# USER AUTHENTICATION BY USING BIOMETRICS & GRAPHICAL PASSWORDS BY IMPROVISING CONVENTIONAL METHODS USING SHA-256 HASH ALGORITHM WITH RANDOMIZED KEY SUPPORT

Jitendra Kumar Kanwaria[1], Krishna Gupta[2]
[1]M.Tech Scholar, [2]Assistant Professor
[1,2]Department of computer science and engineering, Yagyavalkya Institute of Technology, Jaipur (Raj), India

***Abstract : Data security alludes to defensive processed protection estimates that are connected to avoid unapproved access to PCs, databases and sites. Information security in addition shields knowledge from uncleanness. Information security may be a basic a part of IT for associations of every size and kind. Information security is otherwise known as knowledge security (IS) or computer security. Instances of Information security advancements incorporate reinforcements, knowledge meshing and information wipeout. A key information security innovation live is coding, wherever processed knowledge, programming/equipment, and onerous drives are disorganized and afterward rendered unintelligible to unapproved users and programmers. one among the foremost commonly practiced methods for rehearsing knowledge security is that the utilization of authentication. With authentication, users should produce a secret word, code, biometric knowledge, or another form of information to ascertain temperament before access to a framework or knowledge is conceded. The proposed work includes the idea to stack the finger print/picture of the client, the dataset for the finger print is taken for the finger print reenactment of the enlisted clients. The client when snap on the heap photograph catch, pop will seem to choose the area where lives the record comparing to the finger print[1]. At that point the SHA 256 calculation will be included for the age of the hash code which is identified with the fingerprint and the a few pictures are additionally given the alternative of clicking over the pictures, here the selected snaps on every one of the pictures are records and will create the secret phrase in relationship with the hash of the photograph. the created OTP will further raise the degree of security. The outcome examination when contrasted with the base work, by utilizing the different on the web and disconnected instruments of registering the secret word quality, demonstrates that the bit quality is nearly expanded in excess of multiple times the base work and furthermore the entropy for the secret word or OTP which is produced is expanded to the extensive sum. The result of comparison is quite effective and promising towards the security.***

***Index Terms - Authentication, Data Communication, Biometric, Finger Print, SHA-256.***

## I. INTRODUCTION

Biometrics is the estimation and factual investigation of individuals' special physical and social attributes.[1] The innovation is for the most part utilized for ID and access control, or for recognizing people who are under reconnaissance. The fundamental reason of biometric confirmation is that each individual can be precisely recognized by their natural physical or social characteristics. The term biometrics is gotten from the Greek words bio meaning life and metric importance to quantify. [1] Confirmation by biometric check is winding up progressively normal in corporate and public security frameworks, purchaser gadgets and purpose of-offer applications. Notwithstanding security, the main impetus behind biometric check has been comfort, as there are no passwords to recall or security tokens to convey. Some biometric techniques, for example, estimating an individual's walk, can work with no immediate contact with the individual being verified.

Parts of biometric gadgets include:

- A peruser or filtering gadget to record the biometric factor being confirmed.
- Programming to change over the checked biometric data into an institutionalized advanced organization and to think about match purposes of the watched data with put away data.
- A database to safely store biometric data for examination.

Biometric data might be held in a brought together database, albeit current biometric usage regularly depend rather on social affair biometric data locally and afterward cryptographically hashing it so confirmation or recognizable proof can be cultivated without direct access to the biometric data itself.

The two primary sorts of biometric identifiers rely upon either physiological qualities or social attributes.

Physiological identifiers identify with the structure of the client being validated and include: Facial acknowledgment, Fingerprints. Finger geometry (the size and position of fingers), Iris acknowledgment, Vein acknowledgment, Retina filtering, Voice acknowledgment, DNA coordinating etc.

Social identifiers incorporate the special manners by which

people act, including acknowledgment of composing designs, strolling step and different motions. A portion of these social identifiers can be utilized to give ceaseless confirmation rather than a solitary coincidental verification check.
Points of interest and detriments of biometrics
Along these lines utilization of biometrics has a lot of favorable circumstances and impediments with respect to its utilization, security and other related capacities. Advantages include:
Merits of Biometrics Difficult to phony or take, in contrast to passwords. Usability and comfort , Change minimal over a client's life, non-transferrable. Layouts take up less capacity Detriments, expensive to get a biometric framework fully operational. [1]
Biometrics aren't private and are Hackable if used alone for security purposes.

## II. RELATED WORK

Deepti Goswami, Saurabh Mukherjee [1] Author in paper discusses the variied mechanism employed to categorize fingerprints into basic classes like arch, whorl, left loop, right loop and tented arch illustrating the advantages and drawbacks of each approach. Author is providing a concise study and performance based comparison of various fingerprint classification approaches and the different techniques they use to perform the classification. Fingerprint classification plays an important role in automatic recognition of fingerprints, dataset provided. Fingerprint classification depicts a coarse level matching of a fingerprint image to its relevant classes, this results in compacted search space and thus improved recognition rate in any automated recognition system. Varied range of algorithms suggested to perform this task, each with their unique set of advantages and loopholes.

A. M. Eljetlawi et.al 2010 [2] Graphical passwords are an elective validation technique to alphanumeric passwords in which clients click on pictures to confirm themselves instead of sort alphanumeric strings. This exploration expects to think about the ease of use highlights of the acknowledgment base graphical secret word techniques accessible and separate the ease of use highlights of the current strategies. In this paper creators think about the acknowledgment base graphical secret phrase type with the accessible techniques from the ease of use perspective as per past investigations and overviews.

At that point creators coordinate the ease of use highlights (General ease of use highlights, existing ease of use highlights for existing graphical secret phrase strategies, and ISO ease of use highlights) to the current graphical secret phrase techniques and make a correlation contemplate between these techniques and the ease of use highlights. Creators have discovered that there is no technique has the most significant convenience highlights. Along these lines, by finishing this investigation a lot of ease of use highlights is recommended to be in one graphical secret word framework. This set incorporates the simple of utilization, remember, creation, learning and fulfillment. Besides, this work proposes to assemble another arrangement of graphical secret word framework that gives promising ease of use highlights.

M. ArunPrakash and T. R. Gokul 2011 [3] A graphical secret phrase is a validation framework that works by having the client select from pictures, in a particular request, exhibited in a graphical client interface(GUI). The most widely recognized PC validation strategy is to utilize alphanumerical usernames and passwords. This strategy has been appeared to have huge downsides. For instance, client will in general pick a passwords that can be effectively speculated. Then again, in the event that a secret key is difficult to figure, at that point it is regularly difficult to recollect.

In this paper, creators direct a far reaching overview of the current graphical secret key procedures and proposed another strategy. Creators examine the qualities and restrictions of every technique and bring up the future research headings here. And furthermore real plan and usage issues are unmistakably clarified. The principle favorable position of this strategy is it is hard to hack. For instance, If there are 100 pictures on every one of the 8 pages in a 8-picture secret key, there are 100^8 or 10 quadrillion (10,000,000,000,000,000), potential blends that could shape the graphical secret key. In the event that the framework has the worked in deferral of just 0.1 second after the choice of each picture until the determination of the following page, it would enjoy a huge number of years to reprieve into the framework by hitting it with arbitrary picture arrangements. Subsequently hacking by irregular blend is unthinkable.

S. Shen et.al 2017 [4] Smart portable terminal are a fundamental gadget in our life today. The client more often than not enters in the related words or draws a straightforward realistic on the touch screen as passwords for opening the screensaver. Despite the fact that along these lines can furnish clients with straightforward and advantageous security system, the procedure would build the danger of words or realistic data spillage under the severe security thought. As a rule for this sort of keypad lock screen application you can just redo the basic example or swipe-to-open screen with a static picture on a foundation picture that you select to open your telephone.

Accordingly, the invested individuals could get an opportunity to listen stealthily the basic realistic example data so as to hacking the savvy gadget for taking the individual data. Because of absence of the correct character validation system in the normally keypad lock screen application, this paper proposes another realistic example assurance instrument for improve confirmation level in the keypad lock screen application field.

By haphazardly changing the fixed position of the computerized designs that shows on the touch screen, the client can draw diverse realistic example each time dependent on the remarkable or reinforcement PIN secret phrase to open the screen. Not just included the arbitrary realistic example validation strategy without a doubt increment the individual mystery data being stolen trouble and unpredictability, it gives more security level than the customary realistic example verification in keypad lock screen too.

K. Irfan et.al 2018 [5] Traditional content based secret word plans are exposed to lexicon assaults on an extremely huge scale. As an answer, graphical secret word plans are a promising option in contrast to content based acknowledgment plans where rather than content, pictures are picked for a secret key. Be that as it may, these plans are again influenced because of shoulder surfing and less compelling because of huge word reference space.

This paper centers around giving an answer dependent on content based graphical secret word systems, a blend of Déjà vu and Moveable Frame plot. A sensation that this has happened before is additionally supplanted by content based pictures than absolutely designs. Our exploration has two principle destinations: 1) To foil shoulder surfing 2) To limit the inquiry time of pass pictures on the login screen. The undertaking was actualized as a subsequent android application utilizing Android Studio. Results demonstrate the proposed plan of graphical secret word framework with various letters in order pictures is progressively conspicuous and has less subjective burden on client when contrasted with picture based graphical secret key plans. The off base login rate for various letter set based pictures with versatile casing was 15% more than graphical secret word plots therefore a superior answer for secure shoulder surfing.

L. T. Hui et.al 2014 [6] User verification depends to a great extent on the idea of passwords. Be that as it may, clients think that its hard to recollect alphanumerical passwords after some time. At the point when client is required to pick a protected secret key, they will in general pick a simple, short and uncertain secret key. Graphical secret phrase technique is proposed as an elective answer for content based alphanumerical passwords. The reason of such proposition is that human mind is better in perceiving and retaining pictures contrasted with customary alphanumerical string. Consequently, in this paper, creators propose a theoretical system to all the more likely comprehend the client execution for new top of the line graphical secret phrase strategy. Our proposed structure depends on crossover approach joining various highlights into one. The client execution test investigation called attention to the adequacy of the proposed structure.

A. Bianchi et.al 2016 [7] PassBYOP is another graphical secret word plot for open terminals that replaces the static computerized pictures normally utilized in graphical secret word frameworks with customized physical tokens, thus as advanced pictures showed on a physical client possessed gadget, for example, a cell phone. Clients present these pictures to a framework camera and after that enter their secret phrase as an arrangement of choices on live video of the token. Exceedingly particular optical highlights are removed from these choices and utilized as the secret phrase. Creators present three plausibility investigations of PassBYOP looking at its unwavering quality, convenience, and security against perception. The unwavering quality examination demonstrates that picture highlight based passwords are feasible and recommends suitable framework limits - secret phrase things ought to contain at least seven highlights, 40% of which should geometrically coordinate firsts put away on a confirmation server so as to be made a decision about proportionate.

## III. PROPOSED WORK

This section will explain the working of the work which is proposed and the explanation of the algorithms which are for the each section working.

Description of previous work and finding loop holes in conventional system.
Hash algorithms are one way functions thereby turning any amount of data into a fixed-length "fingerprint" irreversible in nature, collectively having the property that if the input-involvement changes by even by minute bit, the resulting hash created is completely altered.[9]
In our paper Hashising is done via SHA-256 is one of the six variants of SHA family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA512/256) hash("hello")=
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e730
43362938b9824
hash("hbllo")=
58756879c05c68dfac9866712fad6a93f8146f337a69afe7dd2
38f3364946366
we want to store passwords in a form that protects them even if the password file itself is compromised, but, we need to be able to verify that a user's password is correct at same instance. The general workflow for account registration and authentication in a hash-based account system stated as follows: 1. The user creates an account. 2. Their password is hashed & stored in the database & In no case is the alphanumeric typescript (unencrypted) password ever written to the hard drive. 3. When the user attempts to login, the hash of the password they entered is checked against the hash of their real password (retrieved from the database). 4. If the hashes match, the user is granted access. If not, the user is told they entered invalid login credentials. 5. Steps 3 and 4 repeat every time someone tries to login to their account for a number of times as desired by system to login cryptographic hash function algorithms used to implement password hashing like SHA256, SHA512, RipeMD, and WHIRLPOOL are renowned. As many ways to recuperate passwords from plain hashes are very quickly developed as cracking via guess. but here are several easy-to-implement techniques that make these "attacks" much less effective and is discussed in this paper as improvising conventional methods to use graphical passwords. most communal ways of guessing passwords are dictionary attacks and brute-force attacks.
Dictionary attack uses a file containing words, phrases, common passwords, and other strings that are likely to be

used as a password. word in the file is hashed, and its hash is compared to the password hash. If they match, that word is the password. A brute-force attack tries every possible combination of characters up to a given length. These attacks though being computationally expensive, are least efficient in terms of hashes cracked per processor time, but these short-lived PINs or secret-code can be cracked.

How Hashes are Cracked: Commonly using tools as Dictionary and Brute Force Attacks, Lookup Tables, Reverse Lookup Tables, Rainbow Tables

Solution to above stated lags and loop holes in cracking hashes is as follows: How can hashes be made Impossible-to-crack: Keyed Hashes and Password Hashing Hardware are possible solutions. In this paper we made a provision to add a secret key to the hash so that only someone who knows the key can use the hash to validate a password. This can be accomplished two ways. Either the hash can be encrypted using a cipher like AES, or the secret key can be included in the hash.

A cryptographic hash function is a hash function that takes an input (or 'dispatch-message') and returns a fixed-size encrypted alphanumeric string, which is called the hash value (also message digest, a digital fingerprint, a digest or checksum). In cryptography, a randomized key support is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase[6]. The primary function of random-keys(salt effect here) is to defend against dictionary attacks or against its hashed equivalent, a pre-computed rainbow table attack.

Proposed work to Strengthen(improvising) Password Security

- A hash function is an one-way function (cannot be transformed input back to the way as it generated from) thus transfiguring a string of characters into a encrypted string of characters.
- A salt-effect is a series of random-keys as characters which are appended to the string before applying a hash function to it. This is to prevent dictionary attacks (attacking lot of common passwords are tested this way) Now that that's out of the way, to improve the security of the previous application we conclude as follows.

A cryptographically secure pseudorandom number generator(CSPRNG) is an algorithm that produces a pseudorandom sequence of bytes. What makes it cryptographically vulnerable and that it is very durable for someone to discriminate output from true randomness. Each password is going to have its own random salt attached to it.

Ingeneratingrandomkeys,we'llbeusing RNGCryptoServiceProvider() whose sole job is to generate random numbers and storing these numbers in a byte array. GetBytes place the bytes in the array given.

Base64 It's a textual encoding of binary data where the resultant text has nothing but letters, numbers and the symbols "+", "/" and "=". It's a convenient way to store/transmit binary data over media that is specifically used for textual data.

### *3. 1 User Registration Algorithm*

This section 3. 1 explains the whole process of registering the new user , with the guidelines of the unique registration.

```
Step 1: Input User Name, Email-ID, Finger Print (each entry be taken uniquely).
Step 2: In the first screen of the registration form , the User Name,Email-ID and Finger Print are captured.
Step 3: If UserName already in Database Then repeat from Step 1 Else Goto Step 4.
Step 4: Generate the hash Code for the Finger Print using SHA algo..
Step 5: If generated Hash code match in Database Then repeat process, else step 6
Step 6: Generate SHA256 code for Graphics Pattern(5X4 grid of the images), generate random-keys(SALT effect) and Generate Password and Save the record in database Step 7: Store all the details in the database.
Step 8: Input Secret Answer and select Show password button
Step 9: If Secret answer matches show password.
Step 10: Stop.
```

### *3.2 User Login Algorithm*

This section 3.2 explains the whole process of login of the existing users, with the guidelines of the entries which are made at the time of the registration process.

```
Step 1: Input User Name, email-id & Finger Print.
Step 2: In the first screen of the login form, the User Name other credentials and Finger Print(BIOMETRIC) are captured.
Step 3: Also enter the pattern code generated on picture selection basis as done at the time of the registration process.
Step 4: Generate the SHA-256 Code for the Finger Print.
Step 5: If User name, encrypted code of Fingerprint and Hash(of graphical credentials with randomized keys) matches Then forwarded to data transfer application.
Login Granted
Else  Step 6
Invalid Details
[End of If structure]
Step 6: Stop.
```

### *3.3 Data Sending Algorithm (shown as an application using sha-256 encryption in data transfer as well).*

This section 3.3 explains the whole process of sending the data to other users

```
Step 1: Access the sender user name using the session variable.
Step 2: Select the User from the list of users in the database.
Step 3: Enter the data or select the file to share.
Step 4: Determine the Size of the File.
Step 5: Determine the Size of the User Name.
Step 6: Subtract them largest value from the lowest.
Step 7: Generate the SHA code of the Data to sent.
Step 8: Extract that vary number of characters from the SHA code which is the Difference value
Step 9: Store the Details in the database together with the transaction ID which is unique. Step 10: Stop.
```

### *3.4 Data Receiving Algorithm*

This section 3.4 explains the whole process of data receiving.

```
Step 1: Enter the Transaction ID.
Step 2: Enter the SHA Code part value.
Step 3:  If the details match in database then:
Grant access to data or the file.
Else
Invalid Details
[End of If structure]
Step 4: Stop.
```

## IV. IMPLEMENTATION AND RESULT ANALYSIS

The implementation is done in Net and C# using SQL Server data base

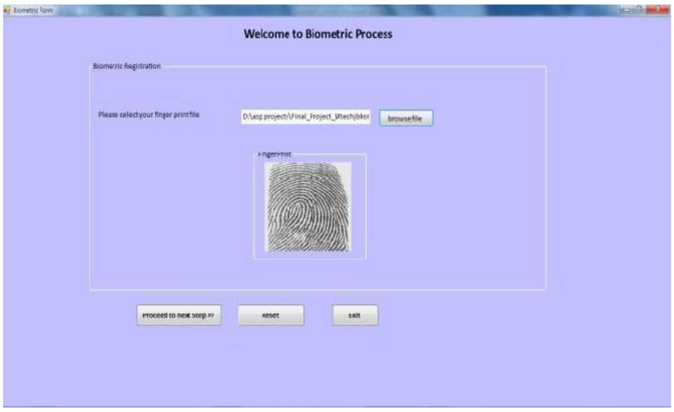

Biometric Form
Welcome to Biometric Process
Biometric Registration
Please select your finger print file
D:\asp projects\Final_Project_Mtech\bkor
browsefile
FingerPrint
Proceed to next step >>
reset
exit

Fig 1. Implementation Registration

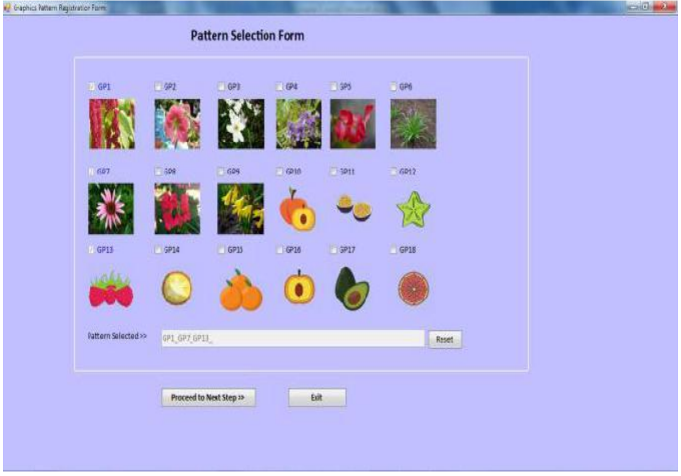
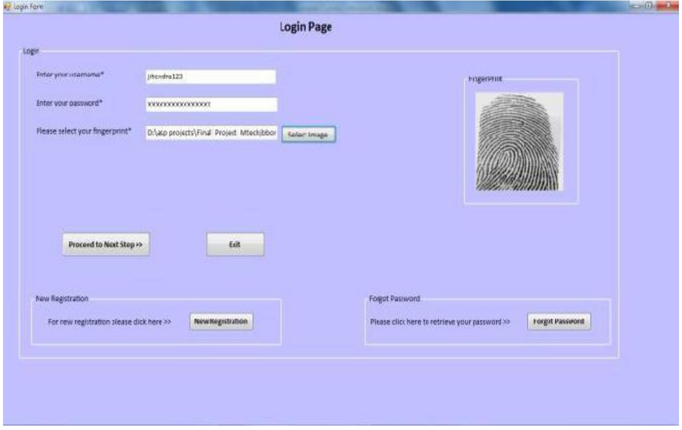
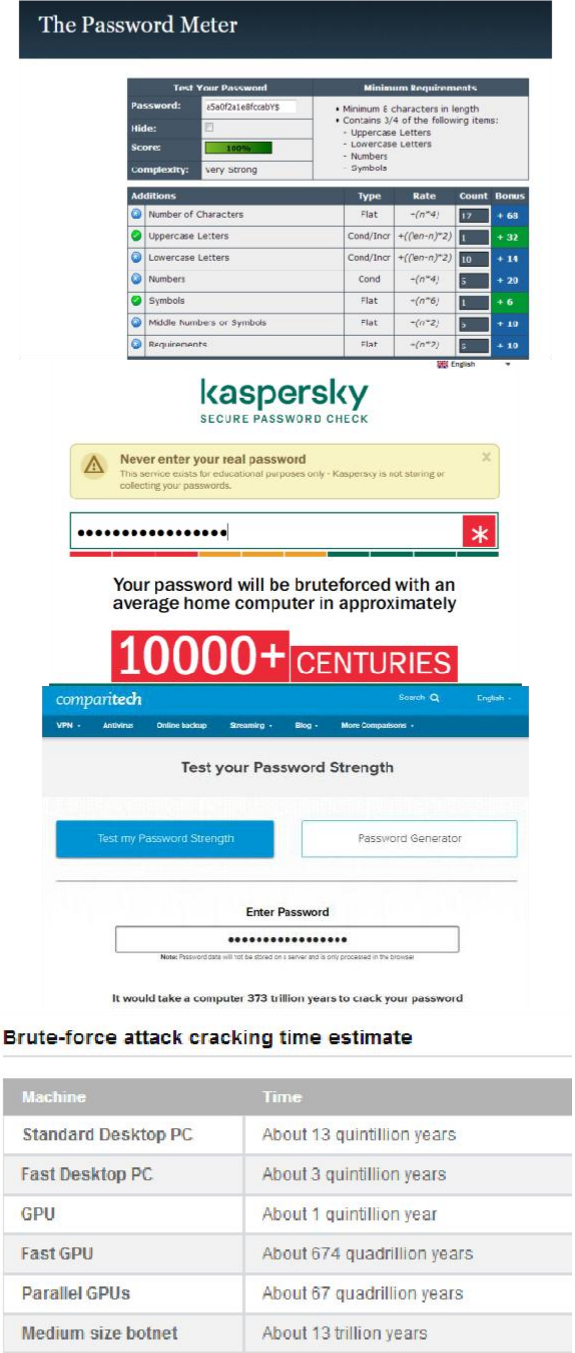


Fig 2. Registration Second Section



Login stage

Table 1.Password Strength Test Results



The Password Meter

| Test Your Password | | Minimum Requirements |
|---|---|---|
| Password: | a5a0f2a1e8fccabY$ | • Minimum 8 characters in length<br>• Contains 3/4 of the following items:<br>- Uppercase Letters<br>- Lowercase Letters<br>- Numbers<br>- Symbols |
| Hide: | □ | |
| Score: | 100% | |
| Complexity: | Very Strong | |

| | Additions | Type | Rate | Count | Bonus |
|---|---|---|---|---|---|
| ● | Number of Characters | Flat | +(n*4) | 17 | + 68 |
| ✓ | Uppercase Letters | Cond/Incr | +((len-n)*2) | 1 | + 32 |
| ● | Lowercase Letters | Cond/Incr | +((len-n)*2) | 10 | + 14 |
| ● | Numbers | Cond | +(n*4) | 5 | + 20 |
| ✓ | Symbols | Flat | +(n*6) | 1 | + 6 |
| ● | Middle Numbers or Symbols | Flat | +(n*2) | 5 | + 10 |
| ● | Requirements | Flat | +(n*2) | 5 | + 10 |

kaspersky
SECURE PASSWORD CHECK

Never enter your real password
This service exists for educational purposes only - Kaspersky is not storing or collecting your passwords.

•••••••••••••••••

Your password will be bruteforced with an average home computer in approximately

10000+ CENTURIES

Test your Password Strength

Enter Password

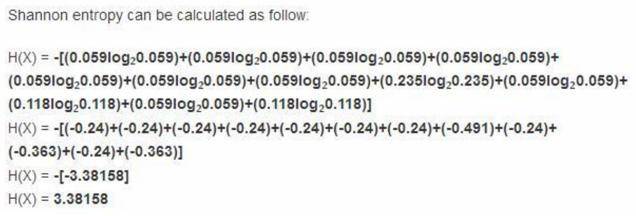
•••••••••••••••••

Note: Password data will not be stored on a server and is only processed in the browser

It would take a computer 373 trillion years to crack your password

Brute-force attack cracking time estimate

| Machine | Time |
|---|---|
| Standard Desktop PC | About 13 quintillion years |
| Fast Desktop PC | About 3 quintillion years |
| GPU | About 1 quintillion year |
| Fast GPU | About 674 quadrillion years |
| Parallel GPUs | About 67 quadrillion years |
| Medium size botnet | About 13 trillion years |



Shannon entropy can be calculated as follow:

$$H(X) = -[(0.059\log_2 0.059)+(0.059\log_2 0.059)+(0.059\log_2 0.059)+(0.059\log_2 0.059)+(0.059\log_2 0.059)+(0.059\log_2 0.059)+(0.059\log_2 0.059)+(0.235\log_2 0.235)+(0.059\log_2 0.059)+(0.118\log_2 0.118)+(0.059\log_2 0.059)+(0.118\log_2 0.118)]$$

$$H(X) = -[(-0.24)+(-0.24)+(-0.24)+(-0.24)+(-0.24)+(-0.24)+(-0.24)+(-0.491)+(-0.24)+(-0.363)+(-0.24)+(-0.363)]$$

$$H(X) = -[-3.38158]$$

$$H(X) = 3.38158$$

Shanon's Entropy Test results

TABLE 4.1 TEST RESULT ANALYSIS TABLE

| Password as Key | Website/Tool | Result |
|---|---|---|
| a5a0f2a1e8fccabY$ | Password Meter | Very Strong |
| a5a0f2a1e8fccabY$ | Password Checker | Excellent Strength |
| a5a0f2a1e8fccabY$ | My1Login | Billion years to crack |
| a5a0f2a1e8fccabY$ | Rumkin | Entropy: 84.9 bits |
| a5a0f2a1e8fccabY$ | Shannon Entropy | Entropy:3.38 |
| a5a0f2a1e8fccabY$ | Kaspersky | Billion years to crack |
| a5a0f2a1e8fccabY$ | Comparitech | Billion years to crack |

## V. CONCLUSION

The current scenario of the information transfer required being secure and no unauthorized person will able to access the crucial information. The proposed work will work in the registration and the data communication modules, in the registration the finger print based SHA-256 code will not only increase the speed of the validation of the finger print based user authentication and but also increase the accuracy of the validation on the basis of the finger print[1]. The password pattern of the data sharing which is generated on the basis of the selection of the picture-portraits of varied classification (here flora and fauna anticipated) [3,4,5,6] is an innovative concept and the increase the security. The generated pattern is evaluated and analyzed on the various tools , the result which is received is quite effective and a better entropy is attained.

In the future, we further like to extend in the field of the retina based passwords, video based passwords [7,8] and more.

## REFERENCES

[1] Deepti Goswami, Saurabh Mukherjee Comparative Analysis of Fingerprint Classification Algorithms- A review Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

[2] G. Yang, "PassPositions: A secure and user-friendly graphical password scheme," 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali, 2017, pp. 1-5.

[3] A.M. Eljetlawi and N. Ithnin, "Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods," 2008 Third International Conference on Convergence and Hybrid Information Technology, Busan, 2008, pp. 1137-1143.

[4] Abdul Rahim M and Anandhavalli D, "Implementation of image based authentication to ensure the security of mail server," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, Ramanathapuram, 2014, pp. 555-558.

[5] S. Shen, T. Kang, S. Lin and W. Chien, "Random graphic user password authentication scheme in mobile devices," 2017 International Conference on Applied System Innovation (ICASI), Sapporo, 2017, pp. 1251-1254.

[6] K. Irfan, A. Anas, S. Malik and S. Amir, "Text based graphical password system to obscure shoulder surfing," 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, 2018, 422-426.

[7] L. T. Hui, H. K. Bashier, L. S. Hoe, G. K. O. Michael and W. K. Kwee, "Conceptual framework for high-end graphical password," 2014 2nd International Conference on Information and Communication Technology (ICoICT), Bandung, 2014, pp. 64-68.

[8] Bianchi, Andrea & Oakley, Ian & Kim, Hyoungshick.,"PassBYOP: Bring Your Own Picture for Securing Graphical Passwords",. IEEE Transactions on Human-Machine Systems. ,2015.

[9] S. Zhou and X. Lu, "Fingerprint Identification and its Applications in Information Security Fields," 2010 International Conference of Information Science and Management Engineering, Xi'an, 2010, pp. 97-99.

[10] D. Brown and K. Bradshaw, "Improved Fingercode alignment for accurate and compact fingerprint recognition," 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2016,pp 1-6