An Adaptive Approach Towards the Selection of Multi-factor Authentication

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

***Abstract*—Authentication is the fundamental defense against any illegitimate access to a computing device or any sensitive online applications. Due to recent trends of emerging security threats, authentication using only a single factor is not reliable to provide adequate protection for these devices and applications. Hence, to facilitate continuous protection of computing devices and other critical online services from an un-authorized access, multi-factor authentication emerges as a viable option. Many authentication mechanisms with varying degrees of accuracy and portability are available for different types of computing devices connected with various communicating media. As a consequence, several existing and well-known multi-factor authentication strategies have already been utilized to enhance the security of various applications. Keeping this in mind, this research is focused on designing a robust and scalable framework for authenticating a legitimate user efficiently through a subset of available authentication modalities along with their several features (authentication factors) in time-varying operating environments (devices, media and surrounding conditions) on a regular basis. This paper highlights the creation of a trustworthy framework to quantify different authentication factors in terms of selection of different types of devices and media. In addition, a novel adaptive selection strategy for the available authentication factors incorporating the trustworthy values, previous history of selection as well as surrounding conditions is proposed in the paper. Selection through adaptive strategy ensures the incorporation of the existing environmental conditions within the selection of authentication factors and provides better diversity in the selection of these factors. Simulation results show that the proposed selection approach performs better than other existing selection strategies, namely, random and optimal selections in different settings of operating environments.**

I. Introduction

With the improvements of internet technologies, users' various online activities proliferate, which need to be trusted and secured in a way to prevent identity theft and data breaches. Authentications through a single factor (user id with password, for example) are suffering from some significant pitfalls. For instance, if a single factor authentication fails, the users cannot access the service until the system administrators restore the actual service. Moreover, the security of the system can never be predicted in case of occurring a system breach for a single factor authentication. So, authentication through different factors is a continuing trend providing more secure, resilient, and robust access verification to legitimate users while also making it harder for attackers to compromise the system. The majority of authentication systems in use today check a user's identity during login to a system. Two factor based authentication systems check the factors at the time of accessing the service for the first time only, increasing the chance of identity theft for failing to validate throughout the session. As the usage of handheld devices (smartphones, tablets, etc.) is rapidly increasing, the authenticity checking of the registered users in a continuous manner is an utmost need. This demand proliferates the need to move towards a multi-factor authentication (MFA) through providing different choices to authenticate user identities. MFA comes with a fail-safe feature in case of compromising any authentication factor. The other non-compromised factors will be used to support the authentication process.

One of the concerns regarding MFA is to choose the better set of authentication factors out of all the available choices within a given operating environment. In general, the choice of authentication factors determines the overall performance of MFA. Using the same factors or random selection of factors for MFA to validate the users in all operating environments (devices, media, and surrounding conditions) is not reasonable because, the selected authentication factors can be predictable and exploitable (for static selection approach) and can be less trustworthy (for random selection approach) than the other factors. Hence, to select the set of authentication factors through adaptive selection (considering trustworthiness, previous selection in the same environment settings, and more) is preferable choice for designing resilient MFA.

In this paper, a trustworthy framework is designed to compare different authentication modalities (along with their features) under different operating conditions (different settings of device and media). To facilitate the selection of multiple authentication factors, a novel adaptive approach is presented incorporating the trustworthy values, previous selection of authentication factors and surrounding conditions (for example: light, noise, motion, etc.). The scope of this paper is to formulate the selection of authentication factors through selecting a better set of authentication factors which are non-repetitive and do not follow any predictable pattern for attackers to exploit.

The rest of the paper is organized as follows. Section II highlights the related works on MFA; section III provides the concept of authentication factors; section IV describes the formulation of a trustworthy framework for different authentication factors; section V illustrates the adaptive selection approach of MFA; section VI mentions the simulation results for different selection approaches and the advantage of the proposed approach; section VII highlights structural comparisons of the proposed approach with other MFA approaches and section VIII mentions the concluding remarks and future research directions.

978-1-4799-7560-0/15 $31.00 © 2015 IEEE
DOI 10.1109/SSCI.2015.75

II. RELATED WORKS OF MFA

Two-factor authentication is the most commonly used approach now-a-days for different online services, where the first factor is the traditional password and the second factor is either an access code through SMS or a PIN-code generated randomly at the time of authentication. Microsoft's Windows Azure Active Directory [1] uses multi-factor authentication for their cloud applications, which incorporates a one-time password, an automated phone call, and a text message (SMS), for a total of three authentication modalities. This approach uses a fixed set of modalities and the different authentication factors are chosen only by user preference. Fast Identity Online (FIDO) alliance [2] developed a framework for online authentication that provides an open and scalable solution to reduce user dependency on passwords. They provide the biometric authentication modalities and PIN-codes to support multi-factor authentication without the use of traditional passwords. However, they did not include passive biometrics like keystroke dynamics, mouse movements, typing behavior etc. Hence, a continuous way of authenticating the users without user interruptions was not part of their framework.

A continuous way of authenticating legitimate users requires both behavioral and cognitive modalities to be considered. Stylometry work [11] uses different stylometric methods (for example, writing style as part of author recognition) to validate the authentic users as they are typing. With the help of these methods, deceptive writing by malicious users can easily be identified and used as a passive authentication technique for continuous MFA. Web browsing behavior [12, 13] is also utilized to identify actual users of a system through continuously monitoring their patterns of browsing over different webpages. This approach captures the semantic behavior of the users through both semantic and syntactic session features (for example, time to click, etc.) to execute user identification. Screen Fingerprints [1, 2, 4, 5, 14, 15, 16] are also good candidates for a biometric modality in continuous authentication. This approach captures a computer screen recording and then explores discriminative visual features from that recording. It works based on visual cues (typing, mouse moving, scrolling, etc.) that are always observable on a screen irrespective of different types of applications. Behavioral biometrics [10, 13, 17, 18] can also be used in online courses to perform assessments of students' work and also for authentication of authors to verify their literary works. Incorporation of keystroke and mouse dynamics have also significantly improved user authentication in a passive way [16, 19, 20]. Thus, these authentication modalities can be applied in continuously authenticating the users of different systems.

A good amount of work has been done to facilitate the use of continuous user authentication. Authors in this body of work [17] use temporal information about the users (like a user's face and other features) which does not change the posture of the users. This approach can even identify a user in the absence of biometric observations. Incorporating different behavioral biometrics (keyboard interactions, mouse movements and application interactions), by BehavioSec [4, 5, 22] provides promising results in continuous authentication of the users. A trust model is designed to include the effect of all three biometrics to provide faster detection of incorrect users. Typing behavior and linguistic style of the users [5, 19, 20] are also considered as passive authentication modalities to help this authentication approach. In this work, features are extracted from properties of word creation, lexical complexity, revision count, and keyboard proficiency, with their sub properties used to build a set of fine grained features. These research works illustrate that user authentication in a continuous manner is possible using a set of passive authentication modalities.

Mobile devices are widely used to maintain online activities such as browsing emails, checking bank accounts, maintaining social networks, etc. Hence, a good amount of research has been conducted on providing continuous authentication to the users' of mobile devices. Smartphone accelerometer features mentioned in [6, 23, 24], provide a way to identify the user's pattern of how a person holds his or her phone. The impact of the position of the phone and context-aware information on the location of the phone during authentication provide significant improvements in authentication accuracy of the users. This work explores the new way of gait-based authentication. By analyzing the typing motion behavior of the users, continuous authentication can be done [16, 24]. Different machine learning based classifiers can be adopted to classify the actual users utilizing the extracted features. As most smart phones have touch screens, typing motion can also be easily integrated within the continuous authentication process. These research studies demonstrate that continuous user authentication using MFA is possible for all the existing devices which do not depend on specific hardware or platforms.

III. CONSIDERED AUTHENTICATION FACTORS

In this paper, an authentication factor is defined in any of the following ways:

(1) A single feature of an authentication modality;

(2) Any combination of features of an authentication modality;

(3) Combination of multiple features of different authentication modalities.

In that way, the available options for authentication factors increase significantly with a fixed set of authentication modalities and their respective features. This definition expands the possible choice of authentication factors and thereby, reduces the chance of selecting the same set of authentication factors in successive triggering events of MFA.

For example, $\{M_1: f_{1,1}\}$ and $\{M_2: f_{2,1}\}$, the first features of M_1 and M_2 respectively, can be considered as two authentication factors (described in scenario 1). Moreover, $\{M_1: f_{1,1}, f_{1,2}\}$, combinations of $\{M_1: f_{1,1}\}$ and $\{M_1: f_{1,2}\}$, can also be considered as an authentication factor (scenario 2). Additionally, the combination of $\{M_1: f_{1,1}\}$ and $\{M_2: f_{2,1}\}$, i.e., $\{M_1, M_2: f_{1,1}, f_{2,1}\}$, can also be considered as one authentication factor (scenario 3).

In this work, ten authentication modalities (seven of them are biometric and the remaining are non-biometric) have been used. The biometric authentication modalities can be classified based on physiological (face recognition, iris, finger print and hand biometric) and behavioral (key stroke, mouse dynamics, and voice recognition) attributes. The brief descriptions of different features of the authentication modalities and their respective error rates are shown in Table I. Additionally, the usability conditions for different authentication modalities are also included.

[1] http://azure.microsoft.com/en-us/services/active-directory/

[2] https://fidoalliance.org/

TABLE I. DESCRIPTIONS OF VARIOUS FEATURES OF DIFFERENT AUTHENTICATION MODALITIES ALONG WITH THEIR EER, FAR, FRR, FMR AND FNMR.

Descriptions & Computational Features
Face Recognition ($\mathbf{M_1}$): **Geometrical Features**: 7 category features ($\{M_1: \{f_{1,i}\}_{i\in\mathbb{Z}^+}\}$)will be considered as follows: **Lip** ($\{M_1: f_{1,1}\}$): The EER of this feature lies between 5.2% and 6.8% [6] . **Eye** ($\{M_1: f_{1,2}\}$): Its FMR and FNMR are 0% and 1% respectively [6] . **Brow and Check** ($\{\mathbf{M_1}: \boldsymbol{f_{1,3}}\}$): Both brow and cheek templates are tracked using Lucas-Kanade algorithm. Here, EER is about 15% [6]. **Textural Features** ($\{\mathbf{M_1}: \boldsymbol{f_{1,4}}\}$): Its' ERR is not very less, about 10% [6] . Overall FAR and FRR for the face recognition modality are 1% and 20% respectively. **Usability**: Under normal lighting conditions, geometric features will used. Under varying lighting conditions, textural features will be utilized. This modality is not reliable if the facial features can be altered through plastic surgery [6, 25]. It is also dependent on the motion of the object [6].
Iris Recognition($\mathbf{M_2}$): **Feature Extraction**: Texture phase structure information will be elicited. Its different features are denoted by$\{M_2: \{f_{2,i}\}_{i\in\mathbb{Z}^+}\}$.Its FAR is about 0.01% [6]. **Usability**:Reliable and accurate biometric trait for ideal environment. If a user suffers from an eye disease, this modality is not suitable. It is also dependent on light. This modality is also dependent on the motion of the object [6].
Finger Print($\mathbf{M_3}$): Three level of finger print features will be considered (with a total of 6 category features $\{M_4: \{f_{4,i}\}_{i\in\mathbb{Z}^+}\}$): **Level 1 features** (Global Fingerprint features) **Level 2 feature** (Minutiae based features) **Level 3 features** (Sweat-pore-based features) The best algorithm for finger print verification yields EER less than 2.07% and more than 30% of the algorithms yield EER less than 5% [6]. The overall FAR, FRR, crossover rate and failure to enrollment rates are 2%, 2%, 2% and 1% respectively. **Usability:** Fingerprints can be forged and altered by transplant surgery [6, 9, 14].
Hand Biometric ($\mathbf{M_4}$): The features $\{M_5: \{f_{5,i}\}_{i\in\mathbb{Z}^+}\}$are as follows: **Palm Print** ($\{M_5: f_{5,1}\}$): It is highly reliable with EER is less than 1%. It's FAR and FRR are 4.49% and 2.04% respectively [6]. **Hand Geometry** ($\{M_5: f_{5,2}\}$): Its **EER** is 0.0012%. It'sFAR and FRR are 5.29% and 8.34% respectively [6]. **Vein Structure** ($\{M_5: f_{5,3}\}$): Its EER lies between 2.3% and 3.75%. **Usability** :Hand biometric can be forged and altered.
Password ($\mathbf{M_5}$): Password [6, 26] is the most common modality. It can be stored in hashed form and matched with the input by hashing the given password as string matching. **Usability:** The security of the passwords depends on the users' ability to maintain the password secret. Also it is susceptible to numerous attacks.
CAPTCHA ($\mathbf{M_6}$): CAPTCHA [6, 30] is used to prevent different automated software or web robots to perform actions and can discriminate between human and bots. **Usability:** This has been using in the online applications widely. But sometimes it is really harder for human to interpret.
SMS ($\mathbf{M_7}$): SMS [6] is used to send the pass-code to a given registered phone number and that code is valid for a short period of time. The features of this modality are given as: any number or character; Emoticon and special character sequence showing a message. **Usability:** It has the issue of expense while sending or receiving. It cannot be used in places with limited cellular coverage.
Voice ($\mathbf{M_8}$): Voice recognition [6] uses pitch and different formant features. The FAR , FRR and the crossover rates for the voice modality are 2%, 10% and 6% respectively. **Usability**: This modality may fail to detect a legitimate user in a noisy environment. Also, if a user suffers from a throat infection, this modality is no longer useful. It is also dependent on motion(M).
Key Stroke($\mathbf{M_9}$): This modality detects the pattern of the keystrokes [6]. The overall FAR, FRR and the crossover rates for the key stroke modality are 7%, 0.1% and 1.8% respectively. Its different features are denoted by$\{M_9: \{f_{9,i}\}_{i\in\mathbb{Z}^+}\}$. **Usability**: This trait is particularly useful for verification only.
Mouse Dynamics ($\mathbf{M_{10}}$): The research on mouse dynamics mainly concentrated on the motor skill features (e.g., time for signal, click, time for double click, and speed in a particular direction) or mouse actions such as cursor positions on the screen, idle time of the mouse and the movement distances [6]. Again, the other features regarding the mouse dynamics are the mouse angles, directions, angle of curvature and curvature distance [6]. The features are represented as $\{M_{10}: \{f_{10,i}\}_{i\in\mathbb{Z}^+}\}$. **Usability**: This trait is particularly useful for verification only.

IV. TRUSTWORTHY FRAMEWORK FOR DIFFERENT AUTHENTICATION FACTORS

In this work, a strategy for calculating the trustworthy values of different authentication factors has been presented to quantify the effects of different factors in different settings of device and media. This metric will later be used to provide selection decision of different authentication factors in different operating conditions. As no straightforward method is available to compute the trustworthy values for different authentication factors, we formulate a non-linear optimization problem to calculate the trustworthy values. Previous works [7, 8] related to the trustworthy framework focused on deterministic approaches to calculate the trustworthy value of the authentication modalities. In this work, probabilistic approach of comparative preferences are considered as no prior data regarding preferences are available in the literature. The pair-wise comparative preferences for different combinations of authentication factor-device-media and individual error rates of different authentication factors are used to calculate the trustworthy values of those factors. These values are calculated for different features of authentication modalities for which the error rates are known. Trustworthy values are later used to design the adaptive selection procedure for MFA.

Now, let us assume that an authentication modality (with a set of features), $M_i; (i = 1,2 \dots s)$ is more (or less or equally) trusted for a user in a device $D_j; (j = 1,2, \dots, d)$ rather than in device $D_k; (k = 1,2, \dots, d; k \neq j)$ for a particular medium $Me_l; (l =$

$1,2 \ldots e)$. The corresponding representation for the pair-wise comparative trustworthy preference is: $T_{ij}(\mathrm{M}_s; f_{s,l})$ for the m^{th} modality (s options) with features $\{\mathrm{M}_s; f_{s,l}\}$ (taking one feature at a time), i^{th} device (d options) and the j^{th} medium (e options). The random variable $\{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l})\}$ can be constructed to determine the comparisons of the trustworthiness of different devices, keeping the **medium selection fixed**. Now, for a particular pair-wise comparison involving i^{th} and k^{th} devices for a fixed (j^{th}) media and fixed (m^{th}) authentication modality, any of the following three conditions will occur:

(1) $\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) > \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}); i \neq k;$
(2) $\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) = \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}); i \neq k;$
(3) $\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) < \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}); i \neq k;$
Since, all of them are equally likely:

$$\{P(\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) > \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}); i \neq k)\} = \{P(\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) < \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}); i \neq k)\} = \{P(\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) = \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}); i \neq k)\} = \frac{1}{3}$$

Similarly, the random variable $\{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l})\}$ has been constructed to determine the comparisons of the trustworthiness of different media, keeping the **device selection fixed**.

Based on the above cases, the following non-linear programming problem with probabilistic constraints (NLPPPC) [9] has been formed to find a set of $\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l})$ values.

$$\textbf{Maximize} \sum_j \sum_i \sum_{\substack{k \\ i \neq k}} \left| \frac{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) - \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l})}{\varepsilon_1} \right| + \sum_i \sum_j \sum_{\substack{k \\ j \neq k}} \left| \frac{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) - \mathrm{T}_{ik}(\mathrm{M}_s; f_{s,l})}{\varepsilon_2} \right| \quad (1)$$

Subject to:

$$P\{T_{ij}(\mathrm{M}_s; f_{s,l}) \geq T_{kj}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } i,k = 1,2,3; i \neq k; l \in \mathbb{Z}^+\} \geq 1 - \varepsilon_1; \quad (2)$$

$$P\{T_{kj}(\mathrm{M}_s; f_{s,l}) > T_{ij}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } i,k = 1,2,3; i \neq k; l \in \mathbb{Z}^+\} \geq \varepsilon_1; \quad (3)$$

$$P\{T_{ij}(\mathrm{M}_s; f_{s,l}) \geq T_{ik}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } i,k = 1,2,3; j \neq k; l \in \mathbb{Z}^+\} \geq 1 - \varepsilon_2; \quad (4)$$

$$P\{T_{ik}(\mathrm{M}_s; f_{s,l}) > T_{ij}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } i,k = 1,2,3; j \neq k; l \in \mathbb{Z}^+\} \geq \varepsilon_2; \quad (5)$$

$$0 \leq T_{ij}(\mathrm{M}_s; f_{s,l}) \leq 1; \ \forall i,j = 1,2,3; \ l \in \mathbb{Z}^+ \quad (6)$$

In the present research, we consider ten mostly used authentication modalities (as mentioned in Table 1), three types of devices (fixed device, handheld device, and portable device) and three different media (wired, wireless, and the cellular medium) to calculate the trustworthy values of the authentication factors. However, the proposed method can be applied for any number of devices, media, and authentication modalities.

The primary objective of the proposed NLPPPC is to find the trustworthy value of every single feature of any authentication modality. The proposed formulation for calculating the trustworthy values is generalized, although, it is more applicable for the biometric authentication modalities. In this work, the trustworthy values are calculated for those authentication factors which has available error rates (FAR, FRR or EER). However, the authors are trying to investigate how the proposed system can produce better visualization of trustworthy values for different non-biometric authentication modalities.

Two random variables are considered to follow standard normal distribution as no data are available regarding the distribution of the pair-wise trustworthy values. These variables become $\{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l})\}_{j=1}^{3} \sim N(0,1)$ (media changed, i.e. $\{\mathrm{T}_{i1}(\mathrm{M}_s; f_{s,l})_{s,l}, \mathrm{T}_{i2}(\mathrm{M}_s; f_{s,l})_{s,l}, \mathrm{T}_{i3}(\mathrm{M}_s; f_{s,l})_{s,l}\}$) and $\{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l})\}_{i=1}^{3} \sim N(0,1)$ (device changed, i.e. $\{\mathrm{T}_{i1}(\mathrm{M}_s; f_{s,l})_{s,l}, \mathrm{T}_{i2}(\mathrm{M}_s; f_{s,l})_{s,l}, \mathrm{T}_{i3}(\mathrm{M}_s; f_{s,l})_{s,l}\}$). $\varepsilon_1 \in (0,1)$ is the critical region [28] for $P\{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) \geq \mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } i,k = 1,2,3; i \neq k; l \in \mathbb{Z}^+\}$ and $P\{\mathrm{T}_{kj}(\mathrm{M}_s; f_{s,l}) > \mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } i,k = 1,2,3; i \neq k; l \in \mathbb{Z}^+\}$. If $\varepsilon_1 \to 1$, then the probability of accepting the hypothesis given in Equation (2) decreases, increasing the probability of accepting the hypothesis presented in Equation (3). Similarly, $\varepsilon_2 \in (0,1)$ is the critical region of $P\{\mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}) \geq \mathrm{T}_{ik}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } i,k = 1,2,3; j \neq k; l \in \mathbb{Z}^+\}$ and $P\{\mathrm{T}_{ik}(\mathrm{M}_s; f_{s,l}) > \mathrm{T}_{ij}(\mathrm{M}_s; f_{s,l}); \forall j = 1,2,3 \text{ and } \forall i,k = 1,2,3; j \neq k; l \in \mathbb{Z}^+\}$.

Similar conclusion can be made in case of the trustworthy value of a particular modality in a device and on different media. Now, combining both the cases the objective function of the proposed NLPPPC has been constructed. The nature of the objective function is convex. . Hence, the solution space of the optimization problem is bounded and we can find a solution of the pair-wise comparative trustworthy preferences and ε_1, ε_2, for which equation(1) will be satisfied.

Now, to illustrate the solution procedure, an example has been cited that considers the pair-wise comparative preference information as a metric to calculate the trustworthy function values. Here, face recognition modality with feature $(\mathrm{M}_1: f_{1,1})$ with three devices ($i = 1$ for fixed device, 2 for portable device and 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. This example can be explained well with the help of the proposed non-linear optimization problem with probabilistic constraints as follows:

Case 1: For wired media (WI), a portable device (PD) is more trustworthy than a handheld device (HD), i.e., $P\{\mathrm{T}_{21}(\mathrm{M}_1; f_{1,1}) > \mathrm{T}_{31}(\mathrm{M}_1; f_{1,1})\} \geq 1 - \varepsilon_1$.
Case 2: For wired media (WI), a portable device (PD) is less trustworthy than a handheld device (HD), i.e., $P\{\mathrm{T}_{21}(\mathrm{M}_1; f_{1,1}) < \mathrm{T}_{31}(\mathrm{M}_1; f_{1,1})\} \geq \varepsilon_1$.
Case 3: Both the devices are equally trusted, i.e., $P\{\mathrm{T}_{21}(\mathrm{M}_1; f_{1,1}) = \mathrm{T}_{31}(\mathrm{M}_1; f_{1,1})\} \geq 1 - \varepsilon_1$.
Case 4: For the portable device (PD), a wired media (WI) is more trusted than a wireless (WL) medium, i.e., $P\{\mathrm{T}_{21}(\mathrm{M}_1; f_{1,1}) > \mathrm{T}_{22}(\mathrm{M}_1; f_{1,1})\} \geq 1 - \varepsilon_2$.
Case 5: For the portable device (PD), a wired media (WI) is less trusted than a wireless (WL) medium, i.e., $P\{\mathrm{T}_{21}(\mathrm{M}_1; f_{1,1}) < \mathrm{T}_{22}(\mathrm{M}_1; f_{1,1})\} \geq \varepsilon_2$.
Case 6: For the portable device (PD), a wired media (WI) is equally trusted like wireless (WL) medium, i.e., $P\{\mathrm{T}_{21}(\mathrm{M}_1; f_{1,1}) = \mathrm{T}_{22}(\mathrm{M}_1; f_{1,1})\} \geq 1 - \varepsilon_2$.

Next, the above optimization problem is solved to obtain in the following T-matrix form:

$$\begin{bmatrix} \mathrm{T}_{11}(\mathrm{M}_1; f_{1,1}) & \mathrm{T}_{12}(\mathrm{M}_1; f_{1,1}) & \mathrm{T}_{13}(\mathrm{M}_1; f_{1,1}) \\ \mathrm{T}_{21}(\mathrm{M}_1; f_{1,1}) & \mathrm{T}_{22}(\mathrm{M}_1; f_{1,1}) & \mathrm{T}_{23}(\mathrm{M}_1; f_{1,1}) \\ \mathrm{T}_{31}(\mathrm{M}_1; f_{1,1}) & \mathrm{T}_{32}(\mathrm{M}_1; f_{1,1}) & \mathrm{T}_{33}(\mathrm{M}_1; f_{1,1}) \end{bmatrix} = \begin{bmatrix} 0.99 & 0.761 & 0.415 \\ 0.502 & 0.856 & 0.473 \\ 0.594 & 0.434 & 0.047 \end{bmatrix} \; and \; \varepsilon_1 = 0.4429, \varepsilon_2 = 0.2392$$

TABLE II: TRUSTWORTHY VALUES OF DIFFERENT FEATURES OF VARIOUS AUTHENTICATION MODALITIES.

Modalities	**Features**	**Trustworthy Values**					
		FD	**PD**	**HD**	**WI**	**WL**	**CL**
$(\mathbf{M_1})$	$(M_1: f_{1,1})$	2.02	1.67	1.00	1.95	1.92	0.87
	$(M_1: f_{1,2})$	2.15	1.79	1.07	2.08	2.04	0.93
	$(\mathrm{M}_1: f_{1,3})$	1.84	1.52	0.92	1.78	1.74	0.8
	...	...	...	...	...	...	...
$(\mathbf{M_2})$	$(\mathrm{M}_2: f_{2,i}; i \in \mathbb{Z}^+)$	2.17	1.79	1.07	2.09	2.05	0.94
$(\mathbf{M_3})$	$(\mathrm{M}_3: f_{3,i}; i \in \mathbb{Z}^+)$	2.12	1.76	1.05	2.04	2.01	0.92
$(\mathbf{M_4})$	$(\mathrm{M}_4: f_{4,1})$	2.07	1.71	1.03	1.99	1.96	0.89
	$(\mathrm{M}_4: f_{4,2})$	2.05	1.70	1.02	1.98	1.94	0.89
$(\mathbf{M_5})$	$(\mathrm{M}_5: f_{6,i}; i \in \mathbb{Z}^+)$	1.76	1.26	1.13	1.76	1.43	1.26
$(\mathbf{M_6})$	$(\mathrm{M}_6: f_{6,i}; i \in \mathbb{Z}^+)$	1.44	0.87	0.87	1.00	0.5	0.5
$(\mathbf{M_7})$	$(\mathrm{M}_7: f_{8,i}; i \in \mathbb{Z}^+)$	0.63	0.78	0.63	1.76	1.64	1.48
$(\mathbf{M_8})$	$(\mathrm{M}_8: f_{9,i}; i \in \mathbb{Z}^+)$	1.95	1.61	0.97	1.88	1.85	0.84
$(\mathbf{M_9})$	$(\mathrm{M}_9: f_{9,i}; i \in \mathbb{Z}^+)$	1.84	1.52	0.91	1.77	1.74	0.80
$(\mathbf{M_{10}})$	$(\mathrm{M}_{10}: f_{10,i}; i \in \mathbb{Z}^+)$	0.99	0.96	0.92	0.92	0.82	0.86

.

To get the trustworthy values (TD) of any particular device (D), we assume all the pair-wise trustworthy values (values with that device and all connecting media) computed in T-Matrix are contributed in standard normal distribution to TD. Hence, the trustworthy values of the FD, PD and HD as well as the WI, WL, and CL for $(\mathrm{M}_1; f_{1,1})$ can be calculated as follows:

$\mathrm{T}_{\mathrm{FD}}(\mathrm{M}_1; f_{1,1}) = 0.99 + 0.761 + 0.415 = 2.17.$
$\mathrm{T}_{\mathrm{PD}}(\mathrm{M}_1; f_{1,1}) = 0.502 + 0.856 + 0.473 = 1.83.$
$\mathrm{T}_{\mathrm{HD}}(\mathrm{M}_1; f_{1,1}) = 0.594 + 0.434 + 0.047 = 1.07.$
$\mathrm{T}_{\mathrm{WI}}(\mathrm{M}_1; f_{1,1}) = 0.99 + 0.502 + 0.594 = 2.08.$
$\mathrm{T}_{\mathrm{WL}}(\mathrm{M}_1; f_{1,1}) = 0.76 + 0.856 + 0.434 = 2.05.$
$\mathrm{T}_{\mathrm{CL}}(\mathrm{M}_1; f_{1,1}) = 0.415 + 0.473 + 0.047 = 0.92.$

The EER for $\mathrm{M}_1; f_{1,1}$ is 6.8%. Hence, for 93.2% cases, this feature performs acceptably. The values of trustworthy factor mentioned above does not consider the error rates. With the incorporation of the EER, we can scale the above mentioned trustworthy values.

$\mathrm{T}_{\mathrm{FD}}(\mathrm{M}_1; f_{1,1}) = 2.02.$ $\mathrm{T}_{\mathrm{PD}}(\mathrm{M}_1; f_{1,1}) = 1.67.$
$\mathrm{T}_{\mathrm{HD}}(\mathrm{M}_1; f_{1,1}) = 1.002.$ $\mathrm{T}_{\mathrm{WI}}(\mathrm{M}_1; f_{1,1}) = 1.95.$
$\mathrm{T}_{\mathrm{WL}}(\mathrm{M}_1; f_{1,1}) = 1.92.$ $\mathrm{T}_{\mathrm{CL}}(\mathrm{M}_1; f_{1,1}) = 0.87.$

In a similar manner the trustworthy values for other modalities with their various features in different devices and media can be calculated. The trustworthy values of various features of different authentication modalities are tabulated and are shown in Table II. In order to calculate the trustworthy values for combination of different features, separate methodology is adopted as error rates (EER, FAR, etc.) are not available for combined authentication factors. The proposed formulation will incorporate the influence of individual error rates into the trustworthy value of the combined authentication factor. Two continuous random variables $X_{d\bar{m}pj}$ and $X_{\bar{d}mpj}$ can be defined as follows:

$\boldsymbol{X_{d\bar{m}pj} \sim N(0,1)}$: The influence of $\mathrm{T}_{d\bar{m}}(\mathrm{M}_p: f_{p,1}, f_{p,2}, \dots)$ on $\mathrm{T}_{d\bar{m}}(\mathrm{M}_1, \mathrm{M}_2, \dots : f_{p,1}, f_{p,2}, \dots)$; $\forall d, m, p, j \in \mathbb{Z}^+$, in a particular medium irrespective of devices.

$\boldsymbol{X_{\bar{d}mpj} \sim N(0,1)}$: The influence of $\mathrm{T}_{\bar{d}m}(\mathrm{M}_p: f_{p,1}, f_{p,2}, \dots)$ on $\mathrm{T}_{\bar{d}m}(\mathrm{M}_1, \mathrm{M}_2, \dots : f_{p,1}, f_{p,2}, \dots)$; $\forall d, m, p, j \in \mathbb{Z}^+$ in a particular device irrespective of medium.

Let assume, the highest and lowest trustworthy values of an authentication factor $(\mathrm{M}_{p_k}: f_{p_k,j})_{k \in \mathbb{Z}^+}$ on different devices are $b_{k \in \mathbb{Z}^+}$ and $a_{k \in \mathbb{Z}^+}$ respectively. Now, the trustworthy value of $\{\mathrm{M}_{p_k}: f_{p_k,j}\}_{k \in \mathbb{Z}^+}$ in any medium irrespective of devices can be calculated as follows:

$$\mathrm{T}_{d\bar{m}}\left(\{\mathrm{M}_{p_k}\}: \{f_{p_k,j}\}_j\right)_k$$
$$= E\{a_1 \le X_{d\bar{m}p_1j} \le b_1; \dots a_n \le X_{d\bar{m}p_nj} \le b_n\}$$
$$= \int_{a_1}^{b_1} \dots \int_{a_n}^{b_n} x_{d\bar{m}p_1j} * \dots * x_{d\bar{m}p_nj}$$
$$* f_{X_{d\bar{m}p_1j}, \dots X_{d\bar{m}p_nj}}(x_{d\bar{m}p_1j}, \dots x_{d\bar{m}p_nj}) dx_{d\bar{m}p_1j} \dots dx_{d\bar{m}p_nj}$$
$$= \int_{a_1}^{b_1} \dots \int_{a_n}^{b_n} x_{d\bar{m}p_1j} * \dots * x_{d\bar{m}p_nj} *$$
$$\frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x_{d\bar{m}p_1j}^2} \dots \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x_{d\bar{m}p_nj}^2} dx_{d\bar{m}p_1j} \dots dx_{d\bar{m}p_nj}$$

Here, $f_{X_{d\bar{m}p_1j}, \dots X_{d\bar{m}p_nj}}(x_{d\bar{m}p_1j}, \dots x_{d\bar{m}p_nj})$ is the joint distribution function of $X_{d\bar{m}p_1j}, X_{d\bar{m}p_2j}, \dots, X_{d\bar{m}p_nj}$ .The random variables $X_{d\bar{m}p_1j}, X_{d\bar{m}p_2j}, \dots, X_{d\bar{m}p_nj}$ are independent to one another in the proposed formulation as different authentication modalities along with their several features are mutually independent to one another. Next, to get the trustworthy value of $\{\mathrm{M}_{p_k}: f_{p_k,j}\}_{k \in \mathbb{Z}^+}$ in a particular medium, the influence of the individual trustworthy values of $\{\mathrm{M}_{p_k}: f_{p_k,j}\}_{k \in \mathbb{Z}^+}$ in that medium (which follows the standard normal distribution with the combined

trustworthy value) has been incorporated with the previous quantity in the following way:

$$E\{a_1 \le X_{d\bar{m}p_1 j} \le b_1; \dots a_n \le X_{d\bar{m}p_{nj}} \le b_n\} + \frac{1}{\sqrt{2\pi}} \sum_k \sum_j e^{-\frac{1}{2}\left\{T_{m_i}\left(\mathrm{M}_{p_k}: f_{p_k,j}\right)\right\}^2},$$

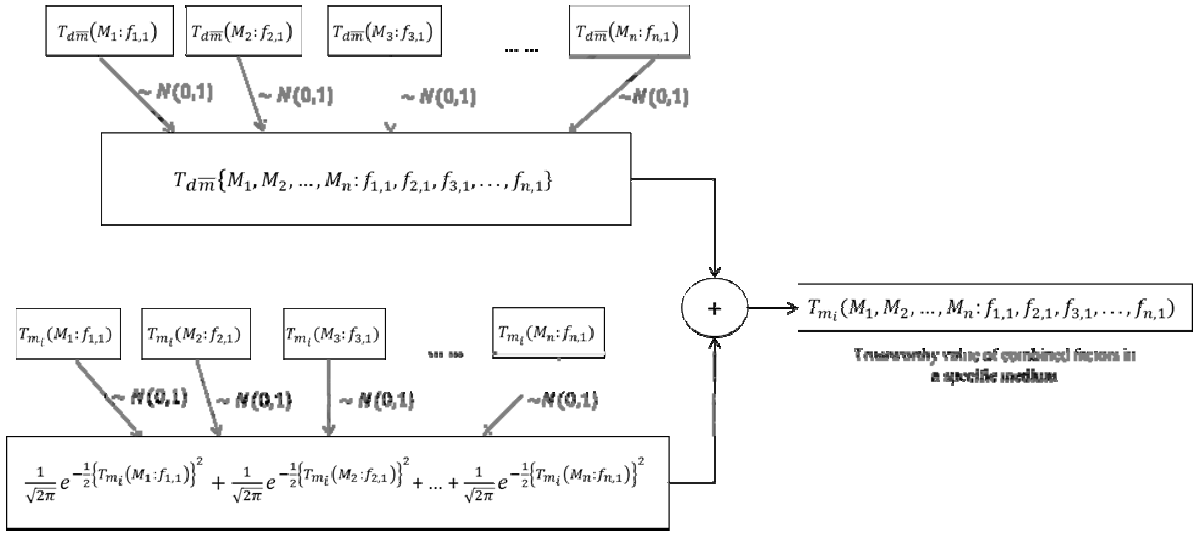

Fig. 1. Calculation strategy of trustworthy values of combined factor from individual trustworthy values.

.

where $T_{m_i}\left(\mathrm{M}_{p_k}: f_{p_k,j}\right)$ is the trustworthy value of $\left(\mathrm{M}_{p_k}: f_{p_k,j}\right)$ on the i^{th} medium. The above quantity gives the combined trustworthy value for the considered factors in a given medium (m_i).

A scenarios is represented in Fig 1 to show the influence of individual trustworthy values of $\mathrm{M}_1: f_{1,1}; \mathrm{M}_2: f_{2,1} \dots \mathrm{M}_n: f_{n,1}$ for a medium (irrespective of any devices) on the combined trustworthy value of $\left\{\mathrm{M}_1: f_{1,1}, \mathrm{M}_2: f_{2,1} \dots \mathrm{M}_n: f_{n,1}\right\}$. The trustworthy value for a specific medium (M_i) is then finally calculated as shown in Fig. 1.

Trustworthy value for $\left\{\mathrm{M}_1: f_{1,1}, \mathrm{M}_1: f_{1,2}\right\}$ in the wired medium, WI (which follows the standard normal distribution with the combined trustworthy value) is shown here as an example.

$$T_{d\bar{m}}\left\{\mathrm{M}_1: f_{1,1}; \mathrm{M}_1: f_{1,2}\right\} + \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}\left(T_{WI}(\mathrm{M}_1: f_{1,1})^2 + T_{WI}(\mathrm{M}_1: f_{1,2})^2\right)} =$$

$$\left(\int_{1.002}^{2.02} x_{d\bar{m}11} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}{x_{d\bar{m}11}}^2} dx_{d\bar{m}11}\right) * \left(\int_{1.07}^{2.15} x_{d\bar{m}12} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}{x_{d\bar{m}12}}^2} dx_{d\bar{m}12}\right) + \left\{\frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}1.95^2} + \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}2.08^2}\right\} \approx 2.67 + 0.06 + 0.05 \approx 2.78,$$

which can be found in the fourth row of Table III. Similarly, the combined trustworthy values of other authentication modalities can be calculated, some of them are listed in Table III.

V. ADAPTIVE SELECTION OF DIFFERENT AUTHENTICATION FACTORS

Trustworthy values calculated in the previous section provide a metric to design the selection algorithm for multi-factor authentication. This section describes the procedure for adaptive selection of the authentication factors to provide secure authentication for legitimate users considering various devices, media, and surrounding conditions, they are connected with. The selected set of authentication factors should have higher total trustworthy values and performance, and it should be different from previous set of selected modalities if device, medium and surrounding conditions are the same. Hence, to achieve this goal in the selection process, a multi objective non-linear quadratic optimization problem with probabilistic constraints has been formulated. Moreover, the effects of surrounding conditions are considered in the selection of set of authentication factors as some of these may have dependence on the light (for example, face recognition), sound (for instance, voice recognition), etc. Brief descriptions regarding the surrounding conditions are given in Table IV.

Hence, to incorporate these realistic situations, a set of surroundings (S) can be constructed which is given as S= {Light (L), Sound and background noise (N), Motion (M), …}. Keeping this in mind, the above mentioned surrounding influences have been incorporated as constraints of the proposed multi-objective quadratic optimization model with probabilistic objective, which is given as follows:

Objectives:

$$\text{Maximize}\left(\mathrm{WD}_p * \mathrm{D}_p + \sum_j \mathrm{WM}_j * \mathrm{Me}_j\right) * \left\{\mathrm{TD}_p\left(\{\mathrm{M}_k\}: \{f_{k,i}\}\right) * \sum_j \mathrm{TMe}_j\left(\{\mathrm{M}_k\}: \{f_{k,i}\}\right)\right\}^{-\left|\left(\{\mathrm{M}_k\}: \{f_{k,i}\}\right)\right|} \quad (7)$$

$$\text{Minimize } P(X_t | X_{t-1}, X_{t-2}, X_{t-3} \dots X_1) \quad (8)$$

Subject to:

$$\left(\mathrm{D}_l - \mathrm{TD}_l\left(\{\mathrm{M}_k\}: \{f_{k,i}\}_i\right)_k\right)^2 + \sum_j \left(\mathrm{Me}_j - \mathrm{TMe}_j\left(\{\mathrm{M}_k\}: \{f_{k,i}\}_i\right)_k\right)^2 \le U_{max};$$

$$\text{where } \begin{pmatrix} a_1 \text{lux} \le \mathrm{L} \le a_2 \text{lux}; a_3 \text{ Hz} \le \mathrm{S} \le a_4 \text{Hz}; \\ \text{motion is within a sustainable range}; \{a_i\}_{i \in \mathbb{N}}, \end{pmatrix} \quad (9)$$

$$\left(\mathrm{D}_l - \mathrm{TD}_l\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_{k\neq 1,2,3,14,15}\right)^2 + \sum_j \left(\mathrm{Me}_j - \mathrm{TMe}_j\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_{k\neq 1,2,3,14,15}\right)^2 \leq U_{max}; \quad (10)$$

where (a_3 Hz ≤ S ≤ a_4Hz; motion is within a sustainable range)

...

$$\left(\mathrm{D}_l - \mathrm{TD}_l\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_{k\neq 1,2,3,9,14,15}\right)^2 + \sum_j \left(\mathrm{Me}_j - \mathrm{TMe}_j\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_{k\neq 1,2,3,9,14,15}\right)^2 \leq U_{max};$$

(where, motion is within a sustainable range) (11)

...

TABLE III: THE TRUSTWORTHY VALUES OF COMBINED FACTORS FROM INDIVIDUAL TRUSTWORTHY VALUES.

Features	Trustworthy Values					
	FD	PD	HD	WI	WL	CL
$(\mathrm{M}_1: f_{1,1}, \mathrm{M}_1: f_{1,2})$	2.72	2.81	3.1	2.78	2.79	3.21
$(\mathrm{M}_1: f_{1,1}, f_{1,2}, f_{1,3})$	3.15	2.99	2.97	2.57	2.71	0.99
...	...	...	...	...	...	...
$(\mathrm{M}_1: f_{1,1}, f_{1,2}, f_{1,3}, f_{1,4})$	3.57	3.79	3.19	2.61	2.75	0.99
$(\mathrm{M}_5: f_{5,1}, f_{5,2})$	3.95	3.94	3.97	3.73	2.78	0.97
$(\mathrm{M}_5: f_{5,1}, f_{5,3})$	3.90	2.89	3.79	3.79	3.69	3.79
$(\mathrm{M}_5: f_{5,1}, f_{5,2})$	3.95	3.94	3.97	3.73	2.78	0.97
...	...	...	...	...	...	...

TABLE IV: EFFECTS OF DIFFERENT SURROUNDING CONDITIONS ON THE PROPOSED SELECTION PROCEDURE

Surrounding Conditions	The acceptable range of surrounding conditions	Effected Modalities
Light (L)	The luminance of the light levels varies with indoor and outdoor conditions. The common light level falls in the range of 100-1000 lux	M_1, M_2
Sound and Background Noise (N)	The reasonable frequency range of audible sound is 20Hz – 20k Hz. Any sound with frequency less than 20Hz and above 20KHz cannot be heard by humans.	M_8
Motion (M)	The authentication factors are also dependent on the motion of the humans. But the detail analysis of the motion on different authentication factors is not found in the literature. This surrounding condition is incorporated in equations (9, 10 and 11) of adaptive selection approach. Proper adjustment (depend on the system requirements) can be made for the minimum and maximum allowed values of motion depending on the applications.	M_1, M_2, M_8

The multi-objective quadratic programming problem with probabilistic objective function can be used for selecting a set of authentication factors which satisfies different optimization criteria to do authentication. The proposed multi-objective quadratic programming problem with probabilistic objective has two objective functions. The first objective is designed to satisfy the higher trustworthy values of authentication factors with lesser number of total auth. factors. This joint effect of trustworthy values and cardinality of the factors are reflected in objective 1 (Equation 7). On the other hand, the second objective function (Equation 8) tries to reduce the probability of selecting the same set of authentication factors in successive authentication triggering times. The inclusion of this objective prevents the selection of authentication factors to follow any predictable pattern. Hence, it reduces the chance of compromising authentication selection patterns to the attackers.

Here $\mathrm{TD}_l\left(\{\mathrm{M}_k\}:\{f_{k,i}\}\right)$ and $\mathrm{TMe}_j\left(\{\mathrm{M}_k\}:\{f_{k,i}\}\right)$ are the trustworthy values of $\left(\{\mathrm{M}_k\}:\{f_{k,i}\}\right)$ in $l^{\mathrm{th}}; (l = 1,2,3)$ device and $j^{\mathrm{th}}; (j = 1,2,3)$ medium respectively. Moreover, $\left|\left(\{\mathrm{M}_k\}:\{f_{k,i}\}\right)\right|$ is the number of the selected set of authentication factors. WD_i and WM_j are the weights of the i^{th} device and j^{th} medium respectively. These weights can be calculated in the following way:

$$\mathrm{WD}_i = \frac{\text{Trustworthy value of usable authentication factors in } i^{\mathrm{th}}\text{device}}{\text{Trustworthy value of all the authentication factors in } i^{\mathrm{th}}\text{device}}$$

$$\mathrm{WM}_j = \frac{\text{Trustworthy value of usable authentication factors in } j^{\mathrm{th}}\text{medium}}{\text{Trustworthy value of all the authentication factors in } j^{\mathrm{th}}\text{medium}}$$

Again, according to the present work, 3.97 is the highest trustworthy value for any authentication factors (found in Table *II*). Hence, in equations 9-11, the value of U_{max} will be 3.97. Lastly, to make the selected set of authentication modalities unpredictable to the hackers, it is important that a new set of authentication factors becomes selected in comparison with previous selection and this criteria has been reflected in the second objective. Here, $\{X_t\}$ is the random variable that can be defined in the following way.

$$X_t = \left\{\left\{\mathrm{TD}_l\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_k\right\} * \left\{\mathrm{TMe}_j\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_k\right\}\right\}_t^{-|(\{\mathrm{M}_k\}:\{f_{k,i}\})|_t}$$

and its $(t-1)^{\mathrm{th}}$ occurrence can be defined as:

$$X_{t-1} = \left\{\left\{\mathrm{TD}_l\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_k\right\} * \left\{\mathrm{TMe}_j\left(\{\mathrm{M}_k\}:\{f_{k,i}\}_i\right)_k\right\}\right\}_{t-1}^{-|(\{\mathrm{M}_k\}:\{f_{k,i}\})|_{t-1}}$$

Here, X_t is the t^{th} observation of the random variable $\{X_t\}$.

Next, to achieve the goal of non-repetitive selection of authentication features (Objective 2, i.e., Equation 8) $P(X_t|X_{t-1}, X_{t-2}, X_{t-3} \ldots X_1)$ should be minimized. In the present work, the distribution of $\{X_t\}$ has been considered as

exponential [28] and, as a consequence, the second objective Minimize $P(X_t|X_{t-1}, X_{t-2}, X_{t-3} \ldots X_1)$ is, in turn, reduced to Minimize $P(X_t|X_{t-1})$ (due to the memory less or Markov property of the exponential distribution [28]).

VI. SIMULATIONS AND RESULTS

This section demonstrates the simulation results of the proposed selection approach of MFA. The results are listed in Table V. The table shows the nature of devices, media, surrounding conditions, and usable the set of authentication modalities for the selected environmental settings in the first four columns. Whereas, the next three columns show the selected set by the proposed method, random selection approach, and the optimal selection approach. Random selection approach chooses the authentication factors in a random manner as part of dynamic selection process. Optimal selection approach chooses the authentication factors based on the trustworthy factors only and does not consider the surrounding conditions and previous selected set of authentication factors. As our proposed approach is novel to provide adaptive selection, it is interesting to compare the performance of three selection approaches. For example, the first row of Table V shows that for a fixed device (with all the usable ten authentication modalities) and in a wired medium, the set of authentication modalities selected by the proposed selection method is $(\mathrm{M}_3; \mathrm{M}_4: f_{4,1}, f_{4,2})$. Whereas $(\mathrm{M}_1, \mathrm{M}_3, \mathrm{M}_9)$ and $(\mathrm{M}_4, \mathrm{M}_9)$ are the set of selected authentication factors for the random and the optimal selection approaches respectively. The other rows of the table can be interpreted in a similar way and in most of the cases the selected set of authentication factors by the optimal and random selection methods are mostly repeated. But, in the case of our proposed method, the selected set of authentication factors are not repeated, making the selection unpredictable to the hackers. It can be considered as a very significant advantage of the proposed strategy over its competitors.

The histogram plot (shown in Fig. 2) shows the comparison of the total trustworthy values of the selected set of authentication factors using the proposed selection procedure and the random and optimal selection strategies. Fig. 2 illustrates the effect of trustworthy values in different device and media combinations for the three selection strategies. It is clear from the figure that the adaptive selection outperforms the other two approaches in all the cases. Optimal selection approach in the best case performs as good as adaptive selection. Hence, with different setting of devices and media, adaptive selection approach performs better than optimal selection and random selection approaches.

The pictorial representation of the simulation results (see Fig. 3) can be consulted for a better and clearer understanding. The first layer shows different time triggering events when the adaptive selection approach will run. Different combinations of devices and media are shown in next two layers. The fourth layer mentions the different surrounding conditions. The possible set of authentication factors are listed in the last layer. For example, in t_1 triggering time, FD and WI are selected and surrounding conditions (light (*L*), motion (*M*), and sound & background noise (*N*)) are not good. Then $\mathrm{M}_3; \mathrm{M}_4: f_{4,1}, f_{4,2}$ is selected by the adaptive selection approach. In other time triggering events with different combination of device, medium, and surrounding condition, the adaptive selection approach provides different set of authentication factors as solutions.

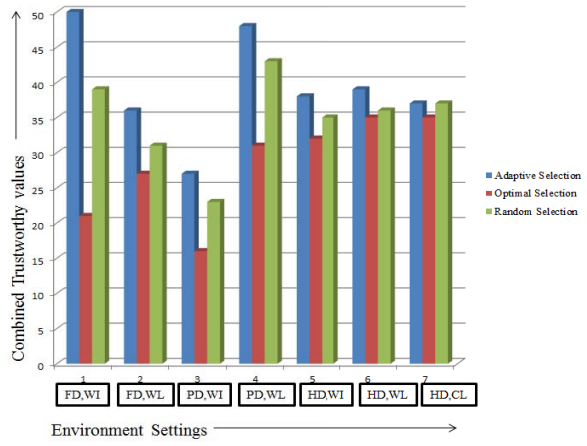

Fig. 2. Comparisons among the proposed adaptive selection, optimal selection, and the random selection approaches.

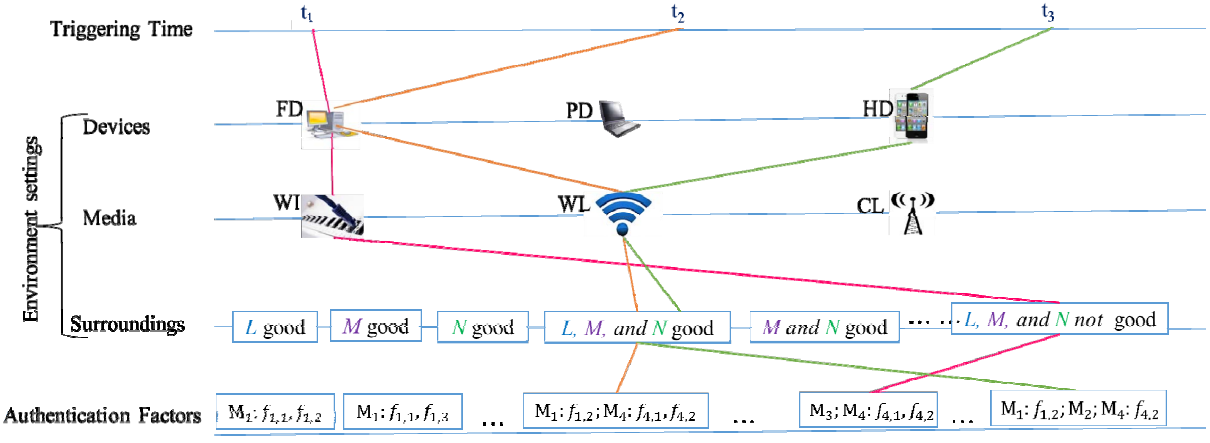

Fig. 3.
Sample scenarios of adaptive selection of the set of authentication factors in different device, media and surrounding conditions with varying time.

TABLE V SAMPLE OUTCOMES OF THE PROPOSED MULTI FACTOR AUTHENTICATION METHOD.

Device	Media	Surrounding Conditions	Set of Usable Authentication Factors	Selected Sets of Authentication Factors		
				Proposed system	Random Selection	Optimal Selection
FD	WI	L, N, M not good	$M_1, M_2, \dots, M_{10}$	$M_3; M_4: f_{4,1}, f_{4,2}$	M_1, M_3, M_9	M_5, M_9
FD	WI	L, M, N good	$M_1, \dots, M_4, M_5, M_7, M_8, \dots, M_{10}$	$M_2; M_3; M_4: f_{4,2}$	M_1, M_3, M_9	M_1, M_9
FD	WI	L, M, N good	$M_1, M_2, \dots, M_3, M_7, \dots, M_9$	$M_1; M_2;\ M_4: f_{4,1}, f_{4,2}$	M_1, M_4, M_9	M_1, M_3
...	...		...	...	...	...
FD	WL	L, M, N good	$M_1, M_2, \dots, M_{10}$	$M_1: f_{1,2};\ M_4: f_{4,1}, f_{4,2}$	M_1, M_5, M_9	M_1, M_3, M_{10}
FD	WL	L, M, N good	$M_1, M_2, \dots, M_4, M_5, M_7, M_8, \dots, M_{10}$	$M_1: f_{1,2}; M_2;\ M_4: f_{4,2}$	M_1, M_5, M_{10-}	M_1, M_3, M_{10}
...	...		...	...	...	...
PD	WL	L, M, N not good	$M_1, M_2, \dots, M_{10}$	$M_4: f_{4,1}, f_{4,2}$	M_1, M_3, M_8	M_1, M_3, M_{10}
PD	WL	L, M, N not good	$M_1, M_2, \dots, M_4, M_5, M_7, M_8, \dots, M_{10}$	M_4, M_{10}	M_2, M_3, M_8	M_1, M_3, M_{10}
...	...		...	...	...	...
HD	WL	L, M, N good	$M_1, M_2, \dots, M_{10}$	$M_1: f_{1,2};\ M_4: f_{4,1}, f_{4,2}$	M_1, M_3, M_7	M_1, M_2, M_4
HD	WL	L, M, N good	$M_1, M_2, \dots, M_4, M_5, M_7, M_8, \dots, M_{10}$	$M_1: f_{1,2}; M_2;\ M_4: f_{4,2}$	M_1, M_5, M_7	M_1, M_3, M_{10}
...	...	…	...	…	...	...

TABLE VI COMPARISON OF THE ADAPTIVE MFA WITH EXISTING MULTI-FACTOR AUTHENTICATION APPROACHES

Different Approaches	Factor Considered	Selection Strategy for Multi-factor	Applicability
Cognitive-centric Text Production and Revision Features [29]	Multi-factor: Behavioral Biometric and keystroke dynamics	Fusion of all features	All devices
Context Aware/gait based [3]	Single Factor: Behavioral Biometric	None	Mobile Devices
Typing Motion Behavior [17]	Single Factor: Behavioral Biometric using statistical features	None	Mobile Devices
Temporal Authentication [21]	Multi-factor: Face Detection and Body Localization	both factors individually	Fixed and Portable Devices
Messaging App Usage [24]	Single Factor: Behavioral Biometrics	None	Mobile Devices
Touch Screen Gestures [23]	Single Factor: Behavioral Biometrics with finger gestures	None	Mobile Devices
Keystroke Dynamics [20]	Single Factor: Behavioral Biometrics	None	All devices
Behavioral Biometrics [10]	Multi-factor: Keyboard, mouse, and application interactions	Fusion of three features in a trust model	Fixed and Portable Devices
Proposed Adaptive MFA Approach	Multi-factor: Behavioral biometrics, physiological biometrics, password, SMS, and captcha. Present work considers every individual authentication modalities and their different features. Hence, two features of the same modality can be considered as two different factors in the selection process.	Adaptive selection of multiple factors sensing the environment conditions	All Devices

VII. QUALITATIVE COMPARISONS WITH OTHER MFA APPROACHES

There are different MFA approaches which support continuous authentication of users. .Table VI listed a comparison of some other existing approaches to our proposed approach. From the table, it is clear that our proposed adaptive approach differs significantly from the other existing approaches. None of the other listed approaches use an adaptive approach as part of their selection strategy. Many of these approaches choose static selection strategies that consider all the factors at the same time. Again, some approaches are applicable to fixed and portable devices while others are applicable to mobile devices only. Our proposed approach is applicable to all three different types of devices and provides the selection decision adaptively sensing the devices, media and surrounding conditions.

VIII. CONCLUSION AND FUTURE WORKS

This work focuses on designing a just-in-time authentication strategy using multiple authentication factors (modalities along with their several features) in order to provide a trustworthy, resilient, and scalable solution for authentication. The proposed trustworthy model computes the trustworthy values for different authentication factors by considering several probabilistic constraints. In particular, it uses pair-wise comparisons among different devices and media. The adaptive selection scheme makes intelligent decisions, choosing authentication factors at run-time by considering the performance, trustworthy values, and the history of the previous selection of the available factors. This approach also avoids repeated selections of the same set of authentication factors in successive re-authentication attempts, thereby reducing the chance of establishing any recognizable patterns. Therefore, no prior information regarding the selected set of authentication factors is available for potential attackers to exploit. Again, the proposed selection mechanism considers individual features of a modality as different authentication factors and hence, the search space of the selection procedure becomes relatively large. This criterion ensures the selection of non-repetitive sets of authentication factors for different authentication triggering times.

A usability study will be conducted in the future to calculate subjective trustworthy values of authentication factors.

Furthermore, users' preferences on different authentication factors will also be considered as another objective in adaptive selection procedures. Other techniques for calculating the trustworthy factors will also be explored in the future as an extension of this research.

REFERENCES

[1] G. Parziale and Y. Chen, "Advanced technologies for touchless fingerprint recognition," in Handbook of Remote Biometrics. Springer, 2009, pp. 83–109.

[2] V. Patel, T. Yeh, M. Salem, Y. Zhang, Y. Chen, R. Chellappa, and L. Davis, "Screen fingerprints: a novel modality for active authentication," 2013.

[3] A. Primo, V. V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements," in Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on. IEEE, 2014, pp. 98–105.

[4] A. Serwadda, S. Govindarajan, R. Pokala, Z. Wang, P. Koch, K. Balagani,V. Phoha, A. Goodkind, A. Rosenberg, and D. G. Brizan, "Scanbased evaluation of continuous keystroke authentication systems," IT Professional, p. 1, 2013.

[5] J. C. Stewart, J. V. Monaco, S.-H. Cha, and C. C. Tappert, "An investigation of keystroke and stylometry traits for authenticating online test takers," in Biometrics (IJCB), 2011 International Joint Conference on. IEEE, 2011, pp. 1–7.

[6] C. Vielhauer, Biometric user authentication for IT security: from fundamentals to handwriting. Springer, 2005, vol. 18.

[7] A. K. Nag and D. Dasgupta, "An adaptive approach for continuous multi-factor authentication in an identity eco-system," in Proceedings of the 9th Annual Cyber and Information Security Research Conference. ACM, 2014, pp. 65–68.

[8] A. K. Nag, D. Dasgupta, and K. Deb, "An adaptive approach for active multi-factor authentication," in 9th Annual Symposium on Information Assurance (ASIA14), 2014, pp. 39.

[9] D. G. Luenberger and Y. Ye, Linear and nonlinear programming. Springer, 2008, vol. 116.

[10] I. Deutschmann and J. Lindholm, "Behavioral biometrics for darpa's active authentication program," in Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the. IEEE, 2013, pp.1–8.

[11] M. Brennan, S. Afroz, and R. Greenstadt, "Adversarial stylometry: Circumventing authorship recognition to preserve privacy and anonymity,"ACM Transactions on Information and System Security (TISSEC), vol. 15, no. 3, p. 12, 2012.

[12] M. Abramson and D. W. Aha, "User authentication from web browsing behavior." in FLAIRS Conference, 2013.

[13] K. Kwok, "User identification and characterization from web browsing behavior," DTIC Document, Tech. Rep., 2012.

[14] J. Feng and A. K. Jain, "Fingerprint reconstruction: from minutiae to phase," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 33, no. 2, pp. 209–223, 2011.

[15] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identityauthentication system using fingerprints," Proceedings of the IEEE, vol. 85, no. 9, pp. 1365–1388, 1997.

[16] A. K. Jain, J. Feng, and K. Nandakumar, "Fingerprint matching," Computer, vol. 43, no. 2, pp. 36–44, 2010.

[17] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior." In Sicherheit, 2014, pp. 1–12.

[18] J. V. Monaco, J. C. Stewart, S.-H. Cha, and C. C. Tappert, "Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works," in Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on. IEEE, 2013, pp. 1–8.

[19] R. P. Guidorizzi, "Security: Active authentication," IT Professional, vol. 15, no. 4, pp. 4–7, 2013.

[20] D. Gunetti and C. Picardi, "Keystroke analysis of free text," ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 3, pp. 312–347, 2005.

[21] K. Niinuma and A. K. Jain, "Continuous user authentication using temporal information," in SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 2010, pp. 76 670L–76 670L.

[22] K. Revett, H. Jahankhani, S. T. de Magalh˜aes, and H. M. Santos, "A survey of user authentication based on mouse dynamics," in Global E-Security. Springer, 2008, pp. 210–219.

[23] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in Homeland Security (HST), 2012 IEEE Conference on Technologies for. IEEE, 2012, pp. 451–456.

[24] E. Klieme, K.-P. Engelbrecht, and S. M¨oller, "Poster: Towards continuous authentication based on mobile messaging app usage."

[25] B. D. Lucas, T. Kanade et al., "An iterative image registration technique with an application to stereo vision." in IJCAI, vol. 81, 1981, pp. 674–679.

[26] J. Kang, D. Nyang, and K. Lee, "Two-factor face authentication using matrix permutation transformation and a user password," Information Sciences, vol. 269, pp. 1–20, 2014.

[27] S. Dunn and S. Peucker, "Genetic algorithm optimisation of mathematical models using distributed computing," in Developments in Applied Artificial Intelligence. Springer, 2002, pp. 220–231.

[28] K. Balakrishnan, Exponential distribution: theory, methods and applications. CRC press, 1996.

[29] H. Locklear, S. Govindarajan, Z. Sitov´a, A. Goodkind, D. G. Brizan, A. Rosenberg, V. V. Phoha, P. Gasti, and K. S. Balagani, "Continuous authentication with cognition-centric text production and revision features."

[30] S. K. Saha, A. K. Nag, and D. Dasgupta. "Human-Cognition-Based CAPTCHAs" , IT Professional 17, no. 5, 2015. Pp. 42-48.