ACTIVE BEHAVIOURAL BIOMETRIC AUTHENTICATION USING CAT SWARM OPTIMIZATION VARIANTS WITH DEEP LEARNING

Princy Ann Thomas

Department of Computer Science and Engineering, Government Engineering College Idukki,
Painavu, Idukki, Kerala, India
princy@gecidukki.ac.in

Dr. Preetha Mathew K

Department of Computer Science and Engineering, Cochin University College of Engineering Kuttanad,
Pullincunnu, Alapuzha, Kerala, India
preetha.mathew.k@gmail.com

Abstract

Security issues have only been compounded by the advent of distributed networks and global internet availability. Combating these security issues depends on being able to correctly authenticate a valid user. This paper presents variants of our CRNM framework which is an efficient cat swarm optimized deep learning model to accurately authenticate a valid user through signature behavioral patterns and biometric information of the user. The behavioral patterns considered here are keystroke and mouse dynamics. Face recognition has been included as a means to decrease the false rejection rate of the system. The major contributions of this work include comparison of various cat optimization variants for active authentication, performance analysis of our model with different state of the art systems. The fitness functions tested include Rosenbrock, Rastrigin and Griewank while CSO variants studied are ADCSO, AICSO and PCSO. Results of our experiments indicate that the proposed authentication system is faster and more efficient than existing frameworks. We achieve accuracy 98.29%, FAR 0.01 and FRR 1.02.

***Keywords*: Active authentication; Behavioral biometric; Cat swarm optimization; Hybrid deep model.**

1. Introduction

Identifying a person is one of the essential steps in conventional security systems. [Barton et al, (2016)] states that traditionally, before the advent of computers, a person was identified by their name, facial features, voice, gait, posture, habitual gestures, handwriting and so many other identification cues. As society advanced and the need to secure country borders arose, person identification took on modifications leading to the use of photographic identity cards, documents like passports, certificate of nativity and other government issued documents. Passwords and secret codes were also used in person identification from time immemorial as in [Pilar et al, (2012)].

In most of the conventional methods there was human involvement in the process of authentication which was both a boon and a bane. The human brain is able to process hundreds of unconscious behavioral and physical cues in identifying a person very quickly. The level of accuracy would be dependent on many factors not just the sensory inputs received by the brain as reported by [Markus et al, (2014)] especially when identifying an unfamiliar person. The down side is that in spite of its vast capability, the human brain is prone to pad its perceptions and previous experiences onto the actual sensory inputs to ultimately give either unusually accurate identification or sometimes very skewed and inaccurate results. It is the ambition of data science engineers all over the world to technically simulate the ability of the human brain while eliminating its shortcomings as emphasized in [Bilal et al, (2021)].

Today, security risks arise from more than just human perpetrators. [Monteith et al, (2021)] says that with the global use of computer systems in every walk of life, it is essential to have an understanding of the risks involved to data, resources and persons. It is a need of the times for the security system to be multifaceted to counter multiple avenues of security threats and breaches in order to block attacks and recover with the least amount of damage. Attacks are categorized into four namely program flow control attack, code injection, information disclosure and denial of service to authentic users. Since the pandemic the crime rate in these categories are significantly higher as made explicit in [Rabie et al, (2021)].

A computer system is theoretically secure if it ensures confidentiality, integrity and availability. Even though this assertion is badly in need of review and updating, it is argued by [Lundgren et al, (2019)] that authentication would fall under the purview of confidentiality and integrity. Therefore it is clear that achieving the individual targets of confidentiality, integrity and availability is not a simple one step process. As soon as one type of threat or attack is neutralized, it is seen from experience that clever perpetrators find new ways to counter the prevalent security measure. This has national as well as international implications to the world of cyber security as shown by [Dennis et al, (2021)].

One of the basic methods to ensure a secure system is to allow access to valid users and in addition allow only restricted access to even authorized users. These are similar to the techniques used in the physical world for secure access and is translated into the cyber world as presented in [Arunesh et al, (2015)]. Digital authentication began with plaintext passwords for file access at the MIT for students in the 1960s and quickly progressed to today's encrypted passwords, cryptography and biometric authentication techniques. The evolution of digital authentication is depicted in Fig 1.

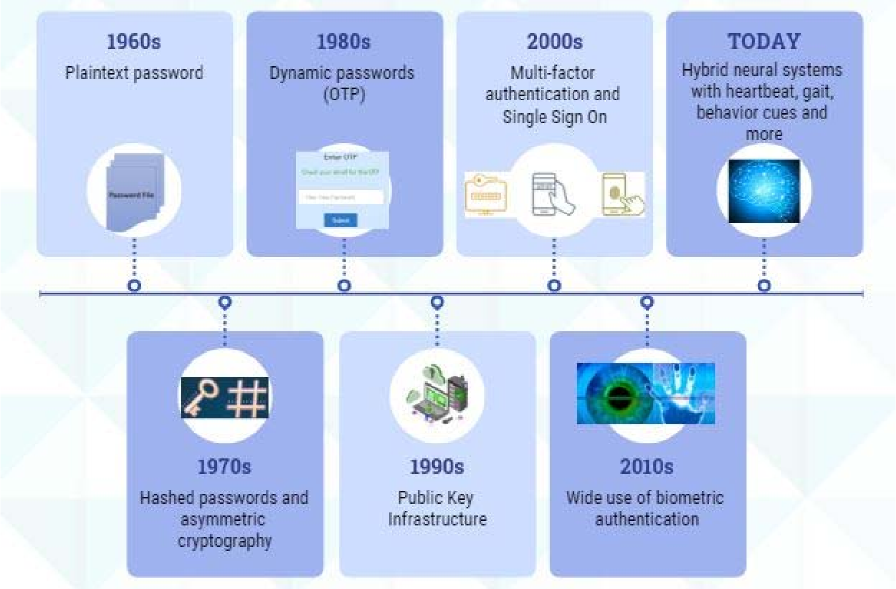

1960s
Plaintext password
Password File
1980s
Dynamic passwords (OTP)
Enter OTP
Submit
2000s
Multi-factor authentication and Single Sign On
TODAY
Hybrid neural systems with heartbeat, gait, behavior cues and more
1970s
Hashed passwords and asymmetric cryptography
1990s
Public Key Infrastructure
2010s
Wide use of biometric authentication

Fig 1. Evolution of Digital Authentication

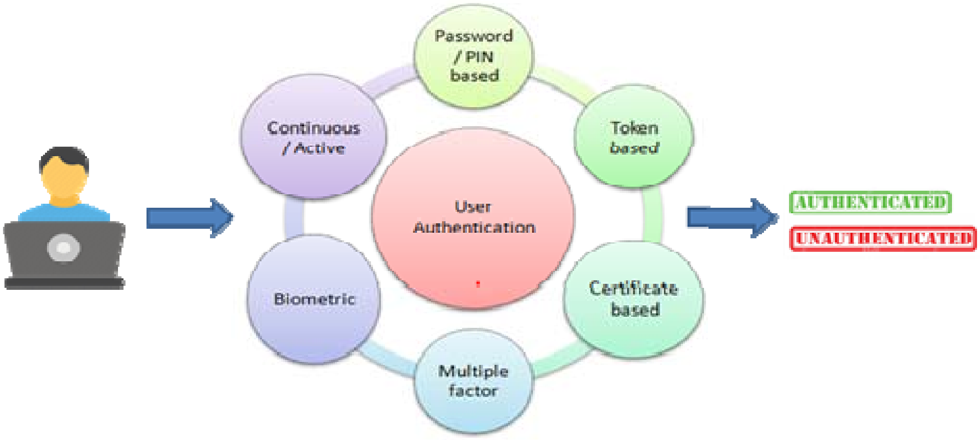


Fig 2. Authentication Process

Today there are several techniques used for user authentication and several more are under research, [Shah et al, (2019)]. User authentication can be broadly put into the something you know, something you have and something you are categories or varied combinations of these three. A general process for user authentication is shown in Fig 2. The userid-password combination falls in the first category. Even though they have several disadvantages it is still the most popular authentication method in use largely due to familiarity and ease of use.

Some of the disadvantages of this method are that in spite of several password rules to create more secure passwords they are still easy to guess and break by hackers largely due to the efficacy of social engineering, key-logging, malware, packet sniffing and so on. Users tend to reuse passwords compounding the problem. When one password is broken, it is likely that several accounts of the user across web services are breached. To add to this, hackers use methods like phishing or pharming techniques to trick users into giving up their password. Personal identification numbers have similar problems to that of the passwords with the difference that it is usually combined with a card or a locker, so this will fall under the second category.

Biometric related authentication fall under the third category which uses physical and behavioral traits for authentication. This method is comparatively new and prone to several vulnerabilities depending on the modality used. It began with physical biometrics like fingerprint, palm print, iris scan, facial recognition, voice recognition and progressed to include behavioral biometrics like voice authentication, keystroke and mouse dynamics. Each of these methods is vulnerable to attacks as pointed out by [Z. Rui et al, (2019)]. These attacks were attempted to be countered by deploying multiple modalities, cryptography and secure protocols. Even with these advancements, user authentication is not adequate. There is scope for improvement in accuracy and computational speed with physical biometrics. In the case of behavioural biometrics, [Casanova et al, (2021)] show that they are considered unreliable and inaccurate opening up the requirement for intensive research in the area.

The major contributions in this work are:

- An efficient active authentication framework with CRNM and face recognition.
- Comparative study of the CRNM fitness functions with CRNM namely Rosenbrock, Rastrigin and Griewank functions.
- Performance comparison of cat optimization variants like ADCSO, AICSO and PCSO.
- Comparisons of state of the art face recognition systems like inferdo, face++, lambda labs API with our proposed model.
- Performance comparison of proposed model with existing frameworks.

The remaining sections of this paper begins with previous works described in section 2, then system architecture in section 3, followed by the details of the proposed model in section 4 and model evaluation results in section 5, ending with section 6 containing concluding remarks and future works.

2. Previous Works

Here, we describe the literature that is currently available on user authentication highlighting the different methods and architectural models used. Since the objective of this paper is fixed on the study of active authentication we have divided the study of related works into existing active authentication models, machine learning methods for active authentication and deep learning models for active authentication. We also present a comparative analysis of these works to bring out the relevance of our study and areas in which current research is deficient.

2.1. *Active authentication systems*

When we think of user authentication what comes to mind is the authentication of a user id and password or methods similar to this which asks the user to authenticate once at the beginning of a session and subsequently the user is declared authentic for the remainder of the session. As pointed out by [Guidorizzi et al, (2013)], the system does not take into account several very plausible scenarios of security breach. The user could have forgotten to log off when leaving his system or user could have temporarily left the system unattended without putting it to sleep. The user could have also used a weak password which is easily guessed, resulting in the account being hacked. The only way to ensure that the user is actually authentic is to have a method that will validate the user at regular intervals of time or continuously. Active authentication is meant to make this possible.

Active authentication has been implemented using several different methods. Initial attempts at active authentication were intrusive and the user had to interrupt his normal work several times in order to self authenticate. This could be done says [Anoud-Bani et al, (2019)], in the form of periodic authentication of user id and password as in online banking. Later, biometric methods like fingerprint scanner as in [Young-Hoo et al, (2016)], facial recognition as described by [Kim et al (2019)], iris scanning presented by [Kenrick et al (2012)]. More recently behavioral biometric methods like keystroke and mouse dynamics as in [Mondal et al, (2016)], voice recognition by [Kim et al, (2010)], gesture recognition presented in [Mondal et al, (2015)] have been added into the mix. Depending on the device used authentication systems have extended to mobile phones as in [Abuhamad et al, (2021)], voice assistants in [Feng et al, (2017)] and many more.

Initially statistical methods were used to analyze the user input at registration time and then create a unique signature in order to authenticate the user in later sessions. This method did not account for the many changes in the signature when a different population or sample was used as shown in [Bzdok et al, (2018)]. This led to the research in machine learning techniques which are able to predict more generalized patterns for a user. The basic architecture of an authentication system based on machine learning algorithms is depicted in Fig 3. The overall process is often modularized into three phases namely training, enrollment and authentication phases. During the training phase all possible patterns are extracted from the input dataset to allow the machine to learn authentic and non authentic patterns. At enrollment, authentic user data is learned and their virtual signature is used to create and store discriminative user patterns which help the authentication system to decide whether a given user is authentic based on the data stored at training and enrollment.

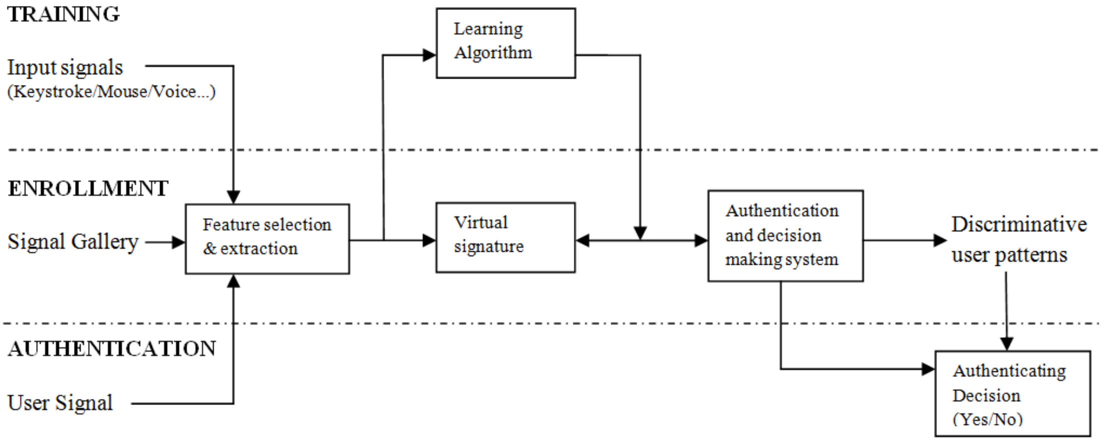

TRAINING
Input signals
(Keystroke/Mouse/Voice...)
Learning Algorithm
ENROLLMENT
Signal Gallery
Feature selection & extraction
Virtual signature
Authentication and decision making system
Discriminative user patterns
AUTHENTICATION
User Signal
Authenticating Decision (Yes/No)

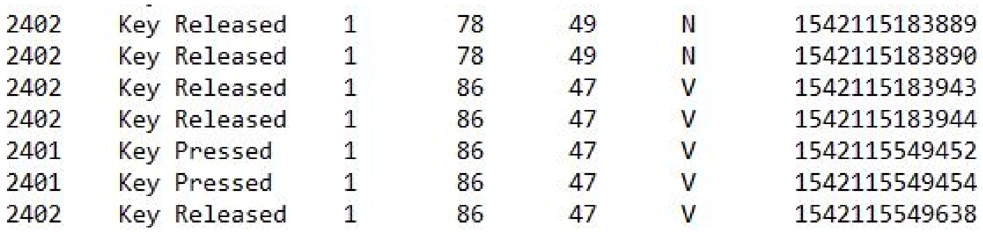
Fig 3. Authentication System Architecture

2.2. *Machine Learning based Active Authentication*

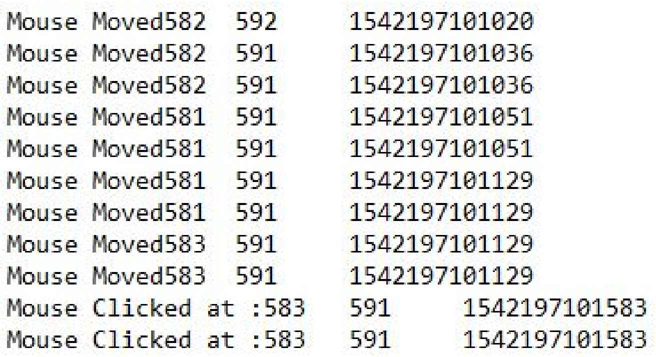
As seen in section 2.1 active authentication can be done using several techniques. Here we narrow the scope by focusing on machine learning techniques used with keystroke and mouse dynamics which is relevant to our proposed model. Detail discussion on different active authentication methods using biometrics is in [Thomas et al, (2021)].

Here we treat keystroke and mouse dynamics as complementary non intrusive biometrics for active user authentication. It is shown by [Earl et al, (2021)] that a combination of keystroke and mouse features lend to better user authentication independent of the machine learning technique used to authenticate the user. Several works has been done using keystroke and mouse data. The raw data gathered on keystroke are shown in Fig 4 the first column is key action code, second column is key action, third column has keyboard area code, fourth column shows key code, fifth column is the virtual keyboard code, sixth column represents the key pressed and the seventh column has time in milliseconds. The raw data on mouse is similarly shown in Fig 5 where each column has < mouse action, x coordinate, y coordinate, time in milliseconds>.

Fig 4. Keystroke Raw Data Sample



```
2402    Key Released    1    78    49    N    1542115183889
2402    Key Released    1    78    49    N    1542115183890
2402    Key Released    1    86    47    V    1542115183943
2402    Key Released    1    86    47    V    1542115183944
2401    Key Pressed     1    86    47    V    1542115549452
2401    Key Pressed     1    86    47    V    1542115549454
2402    Key Released    1    86    47    V    1542115549638
```



```
Mouse Moved582  592     1542197101020
Mouse Moved582  591     1542197101036
Mouse Moved582  591     1542197101036
Mouse Moved581  591     1542197101051
Mouse Moved581  591     1542197101051
Mouse Moved581  591     1542197101129
Mouse Moved581  591     1542197101129
Mouse Moved583  591     1542197101129
Mouse Moved583  591     1542197101129
Mouse Clicked at :583   591     1542197101583
Mouse Clicked at :583   591     1542197101583
```

Fig 5. Mouse Raw Data Sample

The raw data is then subjected to pre-processing and feature extraction. Information that can be derived from keystroke and mouse dynamics include hold time of each key that is pressed, time taken for one key release and a subsequent key press. Timing information of combinations of keys may also be exploited. Similarly timing information of mouse actions and combination of mouse actions can be exploited from mouse dynamics data.

Some of the pioneering work on active authentication using keystroke and mouse was done by [Mondal et al, (2017)]. They describe a trust model that lends itself to multiple biometric modalities. The trust is calculated based on deviation from authentic user behavior learned during enrolment. A penalty and reward system is devised based on the deviation which indicates the trust factor for each user. The model was able to accurately identify authentic users with 94% accuracy and detect unauthentic users with 99.9% accuracy.

The concept of keystroke and mouse dynamics has been extended to application areas like student engagement by [Valdez et al, (2019)] and e-learning by [Fenn et al, (2017)]. The user data is fed into different machine learning algorithms to evaluate classification performance. The former classifies the state of mind of the student with 78% accuracy and the later actively authenticates students using multiple modalities. Several works has been done on active authentication using keystroke dynamics.

[Kim et al, (2018)] improves the performance of keystroke dynamics for active authentication by using the user specific typing behavior for combinations of two keys. The modified feature extraction method improves overall performance by 15.8%. Mouse dynamics was similarly used for active authentication by [Salman et al, (2018)] combining ANN for optimal feature extraction with Gaussian Naive Bayes to achieving 97% accuracy. The improved accuracy is attained by creating a dynamic virtual user signature which assists the classification process. The level of accuracy increases with the availability of data and time. [Yildirim et al, (2021)] uses mouse dynamics to detect insider threats. They tag a user as authentic or non authentic by keeping tabs of legal and non legal mouse sequences. When the numbers of non legal actions have crossed a threshold the user is blocked. They were able to identify insider threats with an accuracy of 96%.

2.3. *Deep Learning based Active Authentication*

Even though most deep learning algorithms are very similar to machine learning algorithms in that they are both used to implement artificial intelligent systems they have some significant differences. All systems that are able to model processes or tasks from their sample data and distinguishing patterns within the sample dataset are essentially machine learning implementations. This eliminates the need to provide explicit instructions that will do the process or task as in conventional programming. Deep learning is a subset of such systems that use artificial neural networks as brought out in [Janiesch et al, (2021)]. Deep learning is made more powerful that the average neural network by simply adding multiple hidden layers to attain better performance and accuracy. In many cases transfer learning is employed to allow for reuse of pre learned networks which is also an added advantage. Convolution operations within deep learning networks allows for raw data to be fed directly into the system skipping the pre processing steps as in machine learning to get a automated representation of the learning task. The basic structure of a deep learning based system is given in Fig 6. The design is comparable to that of an artificial neural network but with many hidden layers. [Rene et al, (2020)] states that a major challenge in deep learning is that the output of deep learning is largely dependent on the amount of training data and its quality. It is generally seen that the system performs better when larger amounts of data are available for the training phase.

There are a number of deep neural networks designed to implement user authentication using behavioral biometrics. Much of the research is devoted to smart phone based active user authentication mostly due to the ease of acquiring sensor data from the user. [Centeno et al, (2017)] uses autoencoders for continuous authentication. It is able to give an EER of 2.2% with a limited number of features collected from an inbuilt 3D accelerometer. The authentication was done by learning motion patterns of users while they were standing and sitting doing activities like reading, writing and browsing on the smart phone. The low dimensionality of the features helps to limit the required computational costs. Comparable results have also been shown with Convolution Neural Networks as presented in [Centeno et al, (2018)]. [Volaka et al, (2019)] uses a combination of user data collected from accelerometer and gyroscope to achieve continuous authentication. The implementation was that of a deep neural network and reported an EER of 15%. [Abuhamad et al, (2020)] adds magnetometer to the mix of sensors achieving an EER of 0.41%. They implement an LSTM based model for the authentication purpose. Gait based authentication as presented in [Zeng et al, (2021)] is also implemented using the smart phone sensor data.

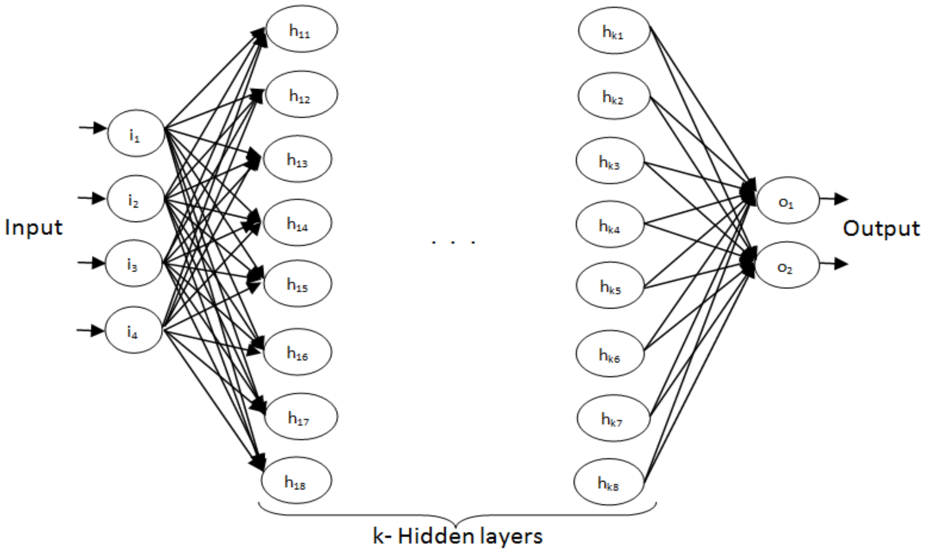


Fig 6. Deep Neural Network

The problem with this method says [Zhu et al, (2020)], is that data from motion sensors very often contain noise which needs to be addressed for accurate authentication. A novel work by [Novak et al, (2020)] uses the URL logs of users to learn the behavior of user browsing pattern for continuous authentication. The implementation uses a combination of autoencoders and CNN. The autoencoder encodes the URL which is then given to the CNN for classification.

Continuous authentication using deep learning with keystroke and mouse dynamics is few compared to authentication using motion sensors. [Aversano et al, (2021)] uses an ensemble classification method with several voting techniques to continuously authenticate users using their typing behavior. The best result that they report is an accuracy of 99.7%. [Yildirim et al, (2021)] uses mouse dynamics to mitigate insider threats by authenticating users. They use ensemble learning and probability aggregation for the authentication decision to implement their system achieving 7.46% EER. A CNN based transfer learning implementation to recognize users with their mouse dynamics data was implemented by [Antal et al, (2020)]. The model is created on a small data set which is later fine tuned by the transfer learning method on a larger dataset achieving an accuracy of 98%.

2.4. *Gap Analysis*

From the above literature review some problems and gaps have come to light namely ineffective user authentication, possibility of malicious attacks, excessive power and energy consumption, inefficient execution time and error rates. These issues are motivation for our proposed model and it is different from the above methodology in that cat swarm optimization is used to optimize the input data from both keystroke and mouse dynamics of a user to achieve active authentication. The optimization not only decrease learning time and get better performance but also helps retain pattern information that is discriminative in nature. This reduces the dimensionality and bulk of the data that needs to be sifted through by the deep neural network for the training process. The classification block blends cat optimization and recurrent neural network to retain the timing dependencies and sequence information in the optimized data. To further improve system performance with regard to false rejection rates, a second layer of authentication is added which is only triggered if the user is classified as unauthentic. This is a novel method and has no precedence in the area of active authentication to the best of our knowledge.

3. System Architecture

Authentication can be either static or dynamic. Since static authentication is done once at entry point they leave the system vulnerable. This is why dynamic authentication is being explored extensively. In static authentication, behavioral authentication is able to combat some of the defects of traditional static authentication namely theft of passwords, social engineering to guess passwords, reuse of single password and many more.
The proposed system is a hybrid model using typing and mouse information along with facial recognition. We discuss problem statement and proposed model architecture in this section. An analysis of cat optimization variants is compared to the performance of our proposed system.

3.1. *Problem Statement*

The need for fast and accurate active authentication is discussed by [Attique et al, (2021)] adding little or no user interaction leads to our proposed system. We provide a novel approach to improve existing accuracy and speed when training and deploying the active authentication system. Our model uses the cat optimization technique as in [Aram et al, (2020)] modified to improve the training time. We use the combined information in keystroke dynamics, mouse dynamics and facial recognition to achieve the desired performance for the system. An efficient active authentication system that is non intrusive based on biometric cues is implemented and results are compared with state of the art frameworks.

3.2. *System Architecture*

Our proposed model has two building blocks. The first is the Cat swarm optimization block and RNN block which takes as input the raw keystroke and mouse user data captured during a session and identifies unique sequences capable of discriminative power for authentication used to determine whether the claimed identity and current user are the same. If the output contradicts the claim then the authentication decision is based on the second block which is the facial recognition module. The optimization contributes to efficient training of the system and the facial recognition decreases the false rejection rate as compared to a system without this module. The advantage of using this method is that it allows for better accuracy without being intrusive. Since the facial recognition only comes into play if there is a contradiction, experiments have shown that the need for block 2 is less than 2% of the time. The proposed architecture is as shown in Fig 7.

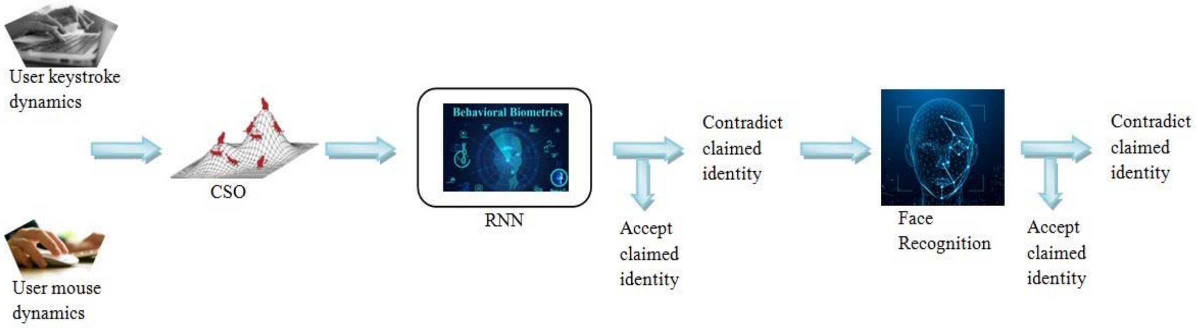


Fig 7. Proposed System Architecture

4. Proposed Model

The proposed system model contains an optimization and authentication block followed by an optional facial recognition block which is only activated in the event of a contradiction on the claimed identity of the user. Here we discuss in detail the working of each of these blocks.

4.1. *Optimization and Authentication block*

The cat swarm optimization (CSO) algorithm was designed by [Chu et al, (2006)]. Studies have shown that CSO gives better performance than most contemporary optimization techniques. It is based on the observation that cats conserve energy with highly efficient utilization on requirement. They observe their environment collecting and analyzing information that allows them to take deliberate actions when needed. The algorithm decides on a number of cats (n) with starting positions (m dimensions), velocity for each dimension (v_i) and a flag indicates either seek or trace mode in which the cat is. The best positions with respect to each cat are stored and the final solution set is chosen from these. The seek mode represents the data collecting and analyzing phase whereas the trace mode depicts a cat moving towards it target. This work is an extension of the CRNM framework presented in [Thomas et al, (2021)]. The steps involved in CRNM are briefly given below. Here we use a fitness function to minimize the distance between claimed identity and current user using their typing and mouse usage information. Termination is reached when the previous best position is same as the current best position or if the difference is negligible. The optimization is applied on the data captured from several sessions in order to get a good representation of user behavior for the training purpose. The variants that we have implemented for comparison are Adaptive Dynamic CSO (ADCSO), Average Inertia weighted CSO (AICSO) and parallel CSO (PCSO). Eq. (1) and Eq. (2) are the inputs to the algorithms. All calculations and necessary parameters are shown in Eq. (3) to Eq. (14).

Input: keystroke information (a_x)and Mouse information (r_x)

$$a_x = \omega(s_v + v_t + a_{x-1} + u_v) \tag{1}$$

Where ω represents trained samples; s_v is time of two consecutive key presses; v_t indicates time of two consecutive key releases; u_v is time of key press of one key and key release of consecutive key; a_{x-1} indicates key action of external users.

$$r_x = \omega(a_s + c_s + r_{x-1} + j_s) \tag{2}$$

Where ω represents trained samples; a_s is mouse action between clicks; c_s is mouse action ending with right click; j_s is no mouse action; r_{x-1} indicates mouse action of external users.

```
Algorithm 1 CSO algorithm
1. Create n cats initialized with random m dimensional positions and corresponding velocities $v_i$.
2. Select cats to be in trace mode and seek mode according to a given ratio such that trace mode is
   (2.5%) very less compared to seek mode.
3. Use position of cats to calculate fitness value ($FS_i$) based on the keystroke and mouse information.
   Save best position. Different fitness functions may be used.
       $FS_i = \frac{|r_x + a_x|}{r_{x\max} - a_{x\min}}$        (3)
4. Run seek mode or trace mode of cats according to their corresponding flags. Refer algorithm 2 and 3.
5. If termination condition is false, repeat steps 2 to 5.
```

```
Algorithm 2 Seek mode
1. Copy present cat position x times based on the target points for that cat. If the current position is a
   target point then x-1 copies are made.
2. For each copy vary dimension as set previously and so that they are within the specified range for the
   cat.
3. Calculate fitness value.
4. If FS values differ then find probability P given that i is within the cat search space. If FS values are
   same then P=1 for each candidate point.
       $P = \frac{|FS_i - FS_{\max}|}{FS_{\max} - FS_{\min}}$        (4)
5. Select next point randomly and replace cat position.
```

```
Algorithm 3 Trace mode
1. Velocity for each dimension is updated, d varies from 1 to m. $cat_{best,d}$ is the best position according
   to fitness function $FS_i$.
       $v_{r_x,a_x} = v_{r_x,a_x} + r_x \times a_x \times (cat_{best,d} - cat_{r_x,a_x})$        (5)
2. If velocities are outside acceptable range then set velocity to maximum limit.
3. Update cat position
       $cat_{r_x,a_x} = cat_{r_x,a_x} + v_{r_x,a_x}$        (6)
```

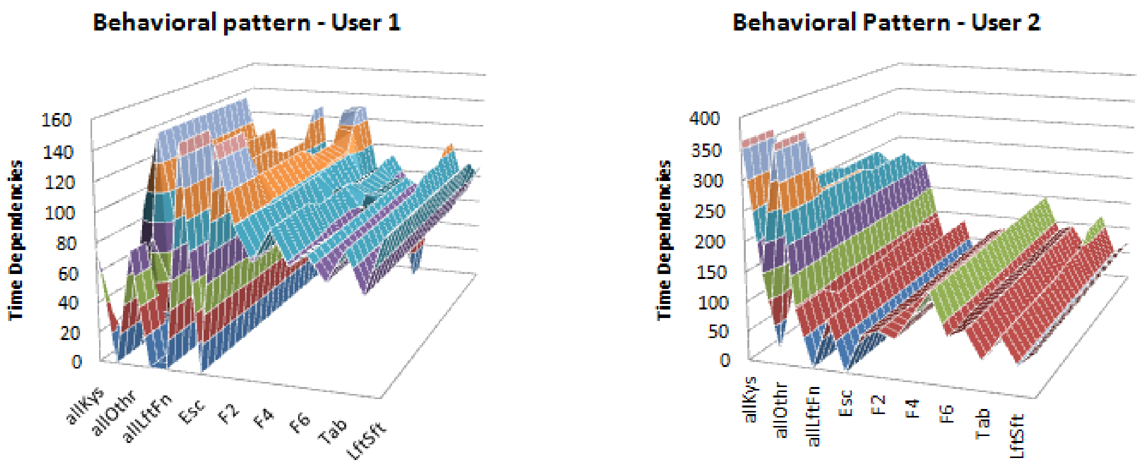
The following are CSO variants that we have tested.

ADCSO Orouskhani (2013)	$w(i) = w_s + \frac{i_{\max} - i}{2i_{\max}}; w_s = 0.5$ $v_{k,d} = w(d)v_{k,d} + r_x a_x (x_{best,d} - x_{k,d})$ $x_{k,d} = \frac{1}{2}[P+V]$ $P = x_{k,d} + \frac{1}{2}(\gamma x_{k,d+1} + (1-\gamma)x_{k,d+2}) + \frac{1}{2}(\gamma x_{k,d-1} + (1-\gamma)x_{k,d-2})$ $V = v_{k,d} + \frac{1}{2}(\gamma v_{k,d+1} + (1-\gamma)v_{k,d+2}) + \frac{1}{2}(\gamma v_{k,d-1} + (1-\gamma)v_{k,d-2})$ $\gamma = 0.6$ (7)
AICSO Orouskhani (2011)	$v_{k,d} = wv_{k,d} + r_x a_x (x_{best,d} - x_{k,d})$ $x_i = \frac{x_i + x_{i-1}}{2} + \frac{v_i + v_{i-1}}{2}$ $w = [0.4,1.0]$ (8)
PCSO Tsai (2008)	$v_{k,d} = v_{k,d} + r_x a_x [x_{best,d} - x_{k,d}]$ $x_{k,d} = x_{k,d} + v_{k,d}$ $ECH = 20$ (9)

Each CSO variant is tested with the modified Rosenbrock, Rastrigin, Griewank functions in addition to our fitness function. The functions are chosen for their suitability in gradient based optimization.

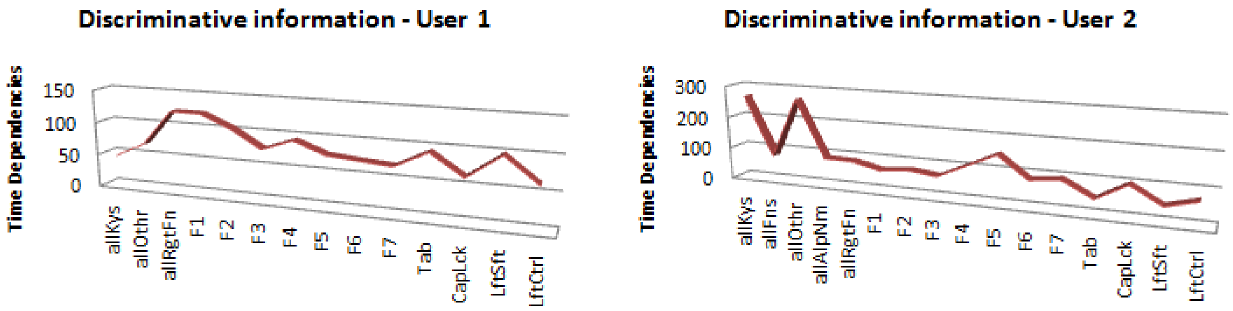
Fitness functions used are given below. Here x_d is taken as r_x+a_x to accommodate both keystroke and mouse information.	
Rosenbrock function	$\sum_{d=1}^{M}[100(x_d - x_{d-1})^2 + (x_{d-1} - 1)^2]$ (10)
Rastrigin function	$\sum_{d=1}^{M}[x_d{}^2 - 10.Cos(2\pi x_d)^2 + 10]$ (11)
Griewank function	$\frac{1}{400}\sum_{d=1}^{M} x_d{}^2 - \prod_{d=1}^{M} Cos(\frac{x_d}{\sqrt{d}}) + 1$ (12)

The input to the CSO module contains timing information about all keystrokes and mouse as shown in Fig 8. The behavioral pattern for each user is distinctive as is evident in the Figure. The CSO algorithm retains the discriminative information while discarding patterns that are non discriminative for a user as represented in Fig 9. This step reduces dimensionality and optimizes computational cost of the overall authentication process.


Behavioral pattern - User 1

Behavioral Pattern - User 2

Fig 8. Behavioural pattern of Users based on time dependencies of keystroke


Discriminative information - User 1

Discriminative information - User 2

Fig 9. CSO Output

The optimized keystroke and mouse data is then authenticated running a recurrent deep neural network to learn user behavior and authenticate the user. Every 3 to 5 seconds the RNN receives the optimized data from the CSO algorithm and then uses this reduced set of data to train the network for authentication. RNN is especially useful with time series datasets and therefore it is used here for the learning process to obtain behavior patterns for keystroke and mouse dynamics of the user. When the system rejects the current user as authentic it then activates the facial recognition block. An image of the user is captured and authenticated again existing user data.

Input to Authentication block k_t (keystroke information), g_t(mouse information)

$$k_t = \omega(a_{k1}a_x + a_{k2}a_{x-1} + p_k) \tag{13}$$

$$g_t = \omega(a_{f1}r_x + a_{f2}r_{x-1} + p_g) \tag{14}$$

Where ω represents trained samples, a_{k1},a_{k2},a_{f1} and a_{f2} represent transition time from input layer to hidden layer and hidden layer to output layer, while p_k ,p_g denotes optimization time.

Algorithm 4: Authentication block

```
1. Initialize $r_x$,$a_x$.
2. Compute $g_t$,$k_t$ input to authentication module.
3. Start seek and trace mode.
4. Calculate fitness using $FS_i$
5. If fitness >= 500 then MATCH else REJECT
6. Compute $v_{r_x,a_x}$ to identify position and output
```

4.2. *Facial recognition block*

The facial recognition model is entered only if there is a contrast in claimed identity and current user after the behavioral authentication phase. This occurs less than 2% of the time but with this secondary authentication the false rejection rates can be brought down significantly. To implement facial recognition we use the modified LBPH (Local Binary Pattern Histogram) algorithm by [Bah et al, (2020)] which gives a 99% accuracy. On authentication, two images of the current user are input to the face recognition module. The images then undergo contrast adjustment, bilateral filter, noise reduction and contrast control, and image histogram equalization. The process enhances the local features and improves feature extraction and comparison. Linear blending with blend fraction β is applied on the output images and then run through the LBPH function for facial recognition. A comparison is made with APIs like inferdo, face++ and lambda labs face recognition. These APIs were named the best facial recognition algorithms in the year 2021.

4.3. *Experiment structure*

The experimentation process implements CRNM with different fitness functions to observe difference in performance on the basis of Precision, Recall, F-measure, FAR, FRR, Error rate and Accuracy. The system is then analyzed for performance enhancement on implementation of the facial recognition methods. A 2:1 ratio of the dataset is used for training and testing. Number of epochs used is 100. We keep authentication by face recognition to a minimum to avoid privacy issues. Experiments are conducted to analyze the performance of our proposed model with different fitness functions, with and without optimization as well as with and without face recognition. In addition we compare the proposed system with variants of CSO and state of the art face recognition APIs.

5. Model evaluation and results

In this section we present the observed results and performance analysis of our proposed model with state of the art technology. The first set of experiments was conducted by modifying the fitness functions of the CRNM framework to study its effect on performance. Table 1 gives the authentication accuracy of the CRNM model compared with the Rosenbrock, Rastrigin, Griewank and CRNM fitness functions. As can be seen in Fig 10, since our dataset has multiple global and local maxima and minima we can see that the best suited fitness functions are those which cater to this characteristic of the data pattern. Here the CRNM fitness function has highest accuracy. We also observe that as the number of stored data increases it becomes increasingly more difficult to identify discriminative features for a single user.

No. of Stored data	Accuracy (%)			
	Rosenbrock	Rastrigin	Griewank	CRNM
100	85	85.3	93.28	**98.25**
300	84.89	85	91.75	**97.8**
500	82.66	82.78	91.22	**96**
700	81.03	81.27	90.16	**93**
1000	80.58	80.88	89.45	**90.22**

Table 1. Accuracy based on fitness function

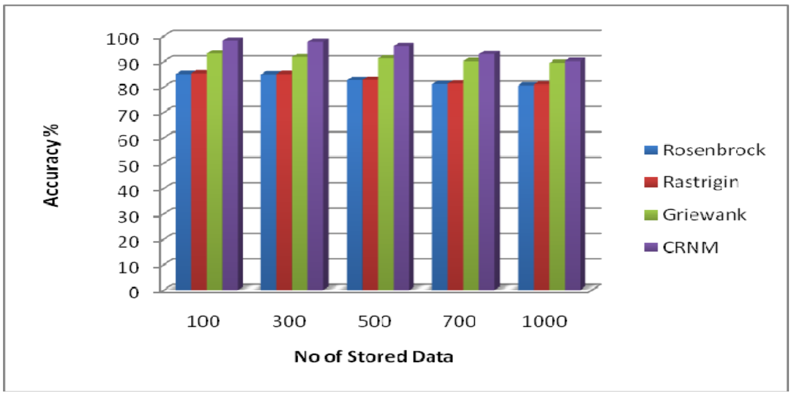


Fig 10. Fitness function based authentication accuracy

The CRNM framework was modified to accommodate different CSO variants. We now present the results and observations of these experiments. The performance of CSO variants are presented in Table 2. As can be inferred from Fig 11, the best results are obtained with the ADCSO variant and PCSO variants shows lower results since it tends to perform better with fewer iterations and lesser population size

CRNM variants	Precision	Recall	FAR	FRR	Error rate	Accuracy
CSO	98.5	98.45	0.01	1.5	0.1	98.25
ADCSO	98.75	98.78	0.01	1.43	0.09	98.78
AICSO	98.17	98.09	0.019	1.45	0.13	98.26
PCSO	95.3	93.23	0.5	2.12	1.25	94

Table 2. Performance analysis of CSO variants on the CRNM framework

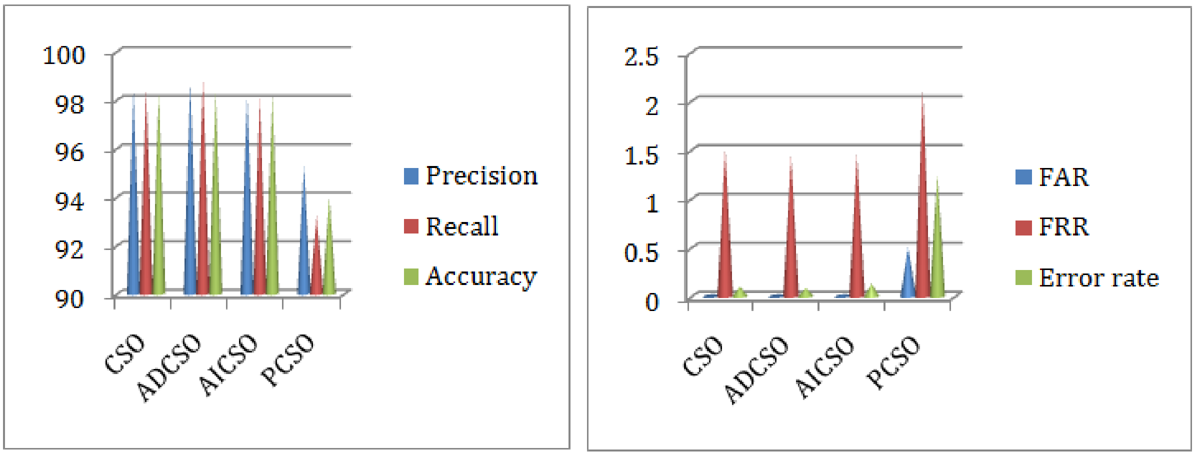


Fig 11. Performance comparison of CSO variants

We now present the results observed when facial recognition is added to control the false rejection rates. Table 3. Shows the results of our facial recognition being added to the CRNM framework and as can be seen in Fig 12. the framework does benefit from the addition of this physical biometric. In addition it has significantly decreased the FRR when compared to the original CRNM framework.

Performance Measures	**RNN without CAT (%)**	**CRNM (%)**	**CRNM +face recognition (%) (proposed system)**
Accuracy	85.11	97.85	98.29
F-measure	93.01	98.31	99.53
False Acceptance Rate (FAR)	0.95	0.01	0.01
False Rejection Rate (FRR)	2.5	1.92	1.02

Table 1. Performance Comparison of CRNM + face recognition

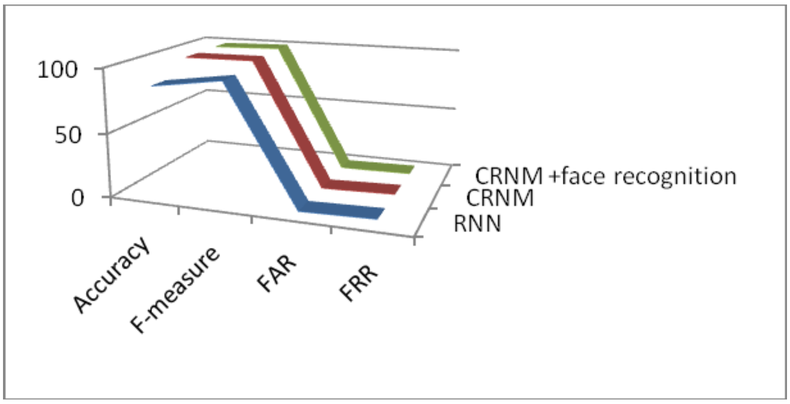


Fig 12. CRNM + face recognition performance comparison

Finally we make a comparison between results obtained by varying the facial recognition algorithm on the CRNM ICSO variant in Table 4. We present the results in Fig 13. based on improvement in FRR and Accuracy as this module is activated on rejection of a claimed identity. Inferdo API gives best results compared to the other face recognition algorithms but all of the methods used are comparable in their high performance.

Face recognition API	FRR	Accuracy
LBPH	1.02	98.29
Inferdo	0.09	98.76
face++	1.03	98.25
lambda labs	1.03	98.26

Table 4. Performance of Face recognition APIs with CRNM

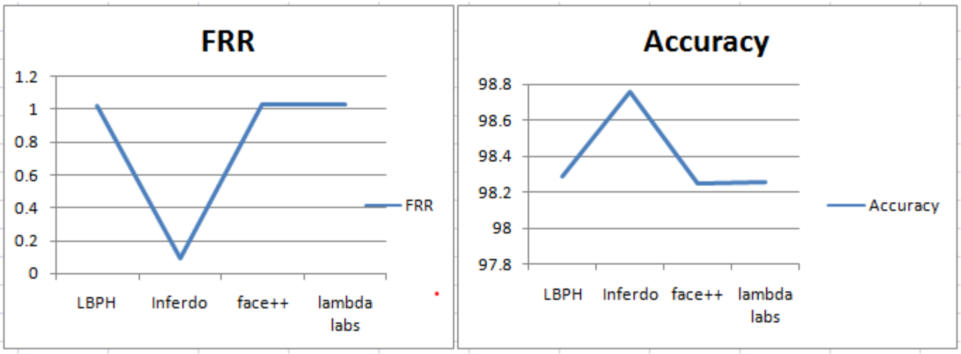


Fig 13. Performance comparison of state of the art face recognition APIs with CRNM

Finally it was observed that the amount of training time differed based on the number of epochs that were set for the model. Fig 14. shows the variations in time required based on the time and amount of training samples used was 100 in each case. As can be seen increasing the number of epochs does not necessarily decrease loss. Here least loss is observed at 85 epochs. The overall time taken for the system to authenticate a claimed identity was around 3 minutes to get the performance that is reported here.

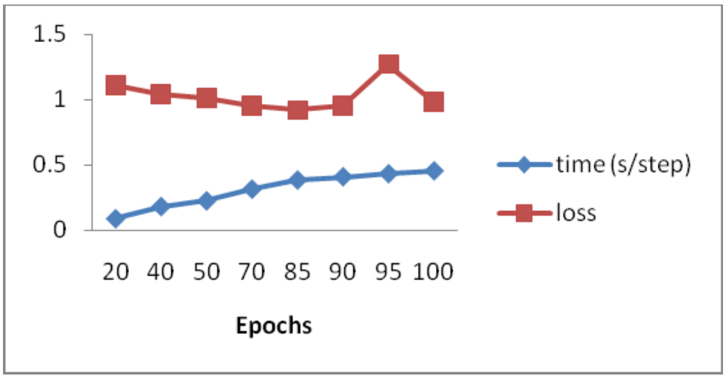


Fig 14. No of Epochs Vs Time and loss

6. Conclusion

We implement variations on our CRNM model with face recognition. The cat optimization contributes to decreasing the learning time and faster authentication. In order for an authentication system to be commercially viable it should have low amounts of FAR and FRR. Security works on the concept that even if an authentic user is rejected and unauthentic user should not be allowed access to protected data or resources. Due to this reason many of our designs have very low FAR but not so low FRR. There is always a give and take between FAR and FRR. If we are interested in keeping intruders out then our focus is on FAR. But with authentication we are interested in both FAR and FRR. This work is a step towards the objective of achieving lower FAR and FRR as much as possible without giving up on security. The results show that our proposed model outperforms other models.

In the future we are interested in broadening this study by comparing different optimization techniques and using a combination of behavioral and physical biometrics. The impact on performance can also be studied using different available datasets to provide insight into whether or not the features chosen can interfere or enhance active authentication. Another possible avenue of research is to broaden the concept to different application areas like banking, education and medical services.

Conflicts of Interest

The authors have no conflicts of interest to declare.

References

[1] Abuhamad M, T. Abuhmed, D. Mohaisen and D. Nyang, "AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors," in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5008-5020, June 2020, doi: 10.1109/JIOT.2020.2975779.

[2] Abuhamad M., A. Abusnaina, D. Nyang and D. Mohaisen, "Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey," in IEEE Internet of Things Journal, vol. 8, no. 1, pp. 65-84, 1 Jan.1, 2021, doi: 10.1109/JIOT.2020.3020076.

[3] Anoud Bani-Hani, Munir Majdalweieh, Aisha AlShamsi, Online Authentication Methods Used in Banks and Attacks Against These Methods, Procedia Computer Science, Volume 151, 2019, Pages 1052-1059, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2019.04.149. (https://www.sciencedirect.com/science/article/pii/S1877050919306167)

[4] Antal, Margit & FejÃ©r, Norbert. (2020). Mouse dynamics based user recognition using deep learning. Acta Universitatis Sapientiae, Informatica. 12. 39-50. 10.2478/ausi-2020-0003.

[5] Aram M. Ahmed, Tarik A. Rashid, Soran Ab. M. Saeed, "Cat Swarm Optimization Algorithm: A Survey and Performance Evaluation", Computational Intelligence and Neuroscience, vol. 2020, Article ID 4854895, 20 pages, 2020. https://doi.org/10.1155/2020/4854895

[6] Arunesh Sinha, Thanh H. Nguyen, Debarun Kar, Matthew Brown, Milind Tambe, Albert Xin Jiang, From physical security to cybersecurity, Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 19–35, https://doi.org/10.1093/cybsec/tyv007

[7] Attique Ur Rehman, Tek Tjing Lie, Brice VallÃ¨s, Shafiqur Rahman Tito, Non-invasive load-shed authentication model for demand response applications assisted by event-based non-intrusive load monitoring, Energy and AI, Volume 3, 2021, 100055, ISSN 2666-5468, https://doi.org/10.1016/j.egyai.2021.100055.

[8] Aversano L, Bernardi ML, Cimitile M, Pecori R. 2021. Continuous authentication using deep neural networks ensemble on keystroke dynamics. PeerJ Computer Science 7:e525 https://doi.org/10.7717/peerj-cs.525

[9] Bah Serign Modou, Fang Ming, An improved face recognition algorithm and its application in attendance management system, Array, Volume 5, 2020, 100014, ISSN 2590-0056, https://doi.org/10.1016/j.array.2019.100014.

[10] Barton JJS, Corrow SL. Recognizing and identifying people: A neuropsychological review. Cortex. 2016;75:132-150. doi:10.1016/j.cortex.2015.11.023

[11] Bilal Alhayani, Husam Jasim Mohammed, Ibrahim Zeghaiton Chaloob, Jehan Saleh Ahmed, Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry, Materials Today: Proceedings, 2021

[12] Bzdok, D., Altman, N. & Krzywinski, M. Statistics versus machine learning. Nat Methods 15, 233–234 (2018). https://doi.org/10.1038/nmeth.4642

[13] Casanova A, Lucia Cascone, Aniello Castiglione, Weizhi Meng, Chiara Pero, User recognition based on periocular biometrics and touch dynamics, Pattern Recognition Letters, Volume 148, 2021, Pages 114-120, ISSN 0167-8655, https://doi.org/10.1016/j.patrec.2021.05.006.

[14] Centeno M P, Yu Guan, and Aad van Moorsel. 2018. Mobile Based Continuous Authentication Using Deep Features. In Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning (EMDL'18). Association for Computing Machinery, New York, NY, USA, 19–24. DOI:https://doi.org/10.1145/3212725.3212732

[15] Centeno M. P., A. v. Moorsel and S. Castruccio, "Smartphone Continuous Authentication Using Deep Learning Autoencoders," 2017 15th Annual Conference on Privacy, Security and Trust (PST), 2017, pp. 147-1478, doi: 10.1109/PST.2017.00026.

[16] Chu SC., Tsai P., Pan JS. (2006) Cat Swarm Optimization. In: Yang Q., Webb G. (eds) PRICAI 2006: Trends in Artificial Intelligence. PRICAI 2006. Lecture Notes in Computer Science, vol 4099. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-36668-3_94

[17] Dennis Broeders, Fabio Cristiano & Daan Weggemans (2021) Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2021.1928887

[18] Earl S., Campbell J., Buckley O. (2021) Identifying Soft Biometric Features from a Combination of Keystroke and Mouse Dynamics. In: Zallio M., Raymundo Ibañez C., Hernandez J.H. (eds) Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity. AHFE 2021. Lecture Notes in Networks and Systems, vol 268. Springer, Cham. https://doi.org/10.1007/978-3-030-79997-7_23

[19] Feng H, Kassem Fawaz, and Kang G. Shin. 2017. Continuous Authentication for Voice Assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom '17). Association for Computing Machinery, New York, NY, USA, 343–355. DOI:https://doi.org/10.1145/3117811.3117823

[20] Fenu, G., Marras, M., & Boratto, L. (2017). A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognition Letters. doi:10.1016/j.patrec.2017.03.027

[21] Guidorizzi, Richard. (2013). Security: Active Authentication. IT Professional. 15. 4-7. 10.1109/MITP.2013.73.

[22] Janiesch, C., Zschech, P. & Heinrich, K. Machine learning and deep learning. Electron Markets (2021). https://doi.org/10.1007/s12525-021-00475-2

[23] Kenrick Mock, Bogdan Hoanca, Justin Weaver, and Mikal Milton. 2012. Real-time continuous iris recognition for authentication using an eye tracker. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). Association for Computing Machinery, New York, NY, USA, 1007–1009. DOI:https://doi.org/10.1145/2382196.2382307

[24] Kim D., K. Chung and K. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," in IEEE Transactions on Consumer Electronics, vol. 56, no. 4, pp. 2678-2685, November 2010, doi: 10.1109/TCE.2010.5681156.

[25] Kim S. T. and Y. M. Ro, "Attended Relation Feature Representation of Facial Dynamics for Facial Authentication," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1768-1778, July 2019, doi: 10.1109/TIFS.2018.2885276.

[26] Kim, J., Kim, H., & Kang, P. (2018). Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. Applied Soft Computing, 62, 1077–1087. doi:10.1016/j.asoc.2017.09.045

[27] Lundgren B, Möller N. Defining Information Security. Sci Eng Ethics. 2019;25(2):419-441. doi:10.1007/s11948-017-9992-1

[28] Markus Bindemann, Janice Attard & Robert A. Johnston | Peter Walla (Reviewing Editor) (2014) Perceived ability and actual recognition accuracy for unfamiliar and famous faces, Cogent Psychology, 1:1, DOI: 10.1080/23311908.2014.986903

[29] Mondal S. and Bours P., "Swipe gesture based Continuous Authentication for mobile devices," 2015 International Conference on Biometrics (ICB), 2015, pp. 458-465, doi: 10.1109/ICB.2015.7139110.

[30] Mondal, S., & Bours, P. (2017). A study on continuous authentication using a combination of keystroke and mouse biometrics. Neurocomputing, 230, 1–22. doi:10.1016/j.neucom.2016.11.031

[31] Monteith, S., Bauer, M., Alda, M. et al. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Curr Psychiatry Rep 23, 18 (2021). https://doi.org/10.1007/s11920-021-01228-w

[32] Nowak J., Holotyak T., Korytkowski M., Scherer R., Voloshynovskiy S. (2020) Fingerprinting of URL Logs: Continuous User Authentication from Behavioural Patterns. In: Krzhizhanovskaya V.V. et al. (eds) Computational Science – ICCS 2020. ICCS 2020. Lecture Notes in Computer Science, vol 12140. Springer, Cham. https://doi.org/10.1007/978-3-030-50423-6_14

[33] Orouskhani, Maysam & Manthouri, Mohammad & Teshnehlab, Mohammad. (2011). Average-Inertia Weighted Cat Swarm Optimization. 321-328. 10.1007/978-3-642-21515-5_38.

[34] Orouskhani, Maysam & Orouskhani, Yasin & Manthouri, Mohammad & Teshnehlab, Mohammad. (2013). A Novel Cat Swarm Optimization Algorithm for Unconstrained Optimization Problems. International Journal of Information Technology and Computer Science. 5. 32-41. 10.5815/ijitcs.2013.11.04.

[35] Pilar DR, Jaeger A, Gomes CFA, Stein LM (2012) Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. PLoS ONE 7(12): e51067. https://doi.org/10.1371/journal.pone.0051067

[36] Rabie A. Ramadan, Bassam W. Aboshosha, Jalawi Sulaiman Alshudukhi, Abdullah J. Alzahrani, Ayman El-Sayed, Mohamed M. Dessouky, "Cybersecurity and Countermeasures at the Time of Pandemic", Journal of Advanced Transportation, vol. 2021, Article ID 6627264, 19 pages, 2021. https://doi.org/10.1155/2021/6627264

[37] Rene Y. Choi, Aaron S. Coyner, Jayashree Kalpathy-Cramer, Michael F. Chiang, J. Peter Campbell; Introduction to Machine Learning, Neural Networks, and Deep Learning. Trans. Vis. Sci. Tech. 2020;9(2):14. doi: https://doi.org/10.1167/tvst.9.2.14.

[38] S. Mondal and P. Bours, "Combining keystroke and mouse dynamics for continuous user authentication and identification," 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), 2016, pp. 1-8, doi: 10.1109/ISBA.2016.7477228.

[39] Salman, O. A., & Hameed, S. M. (2018). Using Mouse Dynamics for Continuous User Authentication. Advances in Intelligent Systems and Computing, 776–787. doi:10.1007/978-3-030-02686-8_58

[40] Shah, Syed & Kanhere, Salil. (2019). Recent Trends in User Authentication - A Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2932400.

[41] Thomas, P.A., Mathew, K.P. An Efficient Optimized Mouse and Keystroke Dynamics Framework for Continuous Non-Intrusive User Authentication.Wireless PersCommun(2021). https://doi.org/10.1007/s11277-021-09363-6

[42] Thomas, P.A., Preetha Mathew, K. A broad review on non-intrusive active user authentication in biometrics. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-021-03301-x

[43] Tsai, Pei-Wei & Pan, Jeng-Shyang & Chen, Shyi-Ming & Liao, Bin-Yih & Hao, Szu-Ping. (2008). Parallel Cat Swarm Optimization. 3328 - 3333. 10.1109/ICMLC.2008.4620980.

[44] Valdez, M. G., Merelo, J.-J., Aguila, A. H., & Soto, A. M. (2019). Mining of Keystroke and Mouse Dynamics to Increase the Engagement of Students with Programming Assignments. Computational Intelligence, 41–61. doi:10.1007/978-3-030-16469-0_3

[45] Volaka Hasan Can, Gulfem Alptekin, Okan Engin Basar, Mustafa Isbilen, Ozlem Durmaz Incel, Towards Continuous Authentication on Mobile Phones using Deep Learning Models, Procedia Computer Science, Volume 155, 2019, Pages 177-184, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2019.08.027.

[46] Yildirim, M., & Anarim, E. (2021). Mitigating insider threat by profiling users based on mouse usage pattern: ensemble learning and frequency domain analysis. International Journal of Information Security. doi:10.1007/s10207-021-00544-9

[47] Yildirim, M., Anarim, E. Mitigating insider threat by profiling users based on mouse usage pattern: ensemble learning and frequency domain analysis. Int. J. Inf. Secur. (2021). https://doi.org/10.1007/s10207-021-00544-9

[48] Young-Hoo Jo, Seong-Yun Jeon, Jong-Hyuk Im, Mun-Kyu Lee, "Security Analysis and Improvement of Fingerprint Authentication for Smartphones", Mobile Information Systems, vol. 2016, Article ID 8973828, 11 pages, 2016. https://doi.org/10.1155/2016/8973828

[49] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," in IEEE Access, vol. 7, pp. 5994-6009, 2019, doi: 10.1109/ACCESS.2018.2889996.

[50] Zeng X, Zhang X, Yang S, Shi Z, Chi C. Gait-Based Implicit Authentication Using Edge Computing and Deep Learning for Mobile Devices. Sensors. 2021; 21(13):4592. https://doi.org/10.3390/s21134592

[51] Zhu, T.; Weng, Z.; Chen, G.; Fu, L. A Hybrid Deep Learning System for Real-World Mobile User Authentication Using Motion Sensors. Sensors 2020, 20, 3876. https://doi.org/10.3390/s20143876

Authors Profile

Princy Ann Thomas has obtained MTech in Cyber Security with the first rank from Mahatma Gandhi University, Kottayam, Kerala, India. Currently, she is an Associate Professor at Government Engineering College Idukki and joined Government service in September 2000. She is also working towards her Ph.D. at Cochin University College of Engineering Kuttanadu. Her research interests include Cyber Security, Machine Learning, and Data Mining.

Dr. Preetha Mathew K has received her Ph.D. from the Indian Institute of Technology, Madras. Her areas of interest are Cryptography and Network Security. She has around 30 years of teaching experience and is currently a Professor in Computer Science and Engineering, Cochin University College of Engineering Kuttanadu, Kerala.