SANGAM International Journal of Multidisciplinary Research

Vol. 01, Issue 01, September (2023 **)**

E-ISSN: 2584-086X

Machine Learning Based Password less Authentication System

[1]Dr. Awanit Kumar, [2]Abdul Hamid Quireshi

[1]Asst. Professor Dept. of Computer Science & Engineering, Modern Institute Of Technology and Research Centre, Alwar, Rajasthan, India, itsawanitkumar@gmail.com

[2]Head of. Dept. Computer Science, International School of Jeddah, Saudi Arabia, hamidsojat@yahoo.com

Available online at: www.sijmr.org

Abstract— Making world password less is not only a optimization technique but it's an Artificial intelligence which runs behind the system, which allows users to secure access to their login portal or apps, and other protected services with just a single finger touch, iris recognition or face detection which is a part of Machine Learning and deep neural network. This all system required lots of data and among those data; it does the feature extraction and finds the patterns from them. Feature selection is the major part for data prediction or finding similarity among them. Finding a pattern from dataset can be possible by training lots of data and then find the similarities among them by applying some machine learning or deep learning algorithms. Recently Microsoft has proposed window hello for similar type authentication.

Keywords—Windows Hello, Finger Print Detection, Pattern Recognition, Machine Learning, Deep Learning.

I. INTRODUCTION

Artificial Intelligence has made todays word easy and more advance, making a machine learn through data and perform certain task is called machine learning. And making more advance level of machine learning is called deep learning. Deep learning has various application like face detection, fingerprint recognition which is now available in maximum mobile devices for device lock. Similar to these applications Microsoft has now introduced Windows Hello which gives permission to users for smart way to access or login into their applications or completes secured transaction using single finger touch or iris recognition and face detection.

Still a question might be moving in your mind that is window hello is a deep learning? Yes such techniques require lots of data to find pattern and follow exact output. Windows Hello has unique feature such as special machine learning techniques which detect patterns and matches from its dataset then permit user to carry forward their transaction or operations technology which allows Windows 10 users to authenticate secure access this takes input from user and store in it and when next time you want to login it fetch data from database or find patterns, as example mobile devices or few of laptops are now a days uses biometric-finger pattern or iris and face to unlock when they are turned on first time. These applications can be used in other peripheral devices or application which allows transaction services or online services like Paytm and Phonepe which is most popular application in india for various purposes like bill payment, online shopping‟s and etc., to complete transaction in these applications password is required, always remembering a password for different applications with different password is not an good idea. To overcome in these situations we need a unique and smart unlock system.

Detecting finger, iris or face can make world Password less. It is essentially an alternative to remembering passwords and typing password always is widely considered to be a more user friendly, traditional logins using passwords and making it remember all the time. Now a days users have various account on social network and application or payment gateway to make it secure and reminding different password for all is not possible, so there should be a technique which can help us to get access in anywhere in just a single touch.

II. WORKING OF BIOMETRIC PATTERN

When someone think to implement passwords less techniques few points to be deliver as key promises:

1. User promise: Users should never have to deal with text password or pattern lock systems ever.
2. Security promise: User credentials cannot be cracked, breached, or phished.

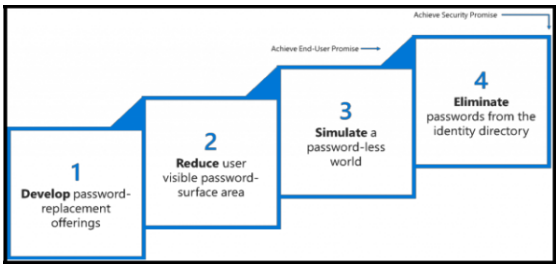

Figure 1: Password-less strategy [1]

Artificial Intelligence (Machine learning or Deep learning) apply some gesture like facial recognition, iris recognition or fingerprint to log into a device. Recently Microsoft has launched Window Hello which aligned with the Fast Identity Online (FIDO) [1]. FIDO2 security keys by the FIDO working group, are updating Windows Hello to enable secure authentication for many new scenarios.

Machine learning has brought a revolution in many industries like E-Commerce, Telemarketing, Finance & Marketing as they predict Data and provide exact or nearby result so that organization can get maximum profit. Machine learning plays major role in Face detection, Iris recognition, and biometric readings. Some Features which should be applied in it are:

1. **Password-replacement:** Remove text or written to Pattern recognition format (Biometric, Facial Recognition, Iris detection).

2. **User invisible password:** Pattern passwords are more secure and invisible.

3. **Simulate a password-less Technique**: Applying devices through which user can authenticate login to any website, payment gateway etc.

4. **Remove passwords from the identity directory:** No need to write and save password anywhere.

III. FINGERPRINT IDENTIFICATION

Similarity metric is used for measuring the apparent „distance" between two fingerprints. Let distance (x, y) the distance between two fingerprints x and y [2]. Let x1…. x_n represent n

fingerprints taken from the same finger.

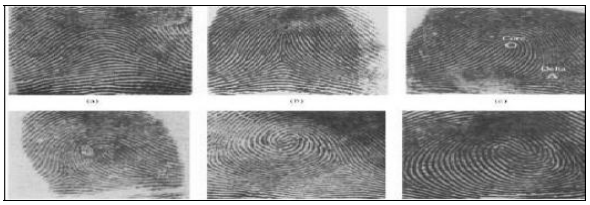

Fig 2: Possible types of finger impressions.

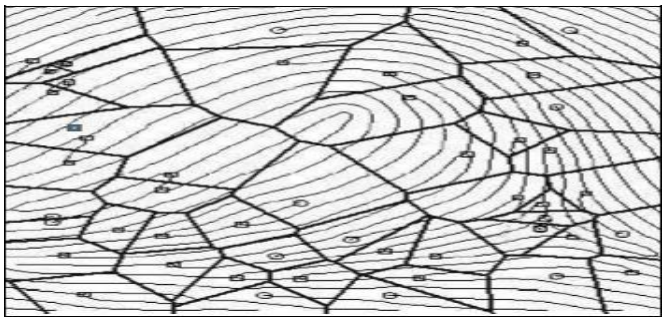

Fig 3: Enhanced image of fingerprint minutiae graphs.

IV. HOW IT WILL WORK

Analyze the data and algorithm to be operated on. Collect

database of categorized fingerprint-images. Then ssystematically generate all points of fingerprint-images. Distance based minutiae calculation to find each point closer and forming angles [7].

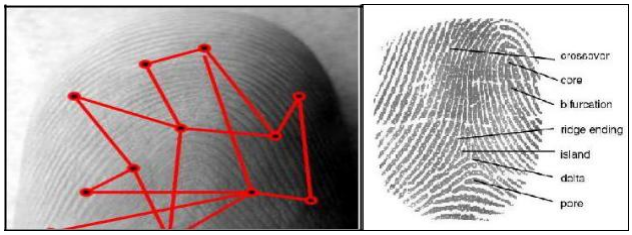

Figure 4: Different point and distance from each.

The first distance, denoted by *dist1*, is the distance between each point denoted in above figure. Applying Euclidian to x_1, x2…x_n represents the distance between the all the points.

$$dist1 = \sqrt{(x_2 - x_{i1})^2 + (y_2 - y_1)^2}$$

$$dist2 = \sqrt{(x_2 - x_3)^2 + (y_2 - y_3)^2}$$

$$dist3 = \sqrt{(x_1 - x_3)^2 + (y_1 - y_3)^2}$$

Where (x2, y_2) are the coordinates of the lower point and (x_1, y_1) are the coordinates of the upper point of the

fingertip, while (x3, y_3) are the coordinates of the central point of the 2 fingertip.

The computed angles are: *alpha*, which is the angle between the two points; *beta*, the 1 angle with Ox axis and *gamma*, the 2 points angle with Ox axis

alpha = beta – gamma

$$\text{beta} = \frac{y_3 - y_1}{x_3 - x_1}$$

$$\text{gamma} = \frac{y_3 - y_2}{x_3 - x_2}$$

The basic idea was to find the pattern of finger on basis of distance and detect finger among large dataset, An algorithm were used, dataset were generated and some coding were done in python programming to classify images and then k-mean algorithm were used to find the distance and detect the pattern. While other option is it can be done by some mathematics behind it.

Images can be of various inputs like rotated, tilted, tightly pressure, shifted downwards or upward, and shifted left or right, analyze these data visually and we have written an pseudo code to obtain graphical view of the sets of minutiae by displaying their x/y-position, type and angle graphically and detect the finger print.

• Find feature formations of minutiae which are present in both datasets.

• Compare it and match.

• See whether there are accurate and appropriate accordance‟s visible between the datasets.

• If not: The above given pattern can be formalized and transformed into an algorithm. It is not possible for a human to check large dataset.

V. POINT DETECTION

First detect the all points marked, choose point which has maximum distance and has the most variant changes in the directions of the lines, A fingerprint can have unique structures, like global and the local structure [8]. In the global structure the it has ridge ending, core and bifurcation where as local structure have island delta and pore with unique pattern around a minutiae which is a point position in the finger where a ridge is suddenly broke and two ridges are merged.

When we did not get clear images of the fingerprint, it‟s called noisy data that means image is not clear [8]. For each point we have special symmetry properties which help to identify the patterns. We have applied complex filtering methods and some basic mathematics like finding distance between two points. The algorithm for point detection is:

1. Complex filter of order m are modeled by exp {Φ }. A polynomial approximation of these filters in Gaussian windows yield (x+iy)g(x ,y) where g is a Gaussian defined as g(x,y)=exp{-x2 +y2 /2σ2 }

2. Now these filters are applied to the complex valued orientation tensor field image z(x,y)=(fx+ify)2 where fx and fy are the derivative of the original image in the 2 plane direction.

3. Differentiate the both derivative points:

$$h1(x,y)=(x+iy)g(x,y)$$
$$=\text{rexp}(i\Phi)g(x,y)$$
$$h1(x,y)=(x-iy)g(x,y)$$
$$=\exp(-i\Phi)g(x,y)$$

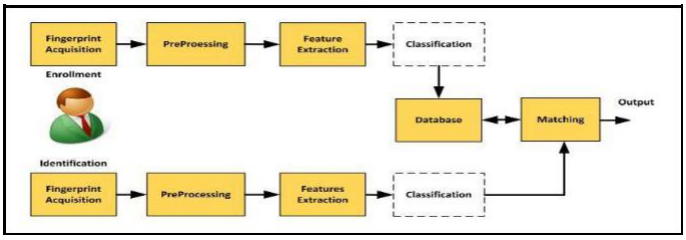

Fig 5: A flowchart of fingerprint identification system (basic components) [4].

REFERENCES

[1] https://cloudblogs.microsoft.com/microsoftsecure/2018/05/01/bui lding-a-world-without-passwords/

[2] https://sites.math.washington.edu/~morrow/mcm/uw28_04.pdf

[3] https://uanews.arizona.edu/story/ua-mathematicians-predict-patterns-fingerprints-cacti

[4] https://www.researchgate.net/publication/291098892_Machine_L earning_Techniques_for_Fingerprint_Identification_A_Short_Re view

[5] https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

[6] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[7] https://pdfs.semanticscholar.org/ec06/71c4ab7c2845e75023adcf0 d8c8967c813ed.pdf

[8] https://www.ijser.org/paper/Finger-And-Face-Recognition-Biometric-System.htm

