**Journal of Mines, Metals and Fuels,** 71(5): 593-601; 2023. DOI: 10.18311/jmmf/2023/34156

Print ISSN : 0022-2755

Journal of Mines, Metals and Fuels

Contents available at: www.informaticsjournals.com/index.php/jmmf

# Collated, Sequential and ML Approaches of Multi-Variant Features of Users on Authentication

**Supriya Chakraborty[1], Arnab Chakraborty[1] and Harshit Purohit[2]**

*[1]Amity Institute of Information Technology Kolkata, Amity University Kolkata. India. E-mail: schakraborty5@kol.amity.edu / chakrabortyarnab586@gmail.com*

*[2]Amity School of Engineering and Technology Kolkata, Amity University Kolkata, India. E-mail: harshit77441@gmail.com*

## Abstract

*In the recent days, gradually essential services and activities are becoming digitally enabled, including banking, electricity, water, etc. The envision is that digital attacks will not be limited to person, but tends to civil, caste or country wars. The authentication schemes allow the valid and original users to access such digital resources. The state-of-the-art study revealed four research questions on the sustainable and vulnerabilities on authentication schemes. These research questions are related to less interaction, resource requirements, coercive verses sequential features, and IT knowledge of users in the authentication process.*

*In this work, comprehensive experimental research is performed with different perspectives in the authentication process. The notion is to allow the users through different level of stringency in the authentication process to access from lower to high level of confidential digital resources. An organization have different impact on different digital resources. In such a context, three approaches different from each other are performed. The first approach coercively validates the authentication process whereas the second approach in sequential order. The objective is to find out the merits and demerits of each one, and in accordance with the level of confidentiality, the policy could be framed within the organization. The last approach uses the machine learning technique for the authentication process with no interactions of users. In all the approaches, the multiple features of users are considered for the experiment.*

***Keywords:*** *Authentication, collated password, sequential password, ML based authentication, Biometrics*

## 1.0 Introduction

Digital interactions in daily life are overwhelmed across the globe in recent days. Individual interactions in personal and professional level are not limited to remote servers, notwithstanding extended to continuous functioning of IoT devices in potentially significant services including power, and water sectors. Even different level of access permissions of the individuals is required in different time frame on lower to higher sensitive digital resources. One recent survey claimed that fifteen more digital interactions will be added with existing interactions of everyone by 2025[1].

In the view of above context, accessing of digital resources are crucial by individual, and devices. In the context of the service provider, before accessing the digital resources, the original end-user is verified by authentication techniques. In the research literature, many different types of authentication techniques were reported[2,3,4,5], where each one has specific scopes and purposes. The conceptual, and logical attacks by internal and external intruders of the system were also reported[6] to break such security mechanisms. The digital world was faced losses billions of dollars across all the continents for breaking such security breaches.

In accordance with specific scopes, variant authentication

*[*]Author for correspondence*

techniques were reported – the study revealed. In a broader scope, all such techniques are classified into five classes. They are Recall based (textual password), Graphical password, Token-based password, Recognition based, and Biometric. One of the common attacks with the password-based technique is the guessing attack due to low entropy[26,27]. This guessing attack could be surprisingly effective due to computational power in offline. Besides, with Trojan Horse attack the attacker may also be successful to collect the password from the end-user. To overcome the demerits of recall-based authentication, a token-based password[10] is included along with recall-based password. In accordance with the correct recall-based password, a token is sent to the registered email/mobile handset to authenticate the end-user. The accessing of mobile information in real-time was criticized by the cloning techniques[6] – A type of cyberattack. The hacking of password in personal inbox is subject to the same vulnerability as discussed above. Additionally, recall-based and token-based authentication schemes needs availability of internet and active phone connections respectively, and both authentication process could not identify, if the end-user pursue the authentication by force in presence of a malevolent person. The recognized based authentication suffers the accuracy, and false high positive results, along with dimension, light, acoustic issues, whereas the biometric based authentication face challenge on aging, life threatening, and susceptible to crime. Different but related cohesive approaches are observed in virtual environment with verification of more than one features[2,6,37] for authenticating users. The above demerits or limitations motivates for a through and detail study on authentication schemes. The observation enlisted above raises the following questions:

i. Could multiple features of users be used with correctness and soundness for authentication?
ii. Which combinations of features are best suited for specific scopes and purpose in terms of confidentiality and performance?
iii. Is it possible to reduce the external resource requirement like internet and active connections of users?
iv. Could the authentication scheme reduces annoy of the less IT knowledge users during the verification process?
v. What if the user attempts to access the higher classified digital resources by force of a malevolent user?

In this work, a comprehensive analysis is performed to discuss the minimum number of feature selections for authentication (Question i and ii) followed by three approaches are devised to address the research questions as mentioned above. Feature probing or acquisition of users are devised either in the organizational set up or applied on the mobile handset of the users. Three approaches of this work are described below:

### Collated X-Features

The number of X-features of users are grouped together for verification. The interception of features normalizes the dominance of one feature during the verification process. The order of acquisition of features are not significant in this approach. The less IT-knowledge users could bypass the intricacy during probing or acquiring the feature value (Question iv).

### Sequential X-Features

The number of X-features are verified in sequence. The order of acquisition of X-features are significant in this approach. This approach could be used in according with the policy for maintaining the confidentiality of the organization. One of the scenarios is that if X/2+1 feature is verified successfully, then the user is authenticated. However, in case of higher classified digital resource, all X-features needs to be verified successfully (Question iii).

### ML X-Features

A machine learning (ML) approach is applied for verification on the dynamic features of users. The specific scope in this regard is to determine whether the user is under any pressure or by force. In case of any inconvenience, the user attitude gets effected. The inconvenience occurs either for personal reasons or by external force. In such a case, the attitude gets differentiated in the verification process (Question v).

All three approaches discussed above, does not focus on the methodology, and verification of one specific feature of users. This work ensembles number of X-features either together or in sequence or ML-based. The proposed methodology of the authentication process described in section 3.2 is less resource intensive (Question iii).

## 2.0 Related Work

Authentication implies whether the user is genuine or not. Unquestionably, the authentication of user also allows the user the privileges and roles on the digital resources. Such privileges and roles are predefined into the system according to the policy definition of the organization. The service provider deploys a verification scheme for authenticating before accessing the services or digital resources. The numerous verification schemes are accessible to answer the different security questions in research literature and practice. These human confirmation methods are classified as follows.

## A. Recall Based

Typical authentication scheme used all over the world. This implies "what we know?". This includes textual password. In recent days, to get rid off the brute forces attacks and guess attacks, a rudimentary policy is applied to strengthen the recall-based password. The strengthen of password conform to m number of symbols where m varies six to nine and includes combination of uppercase and lowercase letters, digits, and special symbols[11]. The choice of passwords that are anything but difficult to recollect and, simultaneously, are difficult to figure. Klein[4,7] attempted to experimentally prove the relationship between all possible passwords of a person and guessing attacks. It has been observed that minimum eight-character length combination of letters and numbers are safe. Recent computational power might reframe the above length.

## B. Recognition Based

Any graphical password or face recognizable proof is example of recognition-based scheme. It Includes graphical password, iris recognition, face recognition, etc. This implies "what we recognize?"[23]. This scheme varies potentially many diversified implementations[7,8,9,10], Recognition Based uses graphical password on identification[18]. The intruder could observe substantial portion of the graphical passwords by shoulder ridding during secrecy is managed by the legitimate user.

At present, developers are still working on innovation with trial and error. A comparison based on attacks on different graphical password is shown in Table 1. Broadly, graphical passwords could be categorised into two sub-categories, namely Recall and Recognition. Pass face[14] and Story Scheme[2] are under the sub-category recognition. A different technique where the original user has to choose a specific point in the background of the image for the secrecy. Little variation of the above method is the Draw-A-Secret key. The difficulty of this scheme is that the intruder could not review the starting and end position of the drawing[2]. A different approach is to touch the different positions of the image in order to form the sub-image, which is the secrete key, such variations exist. as mentioned in[16].

## C. Token Based

This implies that "what do we have?" The collection of valid receiving source including email or mobile number of users plays a significant step, and is called registration of medium. Further, the registered medium is used to send a token within time bound manner to be reciprocated by the user. The token can be both a hard token and a soft token. Hard token are the physical devices that are given for authenticating the user to an authorized user of the network. Token-based systems are helpless against robbery and misfortune; in this way, most token-based frameworks require an individual known device like mobile number. In virtual world, 3D secret word has been proposed and starting outcomes was introduced in[2,3].

## D. Biomatrics

This implies "what we are?" Biomatrices schemes are detection based on unique human characteristics. They consist of the physiology of humans. In few cases, the accuracy of detection especially false positive exist. Personal characteristics are the limitations of using biometrics[11]. Additionally, there is a chance of distorting the natural ability of the biometrics in the long usage as users has to forcibly increase eyeball, fingers impression could be changed due to professional practice. Table 2 summarises the pros and cons of different biometrics. Human properties are helpless against changes every once in a while, because of a few reasons, for example, aging, scarring, face cosmetics, change of hairdo, and disorder (change of voice).

**Table 1: Survey of Biometric Schemes**

| Graphical password | Type of technique | Resistance to attacks | | | | | |
|---|---|---|---|---|---|---|---|
| | | Brute force | Dictionary | Guessing | Spyware or key logger | Shoulder surfing | Social engineering |
| Blonder's scheme | Recognition | YES | NOT | YES | NOT | YES | NOT |
| Draw a secret | Pure recall | NOT | YES | YES | NOT | YES | NOT |
| Passface | Recognition | YES | YES | YES | NOT | YES | NOT |
| Passpoint | Cued recall | YES | NOT | YES | NOT | YES | NOT |
| Passdoodle | Pure recall | NOT | - | - | - | - | - |
| Man et al Scheme | Recognition | YES | NOT | NOT | YES | YES | NOT |

YES- Resistant to attack & NOT- Not resistant to attack

**Table 2: Survey of Biometric Schemes**

| Method | Coded pattern | Security | Application |
|---|---|---|---|
| Hand geometry | Size, thickness, length | Low | Low security facilities |
| Signature | Shapes of letters, writing order and pen pressure | Low | Low security facilities |
| Voice printing | Voice characteristics | Low | Telephone service |
| Facial recognition | Outline, shape & distribution of eyes &nose | Low | Low security facilities |
| Fingerprint | Fingerprint | Medium | Universal |
| Iris Recognition | Iris pattern | High | High security facilities |

# 3.0 Feature Selection and Approaches

To address the first question of the introduction section, the required number of features needs to be identified as such the demerits as mentioned including less IT knowledge, aging, by-force etc are resolved. Consequently, with selected three features, three approaches Collated X-Features, Sequential X-Features and ML-based X-features are applied.

## A. Feature Selection based on Shannon Entropy

To answer the questions of the motivation of this work as enlisted in the introduction section, consider n number of users, and each is having f number of features. The idea is to determine the minimum number of features that detect each of n users and answer the questions and resolve the demerits that are enlisted in the introduction section. Formally the feature selection problem is stated as:

$$S = \underset{S'}{argmin}\{|S'| \; |S' \subseteq F \; and \; H(C \; |S') \leq T\} \quad \text{(i)}$$

Where F is a random variable imply a set of features, and C implies a set of classes, S' is a subset such that S' $\subseteq$ F, threshold value T is considered experimentally. Shannon conditional entropy of C given S' is the average residual entropy of C once S' is known, and it is stated as:

$$\begin{aligned} H_1(C|S') &= \sum_{S'} p(c) H_1(S'|C = c) \\ &= \sum_{S'C} p(s', c) \log p(s'|c) \\ &= H_1(S', C) - H_1(S') \end{aligned} \quad \text{(ii)}$$

The correlation between C and S' of Shannon mutual information is commutative iff C and S' are independent on each other[38,39]. The equation (i) is justified with three features in[39] with specific conditions as mentioned in equation (ii). This justifies with threshold value = 0 implies the highest accuracy; Shannon provides the better results. In the context of the above result, three features are considered to be applied into all the approaches.

# 4.0 Collated X-Features – Facical Expression, Eyeball Movement And Textual Password

Irrespective of using recall based followed by token-based authentication, three features of the real user are collated and verified in the authentication process, This is called Collated X-Features (CXF) password. Different combinations of features of real users are analysed in this work. In this regard, three different experiments have been performed successively to analyse the outcome.

In the Collated X-features considers facial expressions, the movement of eyeball, and textual password. These three parameters collated and form password for each real user. The deployment of this cheme is subject to two successive operations- Password Generation and Password Verification. Each of the operational step is described below.

## A. Password Generation

The three parameters mentioned above is redefined as three vectors. The vector $V_n$ contains the facial expression while entering password. The expressions are recorded as such any annoying things make the end-user worried or not. The vector only records the reflected changes in the facial expression.

The vector $V_m$ records the movement of eyeball. The deviation and/or standstill of the eyeball is measured according to the position of eye relative to the head, for the identification of elements in a visual scene.

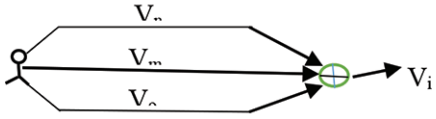
The vector Vo is a textual password while the end-user can input the textual password. Each of the vectors elicit a sequence of 1, and 0 to record the end-user data. In the experimental level, the length of each of the vector is considered as 1000; however, this is subject to further study.

A random simulation is performed to populate each vector. Few restrictions that are compiled with are that values of the expression and eyeball are ranging from (0-255) and (0,1) respectively; however, the keyboard value might be any combination of alphanumeric values with maximum length of

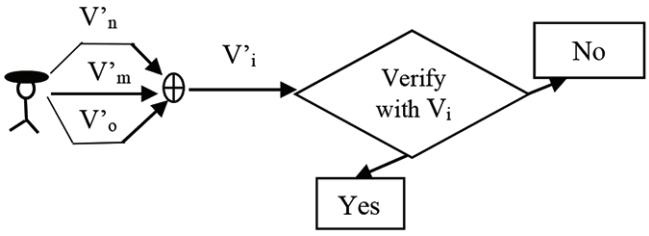
30 symbols. A formal equation is used to normalize as well as to determine the collated 3D password as follows:

$$V_i = \frac{\sqrt{V_n.V_m.V_o}}{V_n+V_m+V_o} \quad \text{(iii)}$$

Where, $V_i$ is the normalized value of the 3D password. The equ. iii provides the normalized value within the range from 0 to 1. This normalized Vi is further saved in persistent storage unit. An encryption is performed on Vi before storing in the persistent unit. The schematic diagram of the proposed methodology is presented in Fig.1. The V'n,V'm and V'o are generated at real-time and computed V'i and finally compared to the persistent Vi. If match successful, the end-user is authenticated; otherwise not.




(a) Password generation phase




(b) Password verification

Figure 1: Schematic diagram of working principle

## B. Password Verification

The verification of the password follows the same steps with the unknown end-user (user with black hat). First generates the password ($V'_i$) in real-time and compared to the existing normalized value ($V_i$). The deviation factor that comes into play is the different emotional status that might provide different facial expression, or/and exhaust mind and body that might occurs into the change in the eyeball expression. Quite obviously in accordance with the position of the present eyeball, and the movement of the eyeball is also deviated, however, the study on facial expression and eyeball movement are out of the scope of this research. In this work, the collated features are measured and test the deviation which is summarized in the result section.

### *Result Analysis*

A simulation is performed to test the proposed scheme. The average of ten sample set for $V_n$, $V_m$, and $V_o$ are generated where the length of each vector is 1000. To analyses the accuracy of the CXF based password authentication, all the sample test cases are persistently saved. we have prepared 200 (20%) random test-cases and run in real-time. The result of the verification of CXF password is plotted in the following diagram.

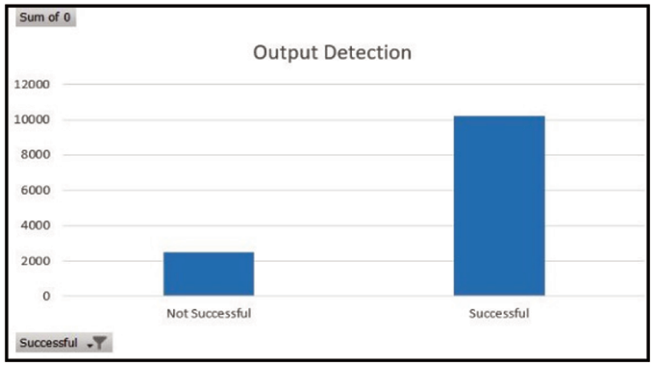



Figure 2: Successful and unsuccessful detection

Among 200 test cases of 10 sample Vectors, more than 10,000 times the end-user was detected successfully. Around 2000 cases are true negatives, and false negatives as per Fig.2. Around 80% successful results for true positive cases are found in these exhaustive experiments.

To critically understands the victims of such 20% false positives and true negatives, each sample set is depicted in Fig.3. From Fig.3, only sample set 5 performed poorly in the detection process. In real-life practice, the poor performed sample set needs to be eradicated to avoid the risk and improve the preciseness of the scheme.

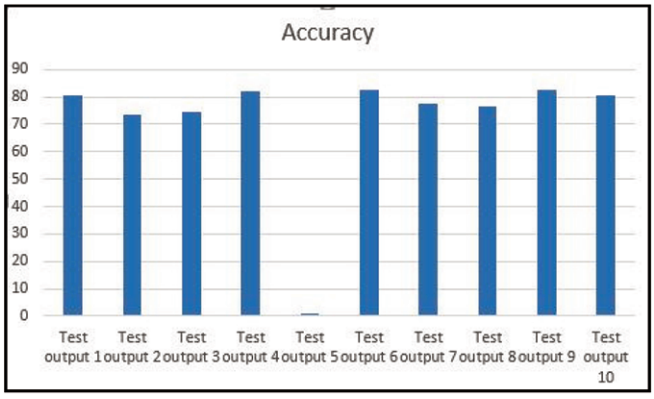



Figure 3: Average results for detecting ten samples

# 5.0 Seqential X-Features

The second analysis is done with three features Textual Password, Fingerprints, and Facial Recognition. The verification step of the authentication is performed in three separate steps for each feature sequentially. The three features with sequential verification assist to address the

**Table 3: Test cases for unique user id and textual password**

| Test | Test cases for strong password and username | Input | Status |
|---|---|---|---|
| Unique user | The details of the user get saved in the database and the registration process is completed. | Username Password | Pass |
| | If the user tries to register with the same email id more than once, then the registration process won't be successful. | | Error |
| Strong Password | It takes an input of at least 1 capital letter 2 small letters 1 special character & 3 numbers as password combinations. | Password | Pass |
| | If the user tries to log in with the wrong password combination, then the login process won't be successful. | | Error |
| User name | Input at least 6 small letters and 3 numbers as username | Username | Pass |
| | If the user provides either 9 characters or 9 numbers or use any special symbol for username | | Error |

second question mentioned in the introduction section. Classically all possible combination of three features needs to be tested on less IT knowledge people, however, in this experiment, we choose three features in such a way that has different way of interactions. The textual password is recall-based, Fingerprint is biometric-based, and facial recognition is posture based with no interaction at all.

## A. Textual Password

This scheme is tested user with strong password. The correctness and soundness need to be ensured., however all possible cases are out of the scope of this work. Six different types of test cases are jotted down in Table 3.

## B. Fingerprint Analysis

The second phase of this analysis is done using fingerprint analysis. The device description is available at "how2Electronics" site. In accordance with the phase one, the significant test cases are designed and tested for ensuring the correctness of the experiment. The summary of such test cases is specified in Table 4.

## C. Facce Recognotion

The last phase of the experiment deals with the face recognition. In this experiment, 3D normalization and template matching for each face is done to convert into the 2D image. 2D images are further compared with the existing database images for verification. Neither the convertion nor the comparsion of the 2D images are the scopes of this work. In this work, the Line Edge Maps Algorithm has used to map the facial characteristics.

The most prominent aspects of the face including eyes, nose, and mouth having the significant characteristics have been compared between existing image and real-time image. The color photos are transformed into greyscale before extracting facial similarities. The conversion from greyscale to binary image have been done using the Sobel edge detection technique.

**Table 4: Testcases for Fingerprint Analysis**

| Test | Input | Test case | Status |
|---|---|---|---|
| Unique ringerprints and repository | Scanning fingerprint | The fingerprint of the user gets saved in the database and the registration process is completed. | Pass |
| | | If the user tries to register with the same fingerprint more than once, then the registration process won't be successful. | Error |
| Area of finger | Impression | The maximum portion of the finger is used during scanning of the user. | Pass |
| | | If the user tries to log in by scanning half of the finger or a side of the finger or different fingers, process won't be successful. | Error |

### *Result Analysis*

This experimental result revealed that when an end-user head is rotated by more than 20 degrees, the identification rate plummets. The lighting effect and a recognition rate below the threshold value are also problems with 2-D face recognition algorithms.

One of the most significant factors is depth information, which is used to detect and recognize eyes, noses, and other facial features. In a two-dimensional picture, we can't see depth information, therefore it's just ignored.

This experiment demonstrated that less IT knowledge user performed very well. True Negatives have been decreased even around 76.3% with less IT-knowledge user. However, with moderated and good IT knowledge, the TRUE negatives are zero; however, the order of performing the verification is significant. In around 6% of cases the fingerprints provided False Positive, however password and face recognition are true positives for such cases. In this regard, the final decision if taken based on the correctness of two features out of three, the true positive case become 100%. However, in such case the overhead time for decision making even for the rest of the 94% of cases are very significant.

The experience of the outcome revealed that sequential verification of multiple features are cumbersome, hectic and subject to unncessarry complexity in nature comparative to collated multiple features.

## 6.0 Seqential X-Features

The ML approach was studied in many systems driven hardware devices especially on sectors like Power, Water, and etc. The popular attacks including Denial of Service[27], hacking by malware[28], Man-in-the-Middle attack[29,30] was studied in the context of IoT devices using ML approaches. The paper[31] demonstrated that false acceptance rate 31.2% less than the previous work, however, the overhead computation was drastically increased. The false reject rate, equal error rate and false/true positives were also demonstrated with ML approaches in[31].

The physical layer of IoT was identified by Received Signal Strength Indicators, Channel Impulsion response, Channel state information, and Media access control using spatial correlation in[31]. The major challenge is the dynamic nature of wireless network that change its physical layer identify over time, and ML algorithm continuously learns the identity of the network. A different approach that detected the deviation of the wireless sensor network using KNN that potentially an energy saving scheme[32]. A more interesting approach was found in[33] where unsupervised learning scheme was applied to detect the spoofing beyond the vicinity of low frequency wireless signals using Bayesian nonparametric procedure and Euclidian distances.

The above discussion revealed that approaches of computer network could not applied to the physical layer of IoT based network due to scalability and resource constraints. In this work, since multiple features were used to detect the end-user, Multiple Linear Regression has used to detect the end-user without intervention of the end-user. In this work, the end-user has been recognized based on the leg angle, leg swing, hand movement, speed of walk, head direction. In the camera view of the end-user, first the background subtraction method has been applied to extract the binary moving object, further detect the state of all the features and finally similarities have been measured with the existing movements to detect the object/end-user.

## A. Movement-based Recognition using ML

The end-user/object walk three feet distance in view of camera. The moving end-user recognition has been done in three steps.

### *State of Object in Binary Frame*

The background image of the object is fixed and unchangeable in this experiment. In the learning phase, the original frame is extracted in sequence of time $t_i$. Each frame is further converted into the HSL format[34] followed by silhouette extraction method[34] has applied in each frame. The silhouette of frames at different time $t_i$ is shown in Fig.4.

The displacement of object here is based on the tempo of the object. The tempo means the velocity of the object. In accordance with the received frames, an interpolation function is defined that exactly map the positions of the object. In each $t_i$ leg angle, leg swing, hand angle, and head direction are computed. The displacement di in each ti is based on the tempo. An interpolation technique called a fast one-pass processing for high Motion Compensated Frame Interpolation[35] has applied to object to define the corresponding function. The proposed function of[35] is modified to position the object exactly at the displacement di at time $t_i$. The frame rate is variable (x) to achieve frame-rate conversion as such object is position exactly at $d_i$ in $t_i$. The original scheme adopts a motion-compensated approach to double the frame rate by inserting one interpolated frames between any two contiguous original frames. Motion Vector Refinement for variable frame rate x is the major processing procedure to assign proper motion vectors for two additional interpolated frames. Based on this proposed scheme, one

Figure 4: Five Silhouettes of an object at different $t_i$.

interpolated frame is generated by x MCFI processing flow (the successive generation of frames generated by 4x MCFI or MEMC processing flow are discarded in this scheme as out of requirement of the scope). True motion vector assignment from x motion candidates will be used for an N×N block (by default N=8). True motions Vi when i equals 0 to 8, are checked with the SAD function from one original frame (frame t or frame t+1). This x motion assignment is formulated by:

$$\overrightarrow{MV_X} = arg\min_{\vec{v}\in S'} \sum_{x\in B} \left| f\left(x-\frac{1}{2}\vec{v},t\right) - f\left(x+\frac{1}{2}\vec{v},t+\frac{1}{2}\right)\right|$$

The above equation exactly regenerates the object position at displacement di at time ti from the initial position. (After matching with the real silhouette). The matching is performed based on four features leg angle, leg swing, hand angle, and head direction. The detail discussion of matching these four features is out of the scopes of this research, for more in-depth knowledge[35], is the reference.

Validation of Object- The learning phase generates the five silhouette images of walking object in the view of camera of 3 feet distances. The validation of object is the testing phase, where the end-user walks, and same process have applied as in the previous phase to generate five silhouettes. The challenge in this regard is the different tempo of the same end-user and therefore displacement gets different. Suppose the displacement in the validation phase is $d_j$ in time $t_i$. The difference between $d_i$-$d_j$, make the position of the silhouette different. In this regard, the modified interpolation function is applied in the validation phase to adjust the gap of the tempo and fit the silhouette of the validation face as accurate (min |di- dj|) as possible.

Result Analysis- The 97.3% accuracy have been achieved while object physical distinctions are significant. In case of Raincoat, Orna for female candidate, long suite for men candidate, the accuracy 2.7% gets reduced. In case, physically similar person, the accuracy rate was 92.7%, again the outfit of the candidate make the impact on the result.

## 7.0 References


1. Soumen Dutta (2022): Presented the Survey of Pricewaterhouse Coopper Private Limited - A Technical Litarature for Future Direction, July.
2. Dhatri Raval and Abhilash Shukla (2015): "Security using 3D Password", CMPICA CHARUSAT, Changa, *International Journal of Computer Applications* (0975-8887) Volume 120 – No.7, June.
3. Dinesha H A and Agrawal V K: "Multi-level Authentication Techniques for Accessing Cloud Services". CORI, Bangalore. Tanvi Naik, Sheetal Koul Multi-Dimensional and Multi-Level Authentication Techniques, *Information Technology*, SKNCOE, Pune
4. Fawaz A. Alsulaiman, Abdulmotaleb El Saddik, (2008): "Three-Dimensional Password for More Secure Authentication", *IEEE transactions on instrumentation and measurement*, vol. 57, no. 9 September.
5. Fawaz A Alsulaiman and Abdulmotaleb El Saddik, (2006): "A Novel 3D Graphical Password Schema", Multimedia Communications Research Laboratory University of Ottawa, Canada, IEEE 2006 International
6. Grover Aman, Narang Winnie, (2012): "4-D Password: Strengthening the Authentication Scene", *Int. Journal of Scientific & Engineering Research*, Volume 3, Issue 10, October, 1 ISSN 2229-5518
7. Jianhua Song1, Degang Wang, Zhongyue Yun1, Xiao Han1 "Alphapwd: APassword Generation Strategy Based on mnemonic Shape" School of Computer Science and Information Engineering, Hubei University, Hubei Wuhan 430062, DOI 10.1109/ ACCESS.2019.2937030, IEEE.
8. Karen Renaud", Peter Mayer†, Melanie Volkamer† and Joseph Maguire, (2013): "Are Graphical Authentication Mechanisms As Strong As Passwords?", *IEEE*
9. Mrs. Aakansha S. Gokhalea, Prof. Vijaya S.Waghmareb (2016): "The Shoulder Surfing Resistant Graphical Password Authentication Technique", 7th International Conference on communication, Computing and Virtualization, published by Elesvier, Vol: 79.
10. Ms. Vidya Mhaske Dhamdhere and Prof. G. A. Patil," Three Dimensional Object Used for Data Security", International Conference on Computational Intelligence and Communication networks, IEEE DOI 10.1109/CICN.2010.83,
11. Ms. Swati Bilapatte, Prof. Sumit Bhattacharjee, "3D Password: A novel approach for more secure authentication", *International Journal of Computer Science & Engineering Technology* (IJCSET)
12. Neha, Mr. Vinod Saroha, (2016): " Hybrid Approach of 3D Password Using Naive Bayes Classification", IJCSMC, Vol. 5, Issue. 6.
13. Prof. Sudhakar Jadhav, Prathamesh Bhawtankar, "Securing the data using advance authentication technique", GRD journals - *Global Research and Development Journal for Engineering*,Volume 1, Issue 7, June 2016 ISSN: 2455-5703
14. Paul C.V. Oorschot, Amirali Salehi-Abari, J. Thorpe, (2010): "Purely Automated Attacks on Pass Points-StyleGraphical Passwords", *IEEE Transactions on Information Forensics and Security*, vol.5, No.3, Sept.
15. Prof. Sonkar S.K, Dr. Ghungrad. S.B, (2011): "Minimum Space and Huge Security in 3D Password Scheme" *International Journal of Computer Applications*;

Vol.29, No.4, September.
16. P.K. Dhanya, M. Keerthiga, S. Dinakar, (2014): "Secured Authentication using 3D Password by Applying Ultimate Planar Algorithm", *Int. Journal of Scientific & Engineering Research*, Vol. 5, Issue 5, May.
17. Paruthi Ilam Vazhuthi P, Geetha M, Parthiban S, (2015): "A Survey on the Use of 3D Password in Security", www.ijraset.com Volume 3 Issue II, February, ISSN: 2321-9653 *Int. Journal for Research in Applied.*
18. Priya Matta , Bhasker Pant, (2018): "TCpC: a graphical password scheme ensuring authentication for IoT resources", Bharati Vidyapeeth's Institute of Computer Applications and Management 2018, Springer.
19. Ronak Talati, Shubham Shah, "Vishwakarma Institute of Information Technology, India," 4-D Authentication Mechanism", *IOSR Journal of Computer Engineering* (IOSR-JCE) e-ISSN: 2278-0661.
20. Sadiq Almuairfi, Prakash Veeraraghavan, Naveen Chilamkurti, (2013): "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices", Mathematical and Computer Modelling Elesvier, Doi: 10.1016/j.mcm.2012.07.005.
21. Sanket Prabhu, Vaibhav Shah, (2015): "Authentication using session based passwords", Int. con. on advanced computing technologies and applications, Elesvier, Doi:10.1016/j.procs.2015.03.079, Vol.45.
22. Shums Tabrez, Jagadeesh Sai D, "Pass-Matrix authentication", Ramaiah Institute of Technology Bangalore, Karnataka, India, 978-1-5386-2745-7/17/ ©2017 IEEE
23. Shah Zaman Nizamani Syed Raheel Hassan Riaz Ahmed Shaikh, (2019): "TQ-Model: A New Evaluation Model for Knowledge-Based Authentication Schemes", springer.
24. V.Sindhuja, S.Shiyamaladevi, S.Vinitha, "A Review of 3D Protected Password", *International Journal of Innovative Research in Computer and Communication Engineering*, ISSN (Online): 2320-9801
25. Vaishali Jain1, Akhil Dubey1, Banita Chadha, (2014): "A Survey in Shoulder Surfing Attack in 3D Password", IEC-College of Engineering & Technology Greater Noida, India, *International Journal of Engineering Research & Technology* (IJERT) Vol. 3 Issue 2, February.
26. Zubayr Khalid, Pritam Paul, Soummyo Priyo Chattopadhyay, Anik Naha Biswas, "Secure Authentication with Dynamic Password", Institute of Engineering and Management, Kolkata, India.
27. Ahad A., Tahir M., Sheikh M.A., Ahmed K.I., Mughees, A., Numani, A. (2020): Technologies trend towards 5g network for smart health-care using iot: A review. Sensors 2020, 20, 4047.
28. Kolias C., Kambourakis G., Stavrou A., Voas J. (2017): DDoS in the IoT: Mirai and other botnets. Computer 2017, 50, 80–84.
29. Ashraf Q.M., Habaebi M.H. (2015): Autonomic schemes for threat mitigation in Internet of Things. *J. Netw. Comput.* Appl., 49, 112–127.
30. Celesti A., Fazio M., Villari M. (2017): Enabling secure XMPP communications in federated IoT clouds through XEP 0027 and SAML/SASL SSO. Sensors 2017, 17, 301. [CrossRef] [PubMed]
31. Xiao L., Wan X., Han Z. (2018): PHY-Layer Authentication with Multiple Landmarks with Reduced Overhead, IEEE Trans. Wirel. Commun. 17, 1676–1687.
32. Branch J.W., Giannella C., Szymanski B., Wolff R., Kargupta H. (2013): In-network outlier detection in wireless sensor networks. Knowl. Inf. Syst., 34, 23-54.
33. Xiao L., Yan Q., Lou W., Chen G., Hou, Y.T. (2013): Proximity-based security techniques for mobile users in wireless networks. *IEEE Trans. Inf. Forensics Secur*, 8, 2089–2100.
34. B Noura Abd El-Moez Semary, Mohiy M. Hadhoud, Alaa M. Abbas; (2011): Space Transformation for HSL Model Encoding; ICICIS 2011.
35. Wang F., Franco-Penya, HH., Kelleher, J.D., Pugh, J., Ross, R. (2017): An Analysis of the Application of Simplified Silhouette to the Evaluation of k-means Clustering Validity. In: Perner, P. (eds) Machine Learning and Data Mining in Pattern Recognition. MLDM 2017. vol 10358. Springer, Cham.
36. Yen-Lin Lee, Truong XUAN Nguyen, (2010): High frame rate Motion Compensated Frame Interpolation in High-Definition video processing; 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP);
37. A.B. Gadicha and V.B. Gadicha, "Virtual Realization using 3D Password", *Int. Journal of Electronics and Computer Science Engineering*, ISSN 2277-1956/ V1N2-216-222
38. Cachin C. (1997): Entropy Measures and Unconditional Security in Cryptography. Ph.D. thesis, ETH.
39. Catuscia Palamidessi, Marco Romanelli. Feature selection with Rényi min-entropy. Artificial Neural Networks in Pattern Recognition - 8th IAPR TC3 Workshop (ANNPR 2018), Siena, Italy. pp.226-239.