Multi-factor authentication for wearables

Multi-factor Authentication for Wearables: Configuring System Parameters with Risk Function

Sergey Bezzateev
ITMO University
Saint Petersburg, Russia
bsv@aanet.ru

Aleksandr Ometov
Tampere University of Technology
Tampere, Finland
aleksandr.ometov@tut.fi

Aleksandra Afanasyeva
State University of Aerospace Instrumentation
Saint Petersburg, Russia
alra@vu.spb.ru

Natalia Voloshina
ITMO University
Saint Petersburg, Russia
nataliv@ya.ru

ABSTRACT

The users of today are already about to enter the era of highly integrated modern wearable devices – the time when smart accessories will, in turn, push aside regular Smartphones and Tablets bringing a variety of new security challenges. The number of simultaneously used bio-sensors, both integrated into smart wearables and connected over wireless interfaces, allows novel opportunities for Multi-factor Authentication (MFA) of the user. This manuscript proposes a solution for configuring the MFA based on the average direct and indirect losses risk analysis. The example application of Bayesian function for MFA presents the applicability of the proposed framework for the utilization with wearables.

CCS CONCEPTS

• **Security and privacy → Multi-factor authentication**; • **Theory of computation → Cryptographic protocols**; • **Hardware** → *Sensor devices and platforms*; *Tactile and hand-based interfaces*; *Sensors and actuators*;

KEYWORDS

Wearables, multi-factor authentication, risk function, information security

1 INTRODUCTION

Today, wearable devices have already taken their niche within the Internet of Things (IoT) paradigm development process [14, 22]. The decrease in the electrical components price and growing popularity of smart wearable electronics thus lead to the expectation of worn devices market to reach $53.2 billion by 2019[1]. The primary sale targets are related to the realization of smartwatches and augmented reality glasses while bringing some significant scenarios to the research community attention [2, 16]. At the same time, the shift towards wearable electronics from conventional smartphones is accompanied by a variety of privacy and safety concerns [5, 9, 23]. The need for robust security frameworks capable of being executed directly on resource constrained devices is now required more than ever before [11, 13].

Evidently, one of the heading security topics is authentication[2]. The following conditions are to be fulfilled for the next-generation authentication frameworks: (i) the authentication protocol should be as user-friendly and straightforward as possible, and (ii) it should be as difficult to be compromised as possible for the attacker at the same time [21].

One of the ways to address these challenges is by utilizing various biometric information being always available to a legitimate user but complicated in forging it [20]. Recently, the possibility to utilize biometric sensors connected to "smart" devices and measuring various human parameters emerged due to broad adoption of the IoT paradigm [7, 15, 18].

In contrast, most of the modern authentication systems utilizing biometrics have a nonzero error probability of the user to: (i) false accepted, or (ii) false rejected. *False Acceptance Rate* (FAR) and *False Rejection Rate* (FRR) parameters are utilized to estimate the probabilities of the corresponding operation errors [1]. The use of multi-factor authentication (MFA) protocols was recommended to obtain an arbitrarily small (i.e., more acceptable) value for these parameters [10]. Such protocols analyze the combined data obtained from several independent sensors for the utilization in the authentication process [6].

The number of works related to this topic is vast [4, 8, 17, 19], here the systems differ based on the set of authentication factors

[1] "Now is the Time to Design for Wearables", by Awwards, 2016: https://www.awwwards.com/now-is-the-time-to-design-for-wearables.html
[2] "Dev Security: Authentication Is More Important Than Ever in 2017", by DZone, 2017: https://dzone.com/articles/authentication-is-more-important-than-ever-in-2017

and in the way of combining the results of independent measurements. While grouping the information obtained with multiple sensors, conventional problems from the field of multi-parametric comparison arise due to potential incomparability of the results obtained from different sensors. Therefore, the analysis of the success and/or failure grouping is reached with FAR and FRR.

In this manuscript, authors propose to utilize the *risk function*, well-known from financial operations and banking systems, for the estimation of authentication system conditions. It allows obtaining the result in the financial losses forecast form. The desired parameters of authentication system (FAR and FRR) are utilized to estimate the proposed risk function. Due to the dependency of FAR and FRR on the selected decision function parameters, the resulting risk function has a direct relation as well. This work proposes a methodology allowing to "adjust" the system parameters according to acceptable losses based on the defined risk policy.

The rest of the manuscript is organized as follows. Section 2 provides the general overview of the proposed system model. Further, Section 3 shortly introduces the risk function and its applicability to the problem of interest. Section 4 discusses the solution based on the Bayesian function. Next section provides the numerical results. Further in Section 6, we briefly discuss the benefits and limitations of the proposed model. The conclusions are given in the last section.

2 THE PROPOSED MULTI-FACTOR AUTHENTICATION SYSTEM

This section describes the concept of the multi-factor authentication system and provides the classification of terms utilized among the lines of this manuscript.

In this work, we assume that there might be two possible decisions made during the user authentication process: (i) H_0 – illegitimate user, and (ii) H_1 – legitimate user.

These hypotheses are mutually exclusive and collectively exhaustive events, so they form the entire sample space as

$$P(H_0) + P(H_1) = 1. \tag{1}$$

The a priori probability distribution of these two cases is further represented by the corresponding values $P(H_0)$ and $P(H_1)$ determined by the risk policy of the authentication system owner. These probabilities are considered as the *configuration parameters* of the system.

We assume that there are n sensors delivering the MFA related data in the system. These sensors measure various biometric parameters representing the *factors*. Today, there are two common methods utilized for combining the results of sensors' measurements [12] listed as follows:

- *Method A:* Each sensor can independently decide whether to authenticate the user based only on its data and return the acceptance or to send the rejection reply. The decision function is responsible for intelligent combining the results followed by the group decision based on the vector, i.e., the weighted decision or preset threshold could be utilized based on the selected sensor;
- *Method B:* The sensor replies with 'raw' results of its measurements and corresponding probabilistic characteristics. At the next step, the data is combined to be utilized during the final decision process. Thus, the whole set of the collected data could be considered during the group decision process.

Each individual sensor measurement from the set $X = \{x_1, \ldots, x_n\}$ is distributed $[0, 1]$ and the corresponding vector is next analyzed based on the considerations given before.

The type A sensor will return the value x'_i from the set $\{0; 1\}$, based on the results of its decision, which corresponds to the binary solutions, i.e., either *YES* or *NO*. Therefore, the conditional probabilities $P\left(x'_i|H_0\right)$ and $P\left(x'_i|H_1\right)$ are defined by FAR_i and FRR_i values, while being calculated for i-th sensor. The values of FAR_i and FRR_i are taken at the point x_i where $FAR_i = FRR_i$.

The B type sensor returns the result of the measured parameter and the template comparison in the form of a match score x'_i *in* $[0, 1]$. For each of the values x'_i, conditional probability $P\left(x'_i|H_0\right)$ is calculated based on the FAR_i values at x'_i. And conditional probability $P\left(x'_i|H_1\right)$ is determined by FRR_i values at x'_i.

The proposed methodology allows to analyze the A type sensor as a particular model type B case, if FAR_i and FRR_i are given only in one point, and the measurement result can take only two values, i.e., lower or higher than the selected threshold.

In this paper, we consider a more general case of a method B, and the combination of the measurement results for individual sensors are made similarly to previous works by using of the Bayes decision function [3]. Since the results of measurements have the probabilistic nature, the decision function is suitable for the maximum a posteriori probability solution. The general model of the system is represented in Figure 1.

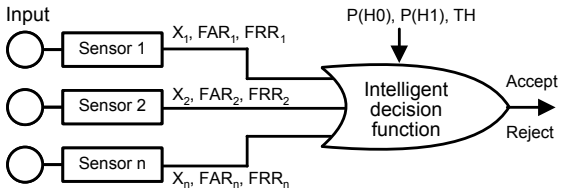


Figure 1: Multi-factor authentication system model with TH as a decision threshold

Next, we describe the decision function. The conditional probability of the measured value from each sensor $P\left(x'_i|H_0\right)$ and $P\left(x'_i|H_1\right)$ and the a priori probabilities of the hypotheses $P(H_0)$ and $P(H_1)$ are given as an input. Further, the decision function evaluates the a posteriori probability of the hypothesis $P(H_1|X)$ and validates that this probability is higher compared to TH being a threshold.

The measured conditional probabilities are considered as independent random variables, and the conditional probability can be presented as follows

$$P\left(X'|H_J\right) = \prod_{x'_i \in X'} P\left(x'_i|H_J\right), J \in \{0; 1\}. \tag{2}$$

Further, the total probability $P(X')$ is

$$P(X') = \prod_{x'_i \in X'} P\left(x'_i \,|H_0\right)P(H_0) + \prod_{x'_i \in X'} P\left(x'_i \,|H_1\right)P(H_1). \quad (3)$$

The total probability is further calculated based on the conditional probabilities with $P\left(x'_i \,|H_J\right)$, where $J \in \{0; 1\}$ are known from the sensors specification, $P(H_0)$ and $P(H_1)$ are a priori probabilities.

Based on the obtained results, the posterior probability for each hypothesis $H_J, J \in \{0; 1\}$ can be estimated as

$$P\left(H_1 \,|X'\right) = \frac{\prod_{x'_i \in X'} P\left(x'_i \,|H_1\right)P(H_1)}{P(X')}. \quad (4)$$

Thus, for a group decision,

$$P\left(H_1 \,|X'\right) > TH \Rightarrow \{Access\}, \text{ else } \{Reject\}. \quad (5)$$

As a result, the decision may be either correct or may lead to an error. The FAR and FRR error probabilities could be estimated for each system [4, 19], but it is still unclear – which system or particular sensors should be utilized by the end-user. The answer to this question could be obtained based on the risk function allowing to estimate the financial result from the separate system utilization perspective. Also, it also allows obtaining the optimal values for the system parameters, i.e., to select the threshold value TH, which minimizes the risks.

3 RISK FUNCTION DEFINITION

The risk analysis is based on the obtained FAR and FRR values. In case the average transaction cost (*AvCost*) and FAR are known, then the Average Direct Losses (ADL) could be calculated as

$$ADL = AvCost \cdot FAR \cdot n, \quad (6)$$

where n is a number of transactions. On the other hand, Average Indirect Losses (AIL) could be evaluated based on both FRR and average indirect transaction cost (*AilCost*)

$$AIL = AilCost \cdot FRR \cdot n. \quad (7)$$

By this means, the risk analysis could be based on the sum of AIL and ADL with the risk function,

$$RF = ADL + AIL. \quad (8)$$

This function could be utilized to compare existing MFA systems with known FAR and FRR, as well as for configuring the systems with Bayesian function-based optimization.

4 PARAMETERS OPTIMIZATION FOR BAYESIAN FUNCTION

Any business model involves minimizing the risk of financial loss as a natural way to obtain the optimal parameters of the system. Therefore, we formulate the optimization problem as

$$\begin{aligned} &RF = ADL + AIL \rightarrow \min, \\ &AvCost \cdot FAR + AilCost \cdot FRR \rightarrow \min, \end{aligned} \quad (9)$$

where $FAR_i(x), FRR_i(x)$ are functions of the sensor probability characteristics, $P(H_1), P(H_0)$ are the a priori distribution of the hypotheses probabilities, and TH is the threshold utilized for the decision making process. Since $FAR_i(x), FRR_i(x), P(H_1), P(H_0)$ are fixed for each implementation of the system, TH is the only parameter that may be affected during the optimization.

FAR corresponds to the case if the posterior probability $P\left(H_1 \,|X'\right)$ is greater than the decision threshold TH under the hypothesis H_0

$$FAR = Prob\left\{P\left(H_1 \,|X'\right) \geq TH \,|H_0\right\}. \quad (10)$$

The value of $P\left(H_1 \,|X'\right)$ can be expressed in terms of the sensor characteristics. Since $FRR_i(x'_i) = Prob(x_i < x'_i \,|H_1)$, then $FRR_i(x'_i)$ can be considered as empirical distribution $F^*_i(x_i \,|H_1)$. Then the value of $P(x'_i \,|H_1) = \frac{\partial F^*_i}{\partial x'_i}$. The empirical function F^*_i is presented in tabular form for each x_i, it could be constructed based on the results of the experiments with individual sensors. Next, it could be differentiated numerically $P(x'_i \,|H_1) = \frac{\Delta FRR_i(x'_i)}{\Delta x'_i}$. For brevity, we denote the $P(x'_i \,|H_1) = FRR'_i(x'_i)$.

Similarly, we consider

$$FAR_i(x'_i) = Prob(x_i \geq x'_i \,|H_0) = 1 - Prob(x_i < x'_i \,|H_0), \quad (11)$$

and, hence, $1 - FAR_i(x'_i)$ can be considered as empirical distribution function $F^*_i(x_i \,|H_0)$ of the random variable x_i. Then the value of $P(x'_i \,|H_0) = -\frac{\partial F^*_i}{\partial x'_i}$. Since empirical function F^*_i is presented in tabular form, built on the results of the experiments with individual sensors, then it can only be differentiated numerically

$$P(x'_i \,|H_0) = -\frac{\Delta FAR_i(x'_i)}{\Delta x'_i}. \quad (12)$$

For brevity we denote $P(x'_i \,|H_0) = -FAR'_i(x'_i)$. Therefore, it could be represented as

$$P\left(H_1 \,|X'\right) = \frac{\prod_{x'_i \in X'} FRR'_i(x'_i)P(H_1)}{\prod_{x'_i \in X'}(-FAR'_i(x'_i))P(H_0) + \prod_{x'_i \in X'} FRR'_i(x'_i)P(H_1)}. \quad (13)$$

FRR describes the case when the posterior probability $P\left(H_1 \,|X'\right)$ is less than the decision threshold TH under the hypothesis H_1, i.e.,

$$FRR = Prob\left\{P\left(H_1 \,|X'\right) < TH \,|H_1\right\}, \quad (14)$$

where, total probability $P\left(H_1 \,|X'\right) < TH$ is

$$\begin{aligned} &Prob\left\{P\left(H_1 \,|X'\right) < TH\right\} = \\ &Prob\left\{P\left(H_1 \,|X'\right) < TH \,|H_1\right\} \cdot P(H_1) + \\ &Prob\left\{P\left(H_1 \,|X'\right) < TH \,|H_0\right\} \cdot P(H_0) = \\ &FRR \cdot P(H_1) + (1 - FAR) \cdot P(H_0). \end{aligned} \quad (15)$$

Let us introduce the following notation $P\left(H_1 \,|X'\right) = Y = g(X')$, then we can modify the equation (15) as

$$\begin{aligned} Prob\{Y < TH\} &= FRR \cdot P(H_1) + (1 - FAR) \cdot P(H_0) \\ &= FRR \cdot P(H_1) + P(H_0) - FAR \cdot P(H_0), \end{aligned} \quad (16)$$

where Y is a random variable that can be expressed in terms of FAR_i and FRR_i, and $Prob\{Y < TH\}$ is it's cumulative distribution function at TH. It can be evaluated empirically based on values of FAR_i and FRR_i as the restriction of a linear optimization function

$$AvCost \cdot FAR + AilCost \cdot FRR \rightarrow \min. \quad (17)$$

Substituting all previous results in the optimization function, we obtain

$$FAR = \frac{FRR \cdot P(H_1) + P(H_0) - Prob\{Y < TH\}}{P(H_0)}, \quad (18)$$

$$
\begin{aligned}
L =& AvCost\frac{FRR\cdot P(H_1) - Prob\{Y < TH\}}{P(H_0)} + \\
& AvCost + AilCost\cdot FRR \rightarrow \min, \\
L =& FRR\frac{AvCost\ P(H_1)}{P(H_0)} - \frac{Prob\{Y < TH\}\ AvCost}{P(H_0)} + \\
& AvCost + AilCost\cdot FRR = \\
& FRR\left(AvCost\frac{P(H_1)}{P(H_0)} + AilCost\right) - \\
& Prob\{Y < TH\}\ \frac{AvCost}{P(H_0)} + AvCost.
\end{aligned}
\tag{19}
$$

To solve the optimization problem, it is required to obtain the derivative of this expression concerning TH. The probability $Prob\{Y < TH\}$ can be considered as a value of the cumulative distribution function $F(Y)$ at TH

$$
\begin{aligned}
\frac{\partial L}{\partial TH} =& \left(AvCost\frac{P(H_1)}{P(H_0)} + AilCost\right)\cdot\frac{\partial FRR}{\partial TH} + \\
& \frac{AvCost}{P(H_0)}\cdot\frac{\partial F(TH)}{\partial TH} = 0.
\end{aligned}
\tag{20}
$$

FRR is a function of the TH, and it can be represented as follows

$$
\begin{aligned}
FRR =& Prob\left\{P\left(H_1\left|X'\right.\right) < TH\,|H_1\right\} = \\
& F(P\left(H_1\left|X'\right.\right) = TH|H_1) = F(TH|H_1).
\end{aligned}
\tag{21}
$$

Substituting (15) in the derivative, we obtain

$$
\begin{aligned}
\frac{\partial L}{\partial TH} =& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{P(H_0)}\cdot\frac{\partial F(TH|H_1)}{\partial TH} - \\
& \frac{AvCost}{P(H_0)}\cdot\frac{\partial F(TH)}{\partial TH}.
\end{aligned}
\tag{22}
$$

The derivative of the cumulative probability function is the probability density function of the integrand so that we can deliver the following

$$
\begin{aligned}
\frac{\partial L}{\partial TH} =& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{P(H_0)}\cdot f(TH|H_1) - \\
& \frac{AvCost}{P(H_0)}\cdot f(TH).
\end{aligned}
\tag{23}
$$

Next, it is required to obtain the probability density functions $f(TH)$ and $f(TH|H_1)$ to solve the resulting equation. There are two possible ways for the estimation:

- *Theoretical estimation*: Since $Y = g(X)$, where X is a random variable with known probability density function, that if $g^{-1}(Y)$ is continuous and differentiable in Y, we can express the probability density function $f(Y)$ and $f(Y|H_1)$ by $f(X)$ and $f(X|H_1)$ respectively.
- *Empirical estimation*: On the other hand, Y can be considered as an independent random variable; then its probability density can be estimated using empirical frequency histogram. It can be done based on the known FAR_i and FRR_i.

In following subsections, we consider previously discussed approaches independently.

4.1 Theoretical estimation

If (i) $g(\bar{X})$ (interconnecting two random variables $\bar{X}$ and Y) is known, reversible and inverse, and (ii) function $g^{-1}(Y)$ is differentiable on Y, it is possible to express the unknown probability density of the random variable Y in terms of known density for the $\bar{X}$

$$
\begin{aligned}
f(Y) &= \frac{\partial g^{-1}(Y)}{\partial Y} f(g^{-1}(Y)), \\
f(Y|H_1) &= \frac{\partial g^{-1}(Y)}{\partial Y} f(g^{-1}(Y)|H_1).
\end{aligned}
\tag{24}
$$

Then, the solution can be obtained explicitly from the following calculations

$$
\begin{aligned}
\frac{\partial L}{\partial TH} =& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{P(H_0)}\frac{\partial g^{-1}(Y)}{\partial Y} \\
& f(g^{-1}(Y)|H_1) - \frac{AvCost}{P(H_0)}\cdot\frac{\partial g^{-1}(Y)}{\partial Y} f(g^{-1}(Y)) = 0, \\
& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{P(H_0)} f(g^{-1}(Y)|H_1) = \\
& \frac{AvCost}{P(H_0)}\cdot f(g^{-1}(Y)), \\
\frac{f(g^{-1}(Y))}{f(g^{-1}(Y)|H_1)} =& \frac{P(H_0)}{AvCost}\cdot\frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{P(H_0)}, \\
& \frac{f(g^{-1}(Y)|H_0)P(H_0) + f(g^{-1}(Y)|H_1)P(H_1)}{f(g^{-1}(Y)|H_1)} = \\
& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{AvCost}, \\
\frac{f(g^{-1}(Y)|H_0)}{f(g^{-1}(Y)|H_1)} =& \frac{AilCost}{AvCost}.
\end{aligned}
\tag{25}
$$

Finally, the optimal value of decision threshold TH_{out} can be found by solving the equation (25) for Y.

4.2 Empirical estimation

An empirical estimate of $f(Y)$ and $f(Y|H_1)$ through the histogram of frequencies $\hat{f}(Y)$ and $\hat{f}(Y|H_1)$ can be applied to find the solution for the optimization problem. A sum of the different vectors probabilities X (if the calculated value Y is equal) is selected as a frequency falling within the range of each value in the histogram of frequencies. Known values of FAR_i and FRR_i are used for the histogram construction

$$
\begin{aligned}
& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{P(H_0)} f(TH|H_1) - \frac{AvCost}{P(H_0)}\cdot f(TH) = 0, \\
& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{P(H_0)} f(TH|H_1) = \frac{AvCost}{P(H_0)}\cdot f(TH), \\
& \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{AvCost} = \frac{f(TH)}{f(TH|H_1)}.
\end{aligned}
\tag{26}
$$

Therefore, the optimization function is

$$
\frac{\hat{f}(Y)}{\hat{f}(Y|H_1)} = \frac{AilCost\cdot P(H_0) + AvCost\cdot P(H_1)}{AvCost}
\tag{27}
$$

with respect to Y, and obtain the value of $Y = TH_{out}$.

5 NUMERICAL EXAMPLE

Let us consider the algorithm execution for a specific example. In this manuscript, we assume that there are three sensors with different error probabilities utilized. Confidence level is specified by probability $P(H_1) = 0.6$, the importance of risk to participants in the system is set to $AvCost = AilCost = 0.5$. Figure 2 shows the measured values of the errors FAR_i and FRR_i probabilities for x.

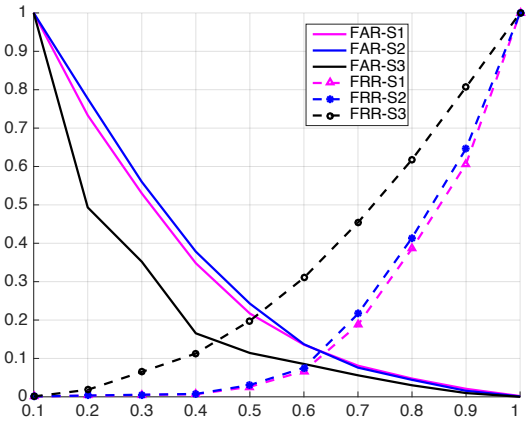


Figure 2: Analytical curves for FAR and FFR for three sensors

All the possible values $Y = P(H_1|X')$ are calculated to estimate $\hat{f}(Y)$ and $\hat{f}(Y|H_1)$ as

$$Y = P(H_1|X') = \frac{\prod_{x'_i \in X'} FRR'_i(x'_i)P(H_1)}{\prod_{x'_i \in X'} -FAR'_i(x'_i)P(H_0) + \prod_{x'_i \in X'} FRR'_i(x'_i)P(H_1)}, \quad (28)$$

where X' is taking all possible triples of values

$$\{x_1, x_2, x_3\}, x_i \in \{0.1; 0.2; 0.3; 0.4; 0.5; 0.6; 0.7; 0.8; 0.9; 1\}. \quad (29)$$

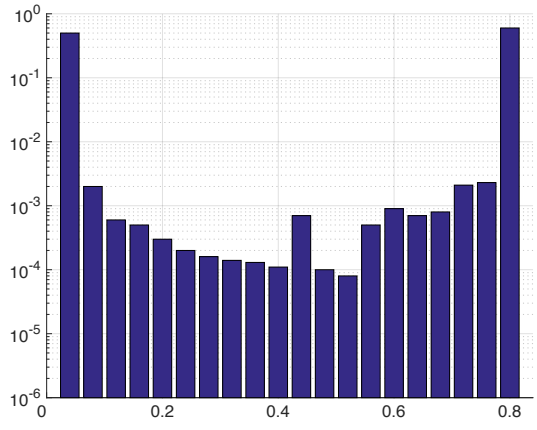
For vector $X' = \{0.1, 0.1, 0.1\}$ the following result is obtained

$$\begin{aligned} Y =& \frac{Y1}{Y2} = 0.0001042856994, \\ Y1 =& \Delta FRR_1(0.1) \cdot \Delta FRR_2(0.1) \cdot \Delta FRR_3(0.1) \cdot P_1 = \\ & (0.001 - 0)(0.001 - 0)(0.01 - 0) \cdot 0.6, \\ Y2 =& \Delta FRR_1(0.1) \cdot \Delta FRR_2(0.1) \cdot \Delta FRR_3(0.1) \cdot P_1 \\ & + \Delta FAR_1(0.1) \cdot \Delta FAR_2(0.1) \cdot \Delta FAR_3(0.1) \cdot P_0 = \\ & (0.001 - 0)(0.001 - 0)(0.01 - 0)0.6 + \\ & (1 - 0.5)(1 - 0.7)(0.99 - 0.3) \cdot 0.4. \end{aligned} \quad (30)$$

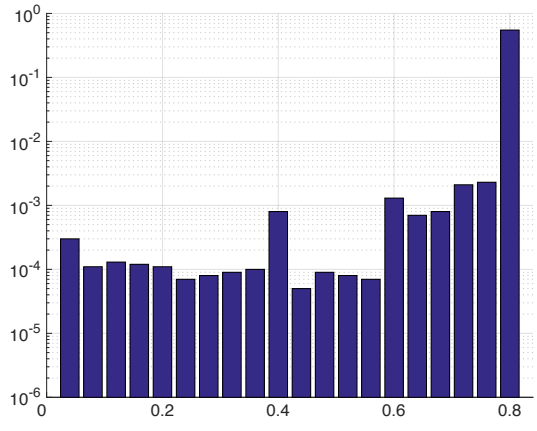
The given probabilities are estimated as follows

$$\begin{aligned} P(Y) =& \Delta FRR_1(0.1) \cdot \Delta FRR_2(0.1) \cdot \Delta FRR_3(0.1) \cdot P_1 + \\ & \Delta FAR_1(0.1) \cdot \Delta FAR_2(0.1) \cdot \Delta FAR_3(0.1) \cdot P_0 = \\ & (0.001 - 0)(0.001 - 0)(0.01 - 0)0.6 + \\ & (1 - 0.5)(1 - 0.7)(0.99 - 0.3)0.4 = 0.042000006, \\ P(Y|H_1) =& \Delta FRR_1(0.1) \cdot \Delta FRR_2(0.1) \cdot \Delta FRR_3(0.1) \cdot P_1 = \\ & (0.001 - 0)(0.001 - 0)(0.01 - 0)0.6 = 10^{-8}. \end{aligned} \quad (31)$$

Similarly, the results are obtained for all $9^3 = 729$ points X. Then, we construct two empirical distribution density histograms for Y, as it is depicted in Figure 3.



(a) $\hat{f}(Y)$



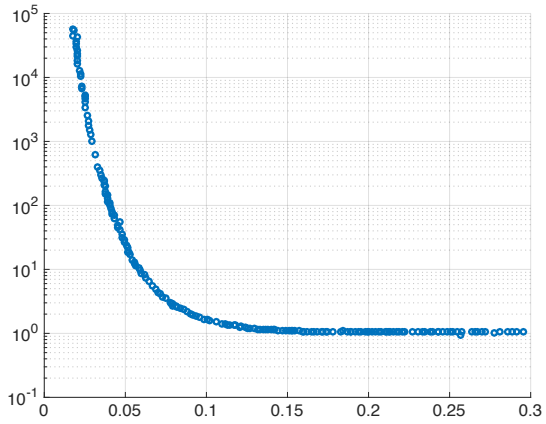
(b) $\hat{f}(Y|H_1)$

Figure 3: Empirical distribution density histograms.

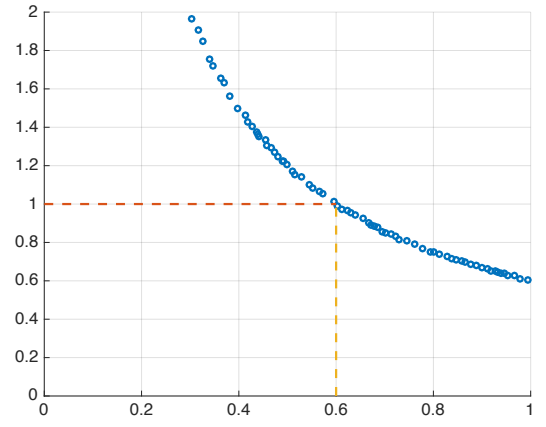
Since the obtained values of Y for all points of the constructed histograms coincide, it remains only to evaluate the curves ratio numerically, and the obtained results are shown in Figure 4(a).

The resulting function is monotonic, so we can find $Y = TH_{out}$ from

$$\frac{AilCost \cdot P(H_0) + AvCost \cdot P(H_1)}{AvCost} = \frac{0.5 \cdot 0.4 + 0.5 \cdot 0.6}{0.5} = 1. \tag{32}$$



(a) The ratio values $\hat{f}(Y)/\hat{f}(Y|H_1)$



(b) Optimal solution for the decision threshold TH_{out} based on Eq. (32)

Figure 4: Optimization process results.

Since the set of points is discrete, the following values can be proposed as a solution

$$\begin{aligned} Y_{f1} &= 0.5921663638, \frac{\hat{f}(Y)}{\hat{f}(Y|H_1)} = 1.013228776, \text{ and} \\ Y_{f2} &= 0.6050177486, \frac{\hat{f}(Y)}{\hat{f}(Y|H_1)} = 0.9917064439. \end{aligned} \tag{33}$$

In the discussed scenario, the optimal value for the decision threshold in the Bayesian function is found $Y_f = TH_{out} = 0.6$, as it is shown in Figure 4(b).

6 BENEFITS AND LIMITATIONS OF THE PROPOSED MODEL

The proposed in this manuscript evaluation methodology based on the risk function analysis provides a sub-optimal approach for the multi-factor authentication system. It allows to improve the false accept and false reject estimation for FAR, and FRR risk minimization cases, i.e., the authentication approval posterior probability guarantees the top-of-the-line approach to obtain the system parameters.

Contemporaneously, the methodology has its limitations due to heterogeneity and variety of the authentication systems. Therefore, some requirements to the applied during the system design should be considered:

(1) The MFA system owner should *properly* select the risk policy, i.e., to provide the 'expectations' as an estimate of possible operational losses due to the system errors.
(2) The precise specifications of the utilized sensing devices are a must, e.g., the more accurate the estimates of FAR and FRR are, the more reliable will be the result of optimizing the values of the system parameters.
(3) It is necessary that a number of requirements to the function of estimating a posteriori probability be fulfilled to obtain a theoretical estimate of the total risks in the system, namely: it should be continuous, reversible, and its inverse function must be differentiated on the whole domain of its definition.

7 CONCLUSIONS

The world of today is adopting new technologies uncontrollably fast. Rapidly developing smart wearable devices already have a possibility for the utilization of data from a variety of integrated sensors that could be used for the authentication purposes. In this manuscript, a new method for multi-factor authentication systems risk evaluation is proposed. The technique is developed for configuring the parameter decision making based on the Bayesian formula and evaluated numerically for a special case. In the future work, we plan to support the analytical framework with experimental results.

ACKNOWLEDGMENT

The work of the first author is supported by the Academy of Finland.

REFERENCES

[1] P. Ambalakat. 2005. Security of biometric authentication systems. In *Proc. of 21st Computer Science Seminar.*

[2] J. Blasco, T. M. Chen, J. Tapiador, and P. Peris-Lopez. 2016. A Survey of Wearable Biometric Recognition Systems. *ACM Computing Surveys (CSUR)* 49, 3 (2016), 43.

[3] F. Castanedo. 2013. A review of data fusion techniques. *The Scientific World Journal* (2013), 1–19.

[4] A. A. Fathima, S. Vasuhi, N. Babu, V. Vaidehi, and T. M. Treesa. 2014. Fusion framework for multimodal biometric person authentication system. *IAENG International Journal of Computer Science* 41, 1 (2014), 18–31.

[5] R. Fujdiak, P. Masek, J. Hosek, P. Mlynek, and J. Misurec. 2015. Efficiency evaluation of different types of cryptography curves on low-power devices. In *Proc. of International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 269–274.

[6] D. Gafurov, K. Helkala, and T. Søndrol. 2006. Biometric Gait Authentication Using Accelerometer Sensor. *JCP* 1, 7 (2006), 51–59.

[7] C. Holz and M. Knaust. 2015. Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication. In *Proc. of 28th Annual ACM Symposium on User Interface Software & Technology*. ACM, 303–312.

[8] T. B. Long, T. Hanh, et al. 2012. Multimodal biometric person authentication using fingerprint, face features. In *Proc. of Pacific Rim International Conference on Artificial Intelligence*. Springer, 613–624.

[9] L. Malina, J. Hajny, and Z. Martinasek. 2016. Privacy-preserving authentication systems using smart devices. In *Proc. of 39th International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 11–14.

[10] Aleksandr Ometov and Sergey Bezzateev. 2017. Multi-factor authentication: A survey and challenges in V2X applications. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2017 9th International Congress on*. IEEE, 129–136.

[11] A. Ometov, S. Bezzateev, J. Kannisto, J. Harju, S. Andreev, and Y. Koucheryavy. 2016. Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things. *IEEE Internet of Things Journal* 4, 4 (2016), 843 – 854. https://doi.org/10.1109/JIOT.2016.2593898

[12] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. 2018. Multi-Factor Authentication: A Survey. *Cryptography* 2, 1 (2018), 1.

[13] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, and Y. Koucheryavy. 2016. Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices. In *Proc. of International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, 1–6.

[14] T. Page. 2015. A Forecast of the Adoption of Wearable Technology. *International Journal of Technology Diffusion (IJTD)* 6, 2 (2015), 12–29.

[15] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy. 2014. Towards the era of wireless keys: How the IoT can change authentication paradigm. In *Proc. of World Forum on Internet of Things (WF-IoT)*. IEEE, 51–56.

[16] R. Rawassizadeh, B. A. Price, and M. Petre. 2015. Wearables: Has the age of smartwatches finally arrived? *Commun. ACM* 58, 1 (2015), 45–47.

[17] S. Sheena and M. Sheena. 2014. A study of multimodal biometric systems. *International Journal of Research in Engineering and Technology, ISSN* (2014), 2321–7308.

[18] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* 76 (2015), 146–164.

[19] A. Teoh, S. A. Samad, and A. Hussain. 2005. A face and speech biometric verification system using a simple Bayesian structure. *Journal of information science and engineering* 21, 6 (2005), 1121.

[20] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David. 2012. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *Proc. of 28th Annual Computer Security Applications Conference*. ACM, 159–168.

[21] J. R. Vacca. 2012. *Computer and information security handbook*. Newnes.

[22] VNI Cisco. 2017. Global Mobile Data Traffic Forecast 2016–2021. White Paper. (2017).

[23] J. Wei. 2014. How Wearables Intersect with the Cloud and the Internet of Things: Considerations for the developers of wearables. *IEEE Consumer Electronics Magazine* 3, 3 (2014), 53–56.