iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50866

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: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Secure Tandem Authentication System

Sheryl Sharon G[1], Samuel Lalawmpuia[2], Priyadharshini M[3], Swarna Ambigai V[4], S. Sharmiladevi[5]
[1, 2, 3, 4]*Student, Computer Science and Engineering, Coimbatore Institute of Technology*
[5]*Assistant Professor, Computer Science and Engineering, Coimbatore Institute of Technology*

***Abstract:** This paper describes a method of implementing two factor authentication using password authentication and face authentication. The proposed method guarantees secure authentication to online banking and other areas of utilizing user credentials with the help of knowledge factor and biometric factor. The proposed method has been implemented and tested.*
***Keywords:** text-based password, Face Authentication, hash, biometric, security, user, protection*

I. INTRODUCTION

In today's digital age, security breaches and cyber-attacks are increasing. One way to protect one's online accounts from being hacked is to enable Two-Factor Authentication. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. The rapid growth in the number of online services leads to an increasing number of different digital identities each user needs to manage. But passwords are perhaps the most common type of credential used today [1]. Passwords can be guessed, stolen, or cracked, and many people often use the same password for several accounts [7, 8, 9]. This makes it easy for cybercriminals to gain access to accounts that contain sensitive and personal information, such as bank accounts [10], email accounts and social media accounts such as Instagram, Facebook and so on. Secure Tandem Authentication System adds an extra layer of security [12], making it much harder for hackers to access one's accounts. This makes the cyberspace more secure and protects user privacy.

II. LITERATURE SURVEY

With the rapid development of the Internet and mobile devices, system authentication has been widely used in the process of accessing the internet and mobile devices to protect devices, data, and user accounts [4]. One of the best password authentication systems was text-based password which has several problems. One of the main problems with text-based password is it was prone to dictionary attacks [3]. However, recent trends have moved onto adoption of two factor authentication which promises secure authentication. Achaliya and et al, have proposed a methodology to secure ATM using Face Authentication and OTP. A conventional ATM system processes the ATM card and PIN together that leads to criminal activities. Thus, it eliminates illegal transactions at ATMs without the knowledge of the account holder. Facial recognition method for authentication makes ATMs more secure [2].

III.METHODOLGY

A. Password Authentication

There are different algorithms for generating hash of a text. The most popular ones are: MD5 and SHA1. However, researchers have found several flaws in the SHA1 and MD5 algorithms. According to researchers, they should use hash algorithms from the SHA2 family like SHA256 or SHA512[6].

These algorithms produce hashes of length 256 and 512 bits. The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.

Each time we generate hash of a password, we use a random salt. You just need to generate a random number of a particular length and append it to the plain text password, and then hash it. In this way, even if passwords for two accounts are same, the generated hashes will not be same because the salts used in both cases are different.

To authenticate the user, you must store the salt used for hashing the password (It's possible to store the salt in another column in same table where you have username and password stored). When the user tries to login, append the salt to the entered password and then hash it with the hash function.

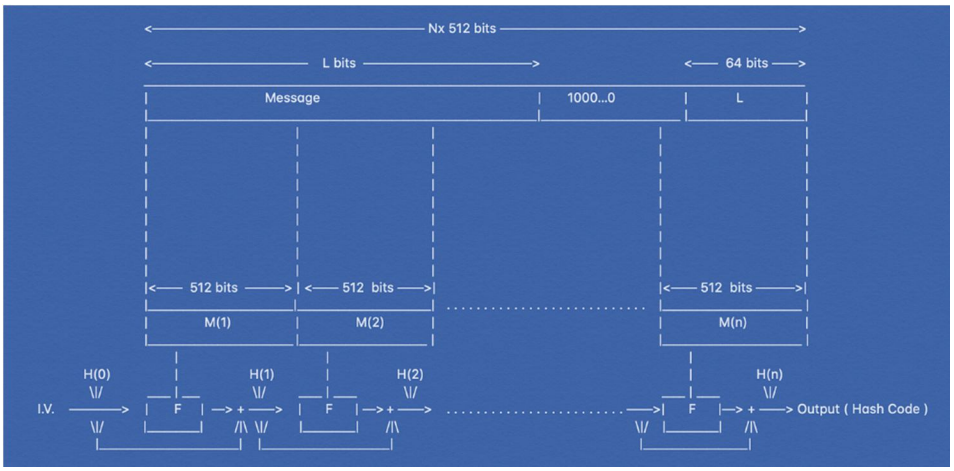


Fig 1. SHA 256

B. SHA-256 Algorithm

```
// Define the input data as a list of strings
inputData ← [.....]
// Define a function to compute the SHA-256 hash for a given input data
function computeSHA256(input):
  md ← MessageDigest.getInstance("SHA-256")
  hashBytes ← md.digest(input.getBytes("UTF-8"))
  hashHexString ← hashBytes.map(byte => formatByteToHex(byte)).join("")
  return hashHexString
// Define a function to format a byte to hexadecimal string
function formatByteToHex(byte):
  hexString ← convert byte to hexadecimal string
  if hexString.length < 2:
    hexString ← "0" + hexString
  return hexString
// Create an empty array to store the hash values
hashArray ← []
// Iterate over each input data element
for input in inputData:
  // Compute the SHA-256 hash for the input data
  hashValue ← computeSHA256(input)
  // Append the hash value to the hashArray
  hashArray.append(hashValue)
```

C. Face Authentication

Face Recognition can be used for a multitude of applications, from security to advertisements.

With the use of face authentication comes a host of potential benefits [5], including:

1) No need to physically contact a device for authentication- compared to other contact-based biometric authentication techniques such as fingerprint scanners, which may not work properly if there is dirt on a person's hand;
2) Improved level of security;
3) Less processing compared to other biometric authentication techniques;
4) Easy integration with existing security features;
5) Accuracy of readings has improved over time; and
6) Can be used to help automate authentication.

D. Algorithm for face authentication

Facial Authentication is the process of mapping facial expressions to identify human face with image processing software.

1) Load preprocessed face images into an array.

faceImages ← loadFaceImages()

2) Compute the mean face image and the covariance matrix.

meanFace ← computeMeanFace(faceImages)

covarianceMatrix ← computeCovarianceMatrix(faceImages, meanFace)

3) Compute the eigenvectors and eigenvalues of the covariance matrix.

eigenvalues, eigenvectors ← computeEigenvaluesAndEigenvectors(covarianceMatrix)

4) Select the top 'k' eigenvectors as the eigenfaces.

k ← selectNumberOfEigenfaces()

5) Project a new input face image onto the eigenface space, compare with known faces, and output the recognized face or "Unknown" based on a distance threshold.

RecognizedFace ← knownFaces[closestKnownFaceIndex]

IV. EXPERIMENTAL SETUP AND RESULT ANALYSIS

A. Experimental Design

The proposed system authenticates a user based on the knowledge factor and then based on the biometric factor that is unique for each individual. Failure at any layer leads to a failed attempt. On succeeding both the layers, the user is granted access to the application or system of critical importance.

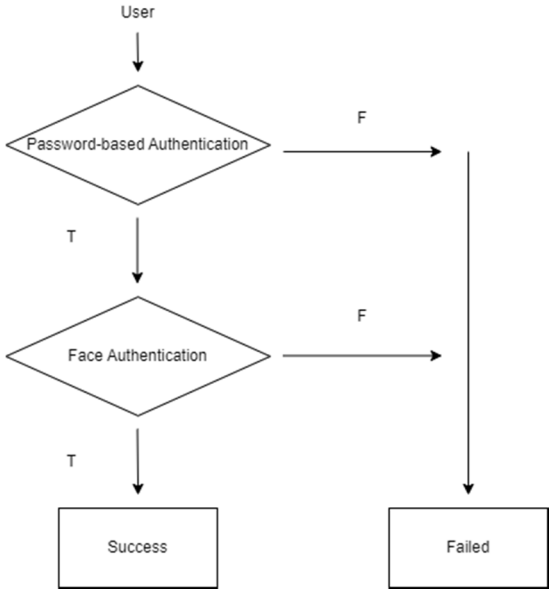


Fig 2. Working Diagram

B. Software Requirements

1) *HTML:* HTML stands for HyperText Markup Language. It is used to design web pages using the markup language. HTML is the combination of Hypertext and Markup language. HTML is used to create the structure of web pages that are displayed on the World Wide Web (www).

2) *CSS:* Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in HTML. CSS is designed to enable the separation of content and presentation, including layout, colors, and fonts.

3) *Python:* Python is a high-level, general-purpose programming language. Python can be used on a server to create web applications.

4) *Flask:* Flask is a microframework for developers, designed to enable them to create and scale web apps quickly and simply. This web application will be a web page, a wiki, or a big web-based calendar application or commercial website.

5) *MongoDB:* MongoDB is a source-available cross-platform document-oriented database program. MongoDB makes working with data easy. MongoDB is developed by MongoDB Inc. and licensed under the Server-Side Public License which is deemed non-free by several distributions.
6) *Computer Vision Library:* Computer vision libraries provide in-built functions and optimized algorithms for various image and video processing tasks. These libraries help data scientists and machine learning engineers save significant time and resources when performing complex image/video processing and analysis tasks with minimal coding.

C. Comparison with Existing System

TABLE I
COMPARISON OF PROPOSED SYSTEM WITH EXISTING SYSTEMS

Existing systems	Proposed System
Existing systems provide authentication based on knowledge (or) ownership (or) biometric factors.	Our proposed system confirms a user's identity using two distinct authentication factors. • Knowledge • Biometric
Unauthorised physical access may or may not be prevented.	Unauthorised physical access is prevented due to the presence of face authentication.
Bots may or may not gain access to the system.	Access of bots is prevented.
Hackers may or may not hack the system.	Involvement of hacking is curbed due to the presence of layer 2: face authentication.
Less reliable and less compliant.	More reliable and more compliant.

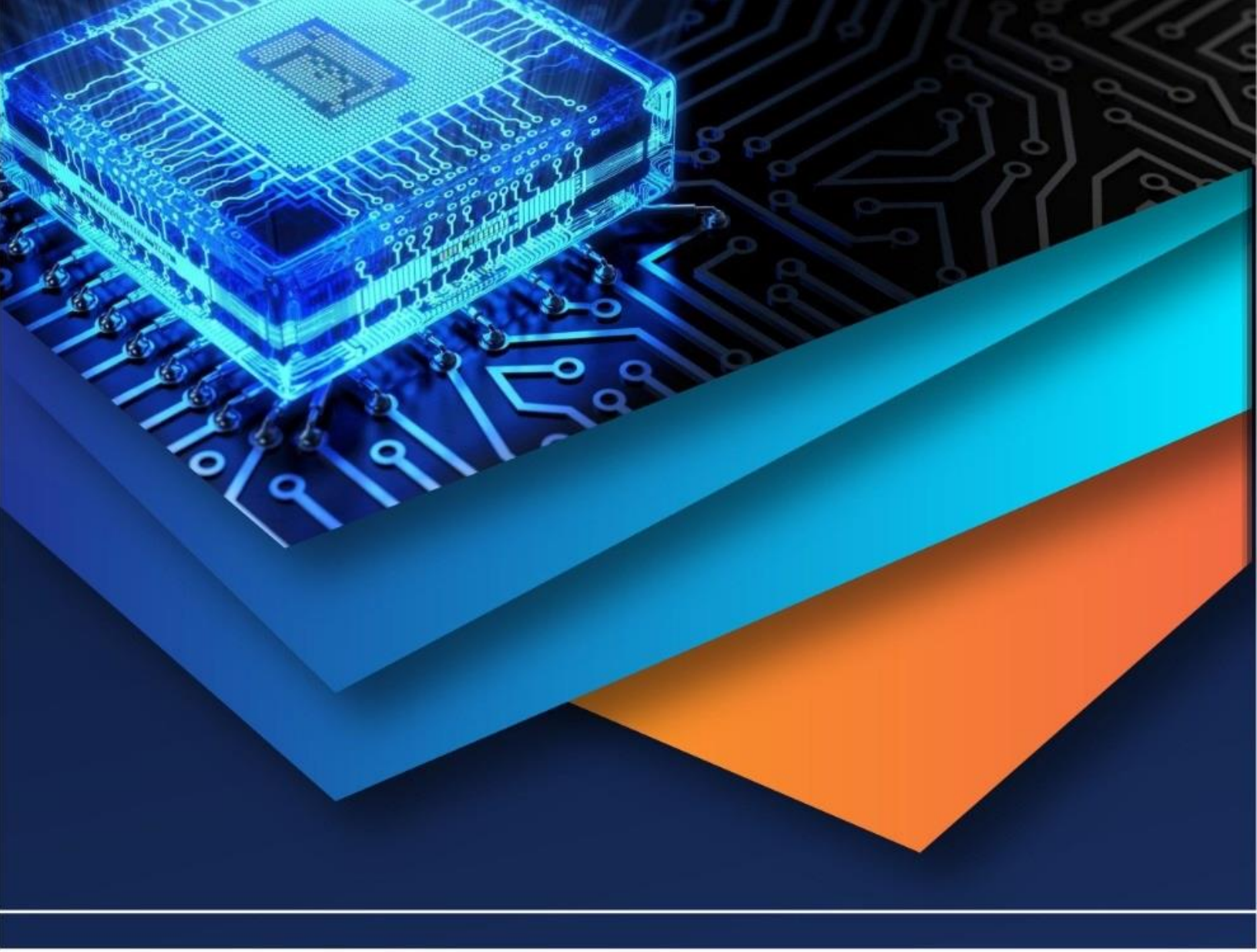
V. CONCLUSION

There are ongoing advancements in 2FA research and development, including the use of biometrics, wearable devices, behavioral-based methods, and machine learning algorithms, among others, to further enhance the security and usability of 2FA. Hence, this secure authentication system significantly increases the security of online accounts and systems by requiring users to provide two different forms of authentication [6], typically something they know (e.g., password) and something they have (biometric feature) [11], making it more difficult for unauthorized users to gain access.

REFERENCES

[1] http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA.
[2] Parag Achaliya, Govind Bidgar, Hrutika Bhosale, Prasad Dhole and Kajal Gholap, Securing ATM using Face Recognition Authentication and OTP, March 2021
[3] Ammar Hameed Shnain and Sarah Hadi Shaheed , The use of graphical password to improve authentication problems in ecommerce, AIP Conference Proceedings 2016, 020133 (2018) https://doi.org/10.1063/1.5055535

[4] Z. Rui and Z. Yan, A Survey on Biometric Authentication: Toward Secure and PrivacyPreserving Identification, in IEEE Access, vol. 7, pp. 5994-6009, 2019, doi: 10.1109/ACCESS.2018.2889996.
[5] Dr S Sasipriya, Dr P. Mayil Vel Kumar and S. Shenbagadevi, Face Recognition based new generation ATM system, European Journal of Molecular & Clinical Medicine, ISSN 2515-8260 Volume 7, Issue 4, 2020
[6] https://en.wikipedia.org/wiki/SHA-2
[7] Edward F. Gehringer Choosing passwords: Security and Human factors IEEE 2002 international symposium on Technology and Society, (ISTAS'02),\ ISBN 0-7803-7284-0, pp. 369 - 373, 2002.
[8] Sagar Acharya, Apoorva Polawar, Priyashree Baldawa, Sourabh Junghare, P.Y. Pawar, Internet Banking Two Factor Authentication Using Smartphone, IJSER, IJSER, Volume 4, Issue 3, March Edition, 2013, (ISSN 2229- 5518)
[9] Aladdin Secure SafeWord 2008. Available at http://www.securecomputing.com/index.cfm?skey=1713
[10] Olufemi Sunday Adeoye Evaluating the Performance of two-factor authentication solution in the Banking Sector IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.
[11] Laka, P., & Mazurczyk, W. (2018). User perspective and security of a new mobile authentication method. Telecommunication Systems, 69(3), 365–379. https://doi.org/10.1007/s11235-018-0437- 1
[12] González Briones, A., Chamoso Santos, P., & López Barriuso, A. (2016). Review of the main security problems with multi- agent systems used in e-commerce applications. https://gredos.usal.es/bitstream/handle/103 66/132092/Review_of_the_Main_Security _Problems_wit.pdf?sequence=1&isAllowe d=y



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY