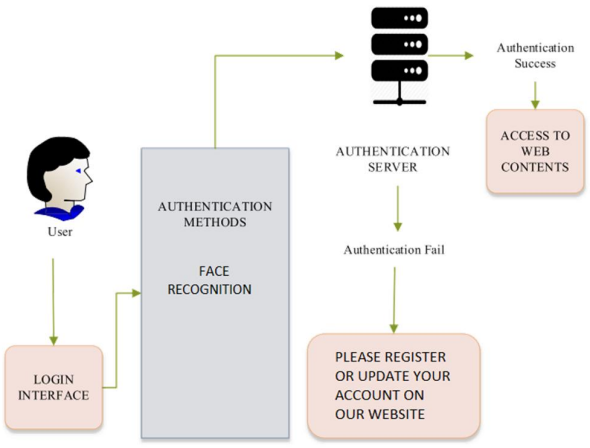

Figure: Workflow

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

Our primary authentication method is Face Recognition, the basic flow of our system is First User will register on our Server. While registering they will fill in their personal details such as email, phone no, etc & Upload/Scan Face Images for identification. After successful registration. Users can now login into other websites & login / Sign up there with help of our Authentication System. When new Users log in through our authentication system, our system will start the camera of the device & capture the user Image & send it to our ML code Authentication Server. After Successful verification, Required User details will be automatically shared from our Authentication server to the Website which user was accessing.

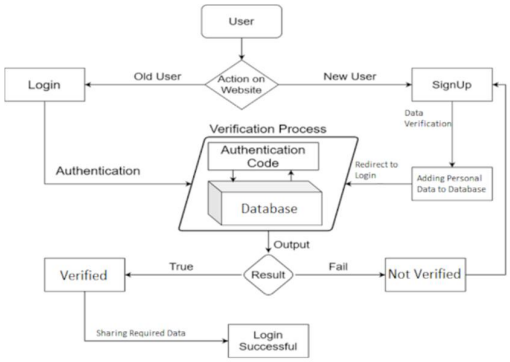

Figure: Flow Diagram of Verification

If User Verification is Unsuccessful, then it means either user did not register on our server so they will get an option to Register on a server or maybe they need to update their Previous Face Images on a server for identification purposes so they can log in in our server & Update their Credentials as per User Need.

IV. Face Recognition

We are going to use Convolution Layer with Max pooling operation. Multiple test cases were performed to examine identification performance. All the regions where faces are present are set as regions of interest then these face images are resized into 160 x 160 and then given to the feature extraction network. At First, all the tests are conducted with a Set of 5 unique face images, then these images are given to the face description network and then extracted embedding features are stored in the main database. For all detected faces from the test images their embedding vectors then get extracted by description network to compare them in gallery images to identify the best match.

The pipeline utilizes a neural network backbone for detecting and describing the faces in each image. In the ML network, any new faces can be inserted to the gallery to make the system identify the faces in each image.

V. Security

We are following the rules & guidelines provided by ISO 27001/ 27002, GDPR & NIST. They have predefined standards for security which can be tested by doing vulnerability assessment on the website.

Our Login page & all subsequent pages will be accessed over Transport Layer Security or other secure solid ways. Because failure of login page will allow the attacker to modify the login page actions easily & it can cause the user credentials to get hacked & send to an unknown location. We will also use a cryptographic hash function algorithm that can be used to verify the authenticity & integrity of a piece of data.

Here are some Vulnerabilities example:

- **Server-Side Request Forgery:** It happens when a web application fetches data through remote resources without doing a proper data validation then it allows a hacker to force the web app to send a modified request to an unknown location & it can even happen when an active firewall protects it.
- **Injection**: common injections are NoSQL, SQL, OS cmd, ORM, Expression Language, or Object Graph Navigation Library injection. Hackers can insert malicious input to a web application using injection methods and change the operation of the application by forcing it to perform required commands.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

- **Software and Data Integrity Failures:** It is crucial to consider while securing a web app. It is related to the failure of infrastructure and web app code that does not have active integrity violation protection.

While doing vulnerability assessment, we will test OWASP top 10 & CWE top 25 Vulnerabilities to find security vulnerabilities of the system & improve the security of the web Authentication Server to secure our system from the malicious attacker.

VI. METHODOLOGY

6.1 Third-Party Authentication System

In third party authentication system or Open Authorization (OAuth) protocol instead building authentication layer. business takes this auth service from third-party providers. so, when the user wants to Authentication (login/signup) on the website instead of using a username and password, the user directly login using a third-party authentication button provided by google, GitHub service so on.

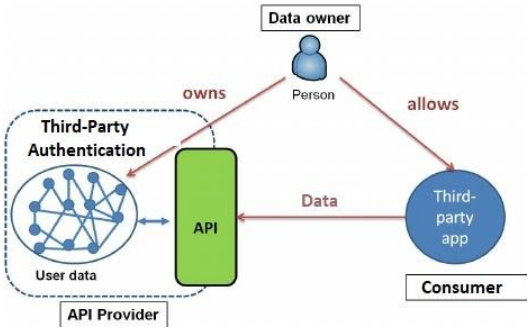

Figure: API Flow

Users save their personal details to third-party authentication service providers and these providers authenticate the user and give the user info to the website that the user wants to access. hence instead of giving a username and password, users can access the website with one click of a button.

6.2 Advanced Approach

Like the third-party system, we are adding an extra security layer with help of face recognition. This will be a robust auth method and it is very much doable because currently every device is equipped with a Camera & for the face auth service we only need a camera. For Identification, we will use a Convolution Layer with a Max pooling operation. VGG16 Neural Network so it has very high accuracy in face recognition & we are also going to use security guidelines of ISO 27001 & GDPR so that security standards will remain maintained. As a new Security vulnerability is discovered daily, Data breaches become a common problem for every Auth server. So, we will take a vulnerability assessment on our project to enhance the security of our project.

VII. CONCLUSION

In this paper, we discussed new ways of Authentication in website/web services & making them more secure by adding a solid layer of third-party face authentication system while replacing traditional username and passwords system. Even if New Authentication types of sound like the perfect system, convenience & security all in one package. We also need to be beware of not trusting any system blindly without proper research. Because each system has its own advantages, it also holds a significant security flaw that traditional username & passwords never had to compensate for.

REFERENCES

[1]. Web Application Vulnerabilities Their Exploitation and Prevention. (2020)
[2]. Combination RSA with One Time Pad for Enhance Scheme of 2-Factor Authentication. (2020)
[3]. Towards Integrated Method of Detection & Description for Face-Authentication System. (2020)
[4]. Discussing Alternative Login Methods & Their Advantages & Disadvantages. (2018)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

[5]. Face & Gender Recognition System based on Convolutional Neural networks. (2019)
[6]. Study on Face Recognition Techniques. (2020)
[7]. IEEE Websites.
[8]. Google.
[9]. Wikipedia.
[10]. Books.