An Adaptive Approach for Active Multi-Factor Authentication

Abhijit Kumar Nag and Dipankar Dasgupta
Department of Computer Science
The University of Memphis
Memphis, TN, USA
\{aknag, dasgupta\}@memphis.edu

Kalyanmoy Deb
Department of Electrical and Computer Engineering
Michigan State University
Lansing, MI, USA
kdeb@egr.msu.edu

Abstract—Multi-Factor Authentication (MFA) is the current trend to genuinely identify authorized users through the active authentication process using passwords, biometrics, cognitive behavior, etc. As new and improved authentication modalities of various types are becoming available, these are opening up options for security researchers to devise solutions facilitating continuous authentication to online systems. This paper focuses on describing a framework for continuous authentication where authentication modalities are selected adaptively by sensing the users’ operating environment (the device and communication media, and historical data). Empirical studies are conducted with varying environmental parameters and the performance of the adaptive MFA is compared with other selection strategies. The empirical results appear promising, which reflects that such a multi-factor decision support technique can be applied to real-world identity management and authentication systems.

Keywords—Active Authentication; Genetic Algorithm; Adaptive Selection; Multi-Modal Framework

I. INTRODUCTION

The challenging issue of today’s authentication system is to correctly identify the legitimate users at different operating environments in a robust and efficient way. With the growth of user-friendly devices and the availability of the Internet, people are now accessing their personal, social, financial, and business information from everywhere (their home, working place, and public places). This versatility of the environment in providing access to cyber information, requires highly secure design of user authentication systems. Most authentication systems today validate the user’s identity only during the login time, and no further verification of identity is required during the session while using the same device. The authentication system should be able to work in a robust and adaptive way in different environments. In the case of multi-factor authentication, the factors can be chosen in different ways. For instance, using static policy, all the factors and their corresponding actions are predefined. With the dynamic policy, these factors may change dynamically based on different time-triggering events. Moreover, dynamic policy can be of two types: random and adaptive. Random policy does not take into account the operating environment, constraints, and past history of users’ authentication. On the other hand, the adaptive policy is a guided random search which incorporates realities and alleviates the shortcomings of the random search. People prefer to use a new device/technology for easy access of online information. As a result, the user authentication strategy needed to be adaptive to allow secure access using both active and passive continuous authentication modalities of different operating environments (such as devices and media).

In today’s authentication systems, the username and password are typically used along with some security questions to identify valid users. For instance, to access a bank account from desktop, laptop, or handheld devices, the same id is typically required for the authentication process. But this authentication process does not consider any environment factors like types of network connection (wired, wireless or public hotspot) and history. This single identity approach is at the risk of theft because of using devices in less trustworthy environment.

In this paper, an approach for adaptive selection of authentication modalities (and their specific features with different parameter settings) is described. The details of the approach and the simulation of adaptive selection at different triggering events are described in the following sections.

II. BACKGROUND AND RELATED WORKS

A number of different modalities are available for authentication systems. The noteworthy modalities are face recognition, fingerprint recognition, password, CAPTCHA, voice recognition and verification code through SMS. Specifically, face recognition [1], [2] is used for authentication in portable devices and handheld devices. For example, skin color based technique [2] is used for detecting frontal human face from the input image. The visual features, namely Profile Fourier Coefficients, are then extracted using template matching. Face recognition method is also used to combat terrorism in the congested public areas, like airports and nations border crossing points [3]. It uses principal component analysis to get the required features. The fingerprint is another biometric modality [4], where improved minutiae extraction algorithm is used to get the essential differentiable features. Sometimes in embedded systems, a fingerprint method is used to increase the security of authentication [5]. But this modality is computationally expensive compared to other existing biometric modalities. There are some reported works in [26], [27], [28] of continuous biometric authentication using only
face and fingerprint. These works show the adoption of multiple modality based authentication decision in contrast with traditional single modality based authentication. But they do not address the effect of environment settings (which device and media the person uses for authentication) and trustworthy of using the selected modalities for a given environment. Voice recognition is also being used modality for authentication to do the recognition task, different levels of features are extracted for pronouncing vowels and consonants like spectral characteristics, duration, sequence of occurrence etc. The overall accuracy of authentication can be quite high when results from many individual measurements are combined. But voice recognition lacks the robustness in a noisy environment or public gathering.

The above mentioned modalities are user interceptive. As the usage of mobile computing devices is increasing, user non-interceptive modalities are becoming available for continuous authentication. Two good examples of such modalities are keystroke analysis [8] and mouse dynamics [9]. Keystroke analysis can be done using the keyboard of the device where the biometric analysis has to be performed. This method performs quite well to authenticate legal users and to reject impostors. The user non-interceptive biometrics support the remote access scenarios that are helpful for some cases such as off-site office location access. But as they are not active modalities, their performance is not as high as the interceptive modalities. Hence, while choosing the modalities for adaptive selection, both user interceptive and non-interceptive modalities are chosen for flexibility, robustness, and ensuring the efficient authentication process.

The two-factor authentication is already adopted by software companies such as Amazon, Google, Yahoo, Dropbox, Facebook, LinkedIn, Twitter, Microsoft, and many others. Microsoft’s Windows Azure Active Directory 1 uses multi-factor authentication for their cloud applications with one-time password, automated phone call and text message. However, this approach is static and does not consider different characteristics, duration, sequence of occurrence etc. The overall accuracy of authentication can be quite high when results from many individual measurements are combined. But voice recognition lacks the robustness in a noisy environment or public gathering.

The above mentioned modalities are user interceptive. As the usage of mobile computing devices is increasing, user non-interceptive modalities are becoming available for continuous authentication. Two good examples of such modalities are keystroke analysis [8] and mouse dynamics [9]. Keystroke analysis can be done using the keyboard of the device where the biometric analysis has to be performed. This method performs quite well to authenticate legal users and to reject impostors. The user non-interceptive biometrics support the remote access scenarios that are helpful for some cases such as off-site office location access. But as they are not active modalities, their performance is not as high as the interceptive modalities. Hence, while choosing the modalities for adaptive selection, both user interceptive and non-interceptive modalities are chosen for flexibility, robustness, and ensuring the efficient authentication process.

The two-factor authentication is already adopted by software companies such as Amazon, Google, Yahoo, Dropbox, Facebook, LinkedIn, Twitter, Microsoft, and many others. Microsoft’s Windows Azure Active Directory 1 uses multi-factor authentication for their cloud applications with one-time password, automated phone call and text message. However, this approach is static and does not consider different user roles, environmental factors, and type of devices and media used while choosing the different modalities. Our proposed approach takes the environmental factors (different devices and media) into consideration to decide the active authentication process which appears to be best suited for accessing sensitive cyber systems.

For designing adaptive MFA, we considered Genetic Algorithm (GA) [20], which is widely used for search and optimization to find near optimal solutions in real-world applications where search space is large and not well-defined.

III. ACTIVE AUTHENTICATION

Active Authentication (AA) is considered as a continuous protection against all kinds of illegal access and use of computing systems [10]. However, AA requires continuous monitoring of user activities (at some levels) for re-authentication. To address the ongoing threat and breaches of authentication systems, the security research community is moving towards an open solution which can expedite continual authentication to the existing computing devices. In general, user authenticity can be challenged in ways such as: what the user knows (password or pin), what the user has (smart card or digital certificate), who the user is (fingerprint, iris scan, or voice recognition), and where the user is (GPS or IP address of the machine). In current practice, two or more of these forms are combined for doing a secure authentication process.

The goal of active multi-factor authentication is to create a robust access verification process to make it harder for an unauthorized person to access a computer system. Recent DARPA programs on Active Authentication [10] also focus on the development of several different modalities (including behavioral and cognitive modalities) for authentication. One of the projects, Stylometry, [11] uses a stylometric method to validate the authentic users (while they are typing). In another project [12], [13], web browsing behavior is used to identify legitimate users by capturing the semantic behavior of the users. This process uses both semantic and syntactic session features to perform the identification. Research shows that Screen Fingerprint [14] can authenticate users based on computer screen recording and extracting discriminative visual features from that recording. In the case of passive authentication modalities, the authors [15] provide a behavioral biometric verification to identify students in online courses. Also, several studies demonstrated that the use of keyboard and mouse dynamics provide some significant improvement of user authentication in a passive way [16], [17]. As these technologies are available for computing devices, the applicability of multi-factor authentication using these sensors will increase significantly.

IV. USE OF AUTHENTICATION MODALITIES

In our current implementation, seven common authentication modalities with their features, are considered. The modalities include face, fingerprint, password, CAPTCHA, SMS, voice, and keystroke. Some of these modalities need user intervention (active modality) while others are passive modalities and do not require any user intervention.

Using these authentication modalities, we designed an active multi-factor authentication framework where each of these modalities (the features and the computation logic) is stored in a server and a user is authenticated with different modalities which are decided by the genetic search. The high-level architecture of our proposed active multi-factor authentication system is shown in Fig. 1. Here different modality calculations are stored in different virtual machines (VMs) and query and retrieval of modalities are done from the user console to the authentication server. The benefits of using VMs for storing the modalities are significant as they are logically separated and run independently. Also if any of the VMs are compromised, the decision-support algorithm will still able to select from the rest of non-compromised modalities.

While choosing the modalities, both biometric and non-biometric modalities are considered. Although the biometric modality has uniqueness as its feature, it also suffers some drawbacks for which it is not good to design an active authentication system based on only biometrics. False reading sometimes occurs among biometrics. This type of vulnerability (false acceptance rate and false reject rate) is the greatest disadvantage. Recently, the fingerprints are forged through copying and even this can be altered by transplant surgery [18]. The facial features are also changed through plastic surgery [18] and these methods are adopted by the bad guys around the world to bypass the security system. Moreover, an effective biometric system is costly in nature and cannot be afforded by small or medium-sized companies for deploying the continuous authentication system in large scale. Biometric modalities like voice recognition or iris recognition are not reliable in case of illness. If a user suffers from throat infection or eye disease, these modalities cannot serve the authentication purpose if they are the only metric used for authentication. Again, in many companies or institutions, the employees work from remote station to login to their workstation. In this scenario, biometric authentication has no luck. Passwords, PIN code, passive authentication such as keystroke, and mouse movement are the good choice for this scenario. Therefore, to build a robust and resilient active authentication system, both biometric and non-biometric modalities are incorporated and the balances of these modalities in selection are ensured through designing the objective functions.

An active multi-factor authentication is likely to be very essential in the near future for all computing environment. Due to the recent trend of identity theft (64.1% in misuse of existing credit card, 35% in misuse of existing bank account) [19], it is not a viable option to authenticate a user for a service, such as accessing a bank account, using only a fixed modality (example: username and password) for different types of environment settings. The design of the authentication framework and the accuracy and feasibility of the existing modalities are not the scope of this work. It is assumed that these modalities are enrolled successfully in the existing system and are available to use in the discussed environments.

V. ADAPTIVE SELECTION OF MODALITIES

In this work, we used Genetic Algorithm (GA) for adaptive selection of modalities and their corresponding features during the active authentication process. Specifically, NSGA-II [23] is used, which is an efficient strategy for solving multi-objective problems using GAs.

Table I illustrates different level of features for each modality. For Fingerprint (M2), the features are categorized in three levels. Accordingly, the GA based selection process will choose features from each of the levels based on its fitness value. This two level encoding (modality space and feature space) provides an adaptive and robust selection for the active authentication system.

There are different products available for doing biometric and passive modality authentication. For instance, KeyLemon2 (facial recognition), Digital Persona3 (fingerprint), Spector Soft Pro4 (keystroke), and Nuance5 (voice recognition). These applications can easily be integrated into the existing systems (fixed and portable devices) to support the proposed active authentication framework.

<table>
<thead>
<tr>
<th>Modality</th>
<th>Computational Features</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face (M1)</td>
<td>Lip: Lip center position(xc, yc), the lip shape (h1, h2 and w), lip orientation (θ)</td>
<td>Lip: L1, L2 and L3. Eye: L4, L5. Brow and Check: L6, L7. Total: 7 category features</td>
</tr>
<tr>
<td>Fingerprint (M2)</td>
<td>Level 1 features: (Global Fingerprint features): singular points, ridge orientation map, ridge frequency map</td>
<td>Level 1: L1, L2, L3. Level2: L4, L5. Level3: L6. Total: 6 category feature</td>
</tr>
<tr>
<td></td>
<td>Level 2 feature: ridge ending and ridge bifurcation. Minutiae location and orientation. Each of them is combination of a good number of features. But they combine make a unique identification of a feature.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Level 3 features: sweat pores. Pores are considered to be highly</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| Password (M3) | 1. Master password  
2. Key pattern  
3. Security question  
4. Profile information | Total: 4 types |
| CAPTCHA (M4) | 1. only numbers  
2. only characters  
3. alphanumeric characters  
4. pictorial CAPTCHA | Total: 4 types |
| SMS (M5) | 1. any number or character  
2. emoticon  
3. special character sequence showing a message | Total: 3 types |
| Voice (M6) | Pitch, different formant features (F1, F2 and F3) | Total: 4 features (but each of them are vectors not a scalar quantity) |
| Keystroke (M7) | 1. Key hold time (how long a key is pressed)  
2. Error Rate (number of times backspace is pressed)  
3. Horizontal Digraph: time to switch between horizontally adjacent keys  
4. Vertical Digraph: time to switch between vertically adjacent keys  
5. Non-Adjacent Horizontal Digraph: time to switch between non-adjacent horizontal keys  

### A. Adaptive Decision Support Implementation

The important design requirement in GA implementation lies in appropriate design of chromosome, constraints, objective functions and penalty functions. In order to achieve this, firstly the criteria for selecting authentication modality has to be determined. Fig. 2 shows some of these criteria including the variability of devices, media, and environments and shows the appropriate frequency and count of authentication modalities in each setting.

**Fig. 2.** Encoding of GA for modality and features for genetic search

The encoding of the GA is shown in Fig. 3 to represent both modalities, and their features in the chromosome. This scheme follows encoding of the structured genetic algorithm [21], where the chromosome is represented in two levels - modality and features. Here $M_i$ represents the modality and $f_{ij}$ represents the $j$th feature of $M_i$ modality. Each $M_i$ is represented by a bit (0 or 1) in chromosome encoding to indicate it is used or not. The chromosome representation shows both the modalities and features. The fitness measure considers the modality part and feature part separately and calculates the individual solution quality accordingly.

**Fig. 3.** Criteria for selecting authentication modalities

In this implementation of the GA, different variants of device and media are considered to create constraints as well as objective and penalty functions. To design the objective function for any particular modality, a new term called trustworthiness factor, is introduced here. This factor is expressed in terms of numeric values for a particular type of device/ media and this value signifies its impact on a particular selected modality. Higher value for this factor means that particular modality is more trustworthy in current settings. The calculation of trustworthiness factor is discussed in the following section.
B. Formulation of Trustworthiness Factor for Different Modalities

In current simulation, seven modalities are considered, where four of these are popular biometrics (face, fingerprint, voice, and keystroke analysis), and the rest are the common methods of authentication (password, CAPTCHA, and SMS). In general, no straightforward method is available to compute the trustworthy factor for these modalities (biometric and non-biometric modalities; active and passive modalities). In this work, we try to formulate an optimization problem to calculate the trustworthiness value.

Here, trustworthy value function for different modality-media-device combinations is done by utilizing pairwise comparative preference information. For instance, we can collect an answer for the following type question:

For a Wired Media, which of the two Devices-- Fixed or Portable-- is more trustworthy?

The answer could be any one of the following three cases:

Case 1: A Fixed Device is more trustworthy than a Portable Device.
Case 2: A Portable Device is more trustworthy than a Fixed Device.
Case 3: Both Devices are almost equally trustworthy or non-trustworthy.

Interestingly, since an optimization method is used to build the model, not all pairwise combinations of modalities, media, and devices are needed to be considered.

The representation of deterministic trustworthy value is: $T_{ij}^m$ for the $m$-th modality (of $M$ options), $i$-th device (of $N$ options), and $j$-th media (of $P$ options). Thus, for a particular pairwise comparison involving $i$-th and $k$-th devices for a fixed ($j$-th) media and fixed (m-th) modality, we would like to come up with $T_{ij}^m$ values, such that $T_{ij}^m > T_{ik}^m$, if Case 1 is the answer; $T_{ij}^m < T_{ik}^m$, if Case 2 is the answer; and $T_{ij}^m = T_{ik}^m$, if Case 3 is the answer. Based on these three cases, the following optimization problem can be formed to find a set of normalized $T_{ij}^m$ values:

Maximize $\zeta \leq c_1 \leq c_2$

Subject to:

$T_{ij}^m - T_{ik}^m \geq 0$, for each $j=1,2,3$ and $i,k=1,2,3, i\neq k$ (Case 1)

$T_{ij}^m - T_{ik}^m \leq 0$, for each $j=1,2,3$ and $i,k=1,2,3, i\neq k$ (Case 2)

$|T_{ij}^m - T_{ik}^m| \leq 0$, for each $j=1,2,3$ and $i,k=1,2,3, i\neq k$ (Case 3)

$max(T_{ij}^m, i,j=1,2,3) = 1$

$T_{ij}^m \geq 0$, for all $ij=1,2,3$.

The above optimization problem considers $\zeta$ as an additional variable and thereby makes a total of $(N \times P + 1)$ variables for each modality. The first three constraints enforce prescribed preferences. The fourth and fifth constraints together ensure that all $T_{ij}^m$ values lie in $[0, 1]$ with the condition that the highest $T_{ij}^m$ value is exactly one. This condition acts as a normalization factor. It will be useful when the trustworthy values for different modalities will be combined later to construct the overall trustworthy function value. The fourth constraint can be relaxed with each $T_{ij}^m \leq 1$ and split the third constraint set into two inequality constraint sets, so that the resulting problem becomes a linear programming (LP) problem. The resulting LP problem can then be solved using an LP solver (for example, using Matlab’s linprog()). The optimal $T$-matrix can be obtained.

If the optimal solution to the above problem causes the objective function value $\zeta^*$ to be strictly positive, a set of acceptable $T$-matrix is then found honoring all prescribed preferences. The $T$-matrix can then be used to compute the overall trustworthy function value (trustworthy factor) for running the genetic algorithm (GA). The detail steps of forming the optimization problem using the preference information and the calculations of trustworthy factors for the first modality are shown below.

This example only considers the pairwise comparative preference information as a metric to calculate the trustworthy function values. We consider the face recognition modality (M1) with three devices ($i=1$ for fixed device, 2 for portable device, 3 for handheld device) and three media ($j=1$ for wired media, 2 for wireless media, and 3 for cellular media), thereby making a total of nine trustworthy values. The preference conditions are shown below:

(i) For wired media (WI), a portable device (PD) is more trustworthy than a handheld device (HD), meaning $T_{21}^1 > T_{31}^1$ $\geq \epsilon_1$ (Case 1).

(ii) Irrespective of media, a fixed device is more trustworthy than a portable device, $T_{FD} > T_{PD}$, meaning $(T_{11}^1 + T_{12}^1 + T_{13}^1) - (T_{21}^1 + T_{22}^1 + T_{23}^1) \geq \epsilon_1$ (Case 1).

(iii) Irrespective of media, a fixed device is more trustworthy than a handheld device, $T_{FD} > T_{HD}$, meaning $(T_{11}^1 + T_{12}^1 + T_{13}^1) - (T_{31}^1 + T_{32}^1 + T_{33}^1) \geq \epsilon_1$ (Case 1).

(iv) A fixed device (irrespective of media) and a wired media (irrespective of devices) are almost equally trustworthy, $T_{FD} \approx T_{WH}$, meaning $(T_{11}^1 + T_{12}^1 + T_{13}^1) - (T_{11}^1 + T_{21}^1 + T_{31}^1) \leq \epsilon_2$ (case 3).

The LP solution for this optimization problem (obtained using Matlab’s linprog() routine) is given by the following $T$-matrix:

\[
\begin{bmatrix}
T_{11}^1 & T_{12}^1 & T_{13}^1 \\
T_{21}^1 & T_{22}^1 & T_{23}^1 \\
T_{31}^1 & T_{32}^1 & T_{33}^1
\end{bmatrix} = \begin{bmatrix}
1 & 0.364 & 0.636 \\
0 & 1 & 0 \\
0 & 0.139 & 0.861
\end{bmatrix}
\]

and $\epsilon_1 = 1, \epsilon_2 = 0, \epsilon^* = 1$. Since $\epsilon^* > 0$, above solution is acceptable. The trustworthy factors are:

$T_{FD} = 1 + 0.364 + 0.636 = 2$

$T_{PD} = 1 + 0 + 0 = 1$

$T_{HD} = 0 + 0.268 + 0.139 = 0.407$

$T_{WI} = 1 + 1 + 0 = 2$

$T_{WH} = 0.636 + 0 + 0.268 = 0.904$

$T_{CL} = 0.364 + 0 + 0.139 = 0.503$
At present, we calculated the trustworthy factors for different devices and media using the pairwise comparative preference values. Other factors (user preference, accuracy rate or false positive rate of the modalities) will be considered in the future to calculate the trustworthy measure. These values are adaptive in the sense that after authenticating users with the selected modalities, these users will also provide their feedback about the trustworthiness value of the used modalities and these values will be considered to tune the trustworthy value of those modalities in the next triggering of authentication. Hence, the trustworthy values can be changed in successive GA runs, which make the trustworthy values adaptive in nature and the selection decisions not to follow any specific pattern. The calculated trustworthy factors using the LP solver for all the seven modalities are shown in Table II.

TABLE II. TRUSTWORTHY VALUE: ASSUMPTIONS FOR DIFFERENT DEVICES AND MEDIA

<table>
<thead>
<tr>
<th>Modality</th>
<th>Trustworthiness factor of each modality for a particular Device</th>
<th>Trustworthiness factor of each modality for a particular Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>2.00</td>
<td>2.00</td>
</tr>
<tr>
<td>M2</td>
<td>1.82</td>
<td>1.76</td>
</tr>
<tr>
<td>M3</td>
<td>1.26</td>
<td>1.43</td>
</tr>
<tr>
<td>M4</td>
<td>0.87</td>
<td>0.87</td>
</tr>
<tr>
<td>M5</td>
<td>0.78</td>
<td>0.63</td>
</tr>
<tr>
<td>M6</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>M7</td>
<td>0.63</td>
<td>0.52</td>
</tr>
<tr>
<td>FD</td>
<td>1.00</td>
<td>0.503</td>
</tr>
<tr>
<td>PD</td>
<td>0.503</td>
<td>0.503</td>
</tr>
<tr>
<td>HD</td>
<td>0.407</td>
<td>0.503</td>
</tr>
</tbody>
</table>

Table II shows the seven previously mentioned modalities (M1, M2, ..., M7) and their respective trustworthiness value for different device and media. The abbreviations of different kinds of devices and media are also mentioned. These abbreviations are used to denote different operating environments in the results section of the paper. Each row shows the trustworthiness value of a particular modality in different devices and media.

C. Objective and Penalty Functions

In order to design the objective function, the effect of both device and media is considered and some weights are assigned to each of them to have varying effects. The objective function can formally be defined in the following way. For every selected modality of GA runs, the trustworthy values are calculated to get the best candidate out of all possible solutions of GA:

\[ T(M) = \sum_i (aX_i + bY_i + c) \]  (1)

where a, b and c are constants and considered as weight to the variables. \( X \) represents device and \( Y \) represents media, \( i \) represents the modality number (here between 1 to 7). The value of \( X_i \) and \( Y_i \) are already mentioned in Fig. 4. The trustworthy factors are summed for the selected modalities to get the cumulative value of the objective function. This value represents the total trustworthiness of the selected modalities for that authentication triggering event.

This form of the objective function captures the possible relations with device and media and the values of \( a \), \( b \) and \( c \) are adjusted for different environment settings. As a simple scenario, \( a = b = 0.5 \) and \( c = 0.0 \) can be considered. This sample values ensures that the change of device and media has the equal effect in making the selection decision of authentication modalities.

In order to design the penalty function for GA search, computational complexity is considered along with a weighting factor. This factor is included to control the selection of modality so that one modality is not always chosen in successive GA runs. The computational complexity of the modalities is the same in all devices and media as the same algorithm is used in different environment settings. It is also possible to choose a different algorithm for a single modality in different environment settings. In this case, the computational complexity will be another objective function. The penalty function can be formally defined in the following way:

\[ P_M = w_f \cdot P_f \]  (2)

where

\( P_M \): penalty value for this modality,
\( w_f \): weight factor for the penalty value, and
cost factor for this modality.

In Fig. 4, sample assumptions of the penalty value for each of the modalities are shown. These values are calculated based on median values of the user action time to make an attempt to do authentication. The values for face (M1), password (M3), and voice (M6) modalities are provided in [22]. The values for other modalities assumed here are based on user reaction time. The values are then mapped to the scale of 1 to 10 for easier calculation. Higher value indicates more time is needed to do the authentication steps and hence, more penalty value is placed on that particular modality so to have less chance to be selected. Generally, user interventional modalities assumed higher cost factors while non-interventional modalities considered lower. These values need to be adjusted as new methods/algorithms for existing modalities become available. Accordingly, the active authentication process needs to give less priority to modalities which take longer to authenticate users.

Weight factor \( w_f \) controls the effect of cost factor while computing fitness value of a set of modalities for selection. If authentication time triggering happens (when GA will run), but the environment settings are not changed after last GA run, the same set of modalities are chosen again. In order to alter the selected modalities and also to remove any pattern of selection of modalities, the weights of previously selected modalities are increased (they are penalized more) so that they are not the candidate for best selected modalities for the current GA run.

VI. Simulation Results

The proposed multi-authentication selection framework is experimented with a different set of simulated data (different device and media combinations). A java-based GA software toolset, called jMetal [24] is used in our implementation. To maintain diversity in candidate solutions, different selection, crossover, and mutation are adopted. In this particular problem, binary tournament is used for selection and a single-point crossover and bit-flip mutation are used. The crossover operation is only used in the first part of the chromosome (modality selection).

In order to restrict the count of selected modalities, a constraint is added so that maximum selected modalities do not exceed a threshold value. The input sequence for the program is generated randomly with different type of devices and media along with their corresponding coefficient parameters. Both repetitive and non-repetitive sequences of inputs are used for evaluating the performance of the GA-based modality selection.

The experiments are conducted with different combination of weights for devices and media as follows:

a) Both device and media have the same weight
b) Media has more weight than device
c) Device has more weight than media

Here, equal weight scenario for both device and media to select the authentication modalities at different time triggering events is described (see Fig. 5). Time elapsed, device change and media change events are shown in the figure along with their selected features.

In Fig. 5, the horizontal axis shows different authentication triggering events at different time steps (T1, T2 and T3). For instance, at T1, fingerprint, keystroke and password are chosen to authenticate the user. These modalities are shown in the upper portion of the vertical axis. The features for these three modalities are shown in the lower portion of the vertical axis. For Fingerprint, ridge frequency-map (F2), ridge ending (F4) and sweat pores (F6) are selected. Similarly, for Keystroke, error rate (F2), horizontal diagraph time (F3) and Vertical Diagraph time (F4) are selected as the features. For password, master password (F1) is selected at this triggering event. These features of these modalities are used to authenticate user at T1 timestamp.

Fig. 5. Results show multiple modality (and features) selection at different triggering events through genetic optimization

From Fig. 5, it is evident that no repetition of the same set of modalities is chosen for different triggering events. Again, we tested with repetitive settings of device and media in successive triggering times, and in all cases non-repetitive set of modalities are observed. Hence, this adaptive selection process ensures the diversity in modality selection. It is to be noted that no predictive pattern in modality selection observed even when the environment remained same for a long period. This guarantees the robustness of the selection framework and makes it difficult for the attackers to find any pattern of modality selection.

The steps involved in every triggering event are shown in Fig 6. This describes how GA can be integrated in an existing authentication system to provide an adaptive decision while performing the continual authentication process.
As only seven modalities are considered in current implementation, one modality may get selected in successive time triggering events while GA runs but select different features of the modalities. Hence, even with the same modality in successive time triggering events, the set of features used to authenticate users can be different. As there is no repetitive pattern, it is difficult for the attackers to guess which set of modalities will be used in any particular authentication triggering time. So this approach appears to provide an effective solution in choosing multiple modalities for active authentication system.

The static decision of modality selection is not an option for different operating environments as they are predefined. Hence, they are more vulnerable to be compromised by cyber attackers. For a dynamic decision policy, adaptive and random selections are the prominent choices. In our experiments, the adaptive selection is compared with complete random selection for different operating environments (Device + Media) and the comparative results are shown in Fig. 7.

From the Fig. 7, it is clear that the adaptive selection approach provides the more trustworthy modalities in a given scenario for most of the cases in comparison to random selection method. The operating environment captures the change of device and media along with other environment scenario (where the time triggering happened because of timeout). But it is noteworthy to mention that with different scenarios, the adaptive selection approach performs better than random selection of modalities in most of the cases.

Our adaptive selection approach is also compared with optimal cost selection method. Every modality has a cost factor associated with it (as previously estimated in Fig. 4) and needs to compute at triggering event times. Generally, the lower cost modality takes lesser time to do the authentication process. This comparative result is shown in Fig. 8.

From the Fig. 8, it is conclusive that optimal cost selection cannot provide the better modalities than adaptive version in terms of total trustworthiness value. Moreover, optimal cost solution in the best case performs as good as adaptive selection. Hence, it is clear that, with different scenarios, adaptive selection performs better than optimal cost selection.

In order to get a comparative picture of the three approaches, a qualitative comparison is performed and given in Table III. From the table, it is clear that adaptive selection outperforms the other two options. Hence, adaptive selection method seems to be effective way to develop the continuous authentication system.
VII. CONCLUSIONS AND FUTURE WORK

An adaptive multi-factor authentication selection is implemented using Genetic Algorithm (GA). The scope of this work is to explore the applicability of this algorithmic approach to adaptively select multiple authentication modalities and their features according to the environment (device and media) changes. This adaptive selection algorithm requires running at the time of triggering and hence, no prior solution is available for hacking and altering the selection decision. Results exhibit the performance of the proposed framework and illustrate the effect of both device and media types in activating the selected modalities in different time triggering events. This simulation also provides visualization support to show the results of modality selection decision in real time.

We believe that the successful implementation of the proposed approach will lead in developing an Identity Management Eco-System and MFA for Massive Open Online Course (MOOC) system in the future. In a MOOC, it is difficult to verify whether the registered person is actually taking the exams or not. Through incorporation of the proposed active authentication framework in MOOC, the reliability and acceptability of these online courses will be increased. In our future work, we will consider non-intervention type modality related to user-context (such as Structural Semantic Analysis, Forensic Authorship, etc.). Also comparison with other selection methods (such as rule-based selections) will be performed as an extension of this work. A usability study will be conducted to assess the burden on users while using this active authentication on a continuous basis. Also, different factors will be considered to calculate the trustworthy value. For instance, uniqueness and universality of the modalities [25] can be incorporated with the existing set of constraints to calculate the trustworthy factors, as well as a proper weighting to get a more representative value for this measure.

REFERENCES