


## Article

# Context-Aware Multimodal FIDO Authenticator for Sustainable IT Services

Seung-Hyun Kim <sup>1</sup> , Daeseon Choi <sup>2</sup>, Soo-Hyung Kim <sup>1</sup>, Sangrae Cho <sup>1</sup> and Kyung-Soo Lim <sup>1,\*</sup>

<sup>1</sup> Information Security Research Division, ETRI, Daejeon 34129, Korea; ayo@etri.re.kr (S.-H.K.); lifewsky@etri.re.kr (S.-H.K.); sangrae@etri.re.kr (S.C.)

<sup>2</sup> Department of Medical Record & Health Information Management, Kongju National University, Gongju 32588, Korea; sunchoi@kongju.ac.kr

\* Correspondence: lukelim@etri.re.kr; Tel.: +82-42-860-5952

Received: 13 April 2018; Accepted: 18 May 2018; Published: 21 May 2018



**Abstract:** Existing sustainable IT services have several problems related to user authentication such as the inefficiency of managing the system security, low security, and low usability. In this paper, we propose a Fast IDentity Online (FIDO) authenticator that performs continuous authentication with implicit authentication based on user context and multimodal authentication. The proposed FIDO authenticator, a context-aware multimodal FIDO authentication (CAMFA) method, combines information such as the user context, state of the mobile device, and user biometrics, then applies implicit and explicit authentication methods to meet the level of authentication required by the service provider. This reduces the user's explicit authentication burden and continually authenticates users at risk during the session. Moreover, it is able to respond to attacks such as the theft of the authentication method or session hijacking. To study the effectiveness of CAMFA, we ran a user study by collecting data from 22 participants over 42 days of activity on a practical Android platform. The result of the user study demonstrates that the number of explicit authentication requests could be reduced by half. Based on the results of this study, an advanced user authentication that provides multimodal and continuous authentication could be applied to sustainable IT services.

**Keywords:** context-aware; FIDO standard; multimodal authentication; continuous authentication; implicit authentication

## 1. Introduction

User authentication is one of the most important issues in sustainable IT services; it is an essential procedure for verifying the identity of entities accessing the system. Currently, authentication methods such as passwords and biometrics are applied to satisfy the security requirements of the system. However, this approach has three limitations that hinder sustainable IT services. Firstly, there is the burden of establishing each user authentication function and the inefficiency of managing system security. Secondly, it is difficult to detect the theft of users' means of authentication, preventing attackers from being blocked. If an attacker passes the point of user authentication, the attacker can exploit the system during the authentication session. Thirdly, in order to use a confidential service, the user must perform troublesome authentication procedures every time.

To solve the first limitation, Fast IDentity Online (FIDO) technology presents a specification embracing various user authentication methods in a single framework. The FIDO protocol creates a secure communication channel between the server and the client using public key cryptography. In addition, the service provider can authenticate the user by various authentication methods such as hardware tokens, biometric information, or passwords. The user authentication means can be added or changed without modification of the FIDO server and client. This reduces the administrative overheads

for the service provider and the burden on the developers of implementing the authentication system, which was presented as the first limitation of user authentication. However, the second and third limitations still present a problem for the security and convenience of user authentication. Several related studies have been attempted to address this issue, but they are still in the initial stage and no firm results have been produced.

In order to solve the limitations of user authentication, we propose a context-aware multimodal FIDO authentication (CAMFA) method as a form of FIDO authenticator. CAMFA integrates the FIDO specification with a continuous authentication technique, which continually verifies the identity of the user during the authentication session, and multimodal authentication, which uses a combination of available authentication methods depending on the context of given situation. We begin this work by applying an entropy-based level of authentication (LOA) classification and a method of continuous management for the user's level of authentication, which allows us to compare and selectively utilize different methods of user authentication against the same criteria. We then explain the detailed implementation procedure of CAMFA in conformance with FIDO specifications. Finally, to show the utility of CAMFA, we perform a long-term user study on 22 participants in the practical Android environment. By analyzing the users' application usage pattern, we can show the resulting improvement in convenience for the user in terms of the reduction in explicit authentication while maintaining the level of security.

Our first step was to devise a method for performing context-based multimodal authentication while applying the FIDO standard, which we explain in detail. This study is the first to not only reference the researchers who perform related research, but also the developers who are actually building sustainable IT services. We also show that continuous authentication reduces users' authentication overhead in half by analyzing the large-scale application usage dataset of practical Android users. The results suggest that CAMFA is useful to practical mobile users and therefore solves the limitations of user authentication—inefficient administration, low security, and user inconvenience—which are concerns in sustainable IT services. CAMFA can reduce the inconvenience of performing user authentication each time and guarantees superior security by satisfying the level of authentication and providing enhanced security through multimodal authentication, along with continuous authentication through implicit authentication methods. Furthermore, a single FIDO-based authentication framework can allow CAMFA to address the inconvenience and reliability issues of existing authentication methods that are deployed on clients and servers. Consequently, CAMFA can help sustain IT services by addressing the low security and convenience aspects of existing authentication technologies.

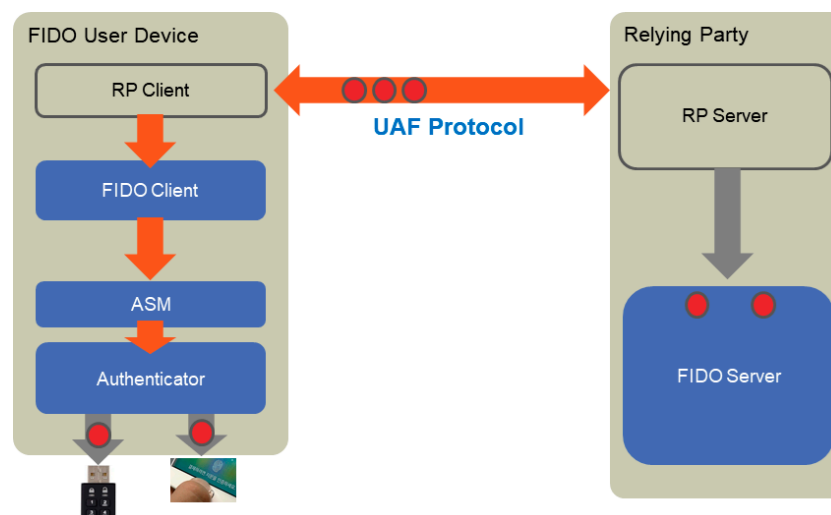
In Section 2, we discuss related works, such as the FIDO standard and multimodal and continuous authentication, and show the limitations of these works. In Section 3, we explain the concept, structure, and operation flow of CAMFA, which we propose to overcome the limitations of FIDO authenticators. Section 4 describes the implementation of CAMFA, and in Section 5, we present a user study for collecting the application usage patterns of practical Android users and the analysis result about the efficiency of CAMFA. We discuss the issues derived from the implementation and the user study of CAMFA in Section 6, and finally, in Section 7, we present some conclusions and suggestions for future research.

## 2. Related Work

### 2.1. FIDO Standards

The FIDO (Fast IDentity Online) Alliance is a federation that provides a convenient and secure authentication system in the online environment and serves as a technical standard for authentication systems [1]. It was formed in 2013 by organizations including PayPal, Lenovo, and NokNok Labs for the purpose of industry standardization. In the same year, Google developed U2F (Universal Second Factor) authentication technology, a strong authentication technology for online services based

on a security token, which was developed as a FIDO standard [2]. In December 2014, the Universal Authentication Framework (UAF), authentication technology that does not use passwords, and the U2F implementation standard were announced [3]. The FIDO Certified Testing Program, which tests and certifies interoperability between FIDO products, now has 382 (UAF: 288, U2F: 94) products worldwide which are classed as “FIDO certified” [4]. To address issues around the inefficient deployment and management of existing user authentication, FIDO UAF technology uses various authenticators in the mobile environment according to the security requirements of the Relying Party (RP). Figure 1 shows the FIDO structure [3]. The FIDO server and FIDO client send and receive messages through a server and client provided by the application service. The application server is called the RP server and the application service client is called the RP client. The request message sent by the FIDO server is delivered to the RP server, and finally reaches the FIDO client via the RP client through the network. The message format from the FIDO server to FIDO client uses UAF protocol. The FIDO client is called by the RP client according to the internal process communication protocol, which is called Intent in the case of the Android operating system, and the calling method is specified in the FIDO standard specification. The way in which the FIDO client communicates with the Authenticator Specific Module (ASM) is similar and uses a separate message specification as described in the standard. The FIDO authenticator is usually implemented as either hardware or software.



**Figure 1.** FIDO high-level architecture.

However, the FIDO authenticators proposed so far have several limitations related to security and user convenience. Firstly, they must authenticate the user at the point of the RP request. Since there is no verification procedure after the authentication session is established, it is difficult to cope with problems caused by an attacker’s exploitation of the authentication method or session hijacking (for example, a man-in-the-middle (MITM) attack). In other words, the user identity cannot be verified continuously throughout the session. Secondly, it requires explicit authentication by the user. The RP requires the user to use a specified method of authentication; that is, implicit authentication methods are not considered by existing FIDO authenticator. Although implicit authentication can be developed under the FIDO specification, none of the 288 UAF products that currently pass the FIDO interoperability test offer implicit authentication. Thirdly, it is possible to use only multifactor authentication. The RP may request the user to pass through various combinations of authentication methods by “AND” and “OR” operations on the available authentication methods. However, since these authentication methods are performed individually and sequentially, they cannot simultaneously authenticate the user. That is, multimodal authentication is not supported.

The limitations of FIDO authenticators have been raised in other studies. AETNA is a company which aims to provide the next generation of authentication by leveraging the FIDO standard. They have proposed a roadmap to combine risk-based continuous authentication with the FIDO standard by before the end of 2018 by using behavioral authentication (e.g., swipe, keystroke) and geo-location information [5]. In addition, multimodal authentication, continuous authentication, and dynamic LOA are presented as the main features of their product and are very similar to the purpose of this study. RSA Security, an American computer and network security company, has also introduced the concept of continuous authentication [6]. They utilize the FIDO standard to allow users who have been authenticated by existing authentication methods to adapt the authentication strength of the user session as the status of other authentication methods (e.g., wearable device) changes. However, these studies are conceptual, and detailed research contents and products have not yet been disclosed.

## 2.2. Multimodal and Continuous Authentication

Crawford et al. observed that user authentication at the start of a session on a mobile device ignores the varying sensitivity of different services; they proposed a transparent authentication framework that integrates existing authentication methods and behavior-based biometric authentication [7]. This framework determines whether the current device user is the owner by combining the probabilities of keystroke, voice, and PIN authentications. If the user's reliability is greater than that required by the service, the service is performed without further authentication, otherwise the user is requested to perform explicit authentication. Simulation of this method showed a 67% reduction in the number of user authentications compared to existing explicit authentication methods.

Deutschmann and Lindholm proposed a trust-threshold model using behavioral-based authentication systems that do not rely on specific hardware or sensors [8]. The existing score-threshold model depends only on a predetermined threshold to determine user authentication, so even a small deviation in the user's behavior can cause a false rejection. Therefore, they used a trust-threshold model to increase/decrease the reliability of the user according to the score of each element (e.g., keystroke, mouse, application) and determine whether the owner is authenticated according to the final reliability score. Experimental results have shown that the wrong users can be quickly detected without false rejections.

Murmura et al. proposed a technique for continuous user authentication of mobile devices based on power consumption, touch gesture, and movement [9]. Based on the fact that each user has a different behavioral pattern described by these features when using an application, they verified that the accuracy of user authentication is affected by the characteristics of the application. As a result of their user study, they found that the user's behavioral authentication is dependent on the context of the application.

Although the existing studies on continuous and multimodal authentication are similar to our study, they have two limitations. Firstly, existing studies focus mainly on continuous authentication. In order to build a practical authentication system, other aspects such as collection, combination, analysis, and monitoring of behavioral and environmental information should be considered. Secondly, existing studies were not down-user studies based on a practical environment. The user studies cited were based on simulations or limited environmental/behavioral information over a short period of time. It is necessary to evaluate performance verification based on the environmental/behavioral information of various users.

## 3. Context-Aware Multimodal Authentication for FIDO Authenticator (CAMFA)

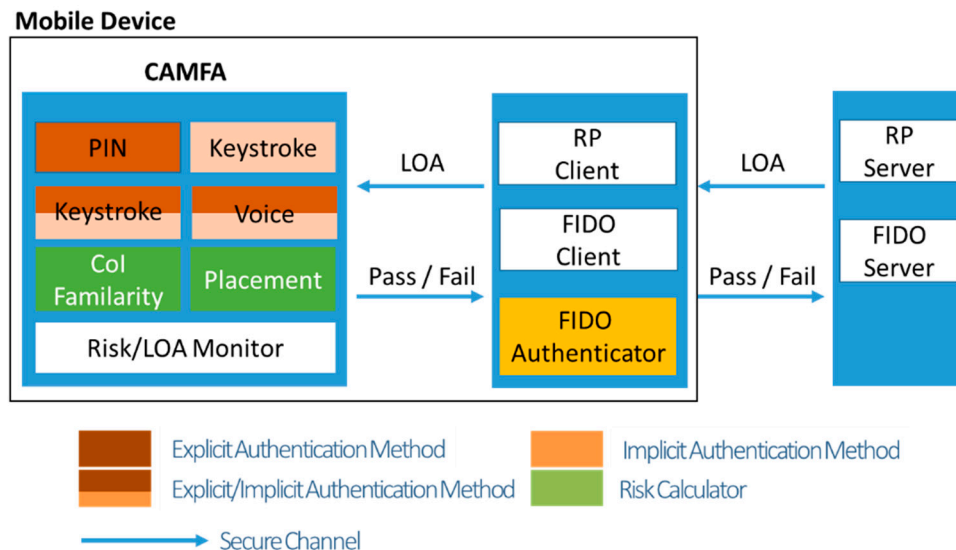
We propose a FIDO authenticator called CAMFA which provides the following features to solve the limitations of existing user authentication. Firstly, it provides continuous authentication. It can authenticate the user according to his behavioral pattern by using sensor information from the mobile

device during the authentication session. For example, images of the face, voice, and keystroke patterns can be obtained via the front facing camera, microphone, and keyboard, respectively, and used to authenticate the user continuously.

Secondly, it provides risk-based authentication. Using the sensor information of the mobile device, the risk of the current situation can be calculated. For example, the risk may vary depending on whether the current place is familiar with the user or whether the user currently possesses the mobile device. This calculated risk is used to adapt the authentication strength of the user's current session. For example, if the risk is low, the authentication strength of the session is maintained for a long time, but if the risk is high, this time is reduced.

Thirdly, it provides multimodal authentication according to LOA. For service provisioning, the RP represents a threshold authentication strength as an LOA, rather than an arbitrary authentication method. The FIDO authenticator combines the currently available authentication methods to satisfy this LOA. At this time, it considers the authentication strength of the current session and the implicit authentication methods preferentially. If the LOA is not satisfied, an explicit authentication method with appropriate authentication strength is selected and requested from the user to satisfy the required LOA.

Figure 2 shows the conceptual architecture of CAMFA. The left side of the figure is the proposed FIDO authenticator. It can freely add the available explicit/implicit authentication methods. The monitor module of CAMFA is responsible for calculating the risk of the current user context, tracking and adapting the authentication strength of the user's session, invoking the implicit/explicit authentication methods, and handling the call and response messages of the FIDO server. On the right side of the figure, the entities related to the FIDO standard present the LOA without explicitly requesting the authentication methods. The detailed explanation of Figure 2 can be found in Figure 6 of Section 4.3.



**Figure 2.** Conceptual architecture of CAMFA.

### 3.1. Entropy-Based LOA

The existing LOA simply divides the authentication strength according to the characteristics of each authentication method. In general, authentication methods are divided into three categories: “what you know”, “what you have”, and “who you are”. “What you know” methods of authentication, such as passwords, have a low LOA because this information is easy to steal and misuse by a remote attacker. On the other hand, physical authentication methods such as hardware tokens (“what you

have”) or biometrics (“who you are”) have a high LOA because they are much harder for attackers to steal.

However, the existing LOA has some limitations. Firstly, it is difficult to distinguish the difference in authentication strength because it is not considered by the current LOA. The authentication strength may be different even within the same authentication method. For example, as the key size of a password increases, the authentication strength may increase as it becomes harder for an attacker to predict. Secondly, the criteria required to estimate the authentication strength at the time of multifactor/multimodal authentication is ambiguous. Currently, the LOA is set by the service provider according to a combination of arbitrary authentication methods, but it is difficult to objectively compare authentication strength according to the combination of methods used. Thirdly, the LOA has a fixed combination of authentication methods for multifactor/multimodal irrespective of the user’s situation. When the service provider sets the LOA by applying specific authentication methods, the LOA is inherently difficult to achieve if the user cannot use the authentication method.

We use an entropy-based LOA as a means for a common comparison of authentication methods. Entropy is assigned to each authentication method and the LOA is classified according to the authentication strength represented as entropy.

Entropy is applied based on the key space required for the authentication method [10]. The key space of an alphabetic password  $K_{pw}$  is

$$K_{pw} = C^n \quad (1)$$

where  $C$  is an alphanumeric character and  $n$  is the length of password. The entropy  $E_{pw}$  of the password is

$$E_{pw} = \log_2 K_{pw} \quad (2)$$

Entropy derived from several existing authentication methods is shown in Table 1.

**Table 1.** Entropy of several existing authentication methods.

| Authentication Method       |          |  | Key Space | Entropy (bit) |
|-----------------------------|----------|--|-----------|---------------|
| PIN <sup>1</sup> (4 digits) |          |  | $10^4$    | 13.2877       |
| Password<br>(8 digits)      | PW—Type1 | (Uppercase (or lowercase) + number + Special character) <sup>8</sup> |           | 48.6997       |
|                             | PW—Type2 | (Uppercase + lowercase + number) <sup>8</sup>                        |           | 47.6336       |
|                             | PW—Type3 | (Uppercase + lowercase + Special character) <sup>8</sup>             |           | 51.1385       |
|                             | PW—Type4 | (Uppercase + lowercase + number + Special character) <sup>8</sup>    |           | 52.4367       |
| 6-digits OTP <sup>2</sup>   |          |  | $10^6$    | 19.9316       |
| Security card               |          |  | 35P2      | 10.2167       |
| SMS <sup>3</sup>            | 4 digits |  | $10^4$    | 13.2877       |
|                             | 6 digits |  | $10^6$    | 19.9316       |

<sup>1</sup> Personal Identification Number, <sup>2</sup> One Time Pin, <sup>3</sup> Short Message Service.

In the case of biometrics, false match rate (FMR) is used as a criterion for entropy to measure its authentication strength. FMR can be defined as the rate of mismatching biometric information between two people involving a particular person. FMR is an important performance measure for a biometric authentication system since it indicates the rate of allowing a user to perform authentication on the behalf of other people. The key space of the biometric derived from FMR,  $K_{bio}$ , can be expressed as

$$K_{bio} = \frac{1}{FMR(1)} \quad (3)$$

where  $FMR(1)$  implies  $P(\text{false match})$  [11]. Table 2 shows the FMR of biometric authentication methods derived from previous studies and the resulting entropy.



**Table 2.** Entropy of several existing biometric authentication methods.

| Biometric Authentication Method | FMR (%) | Entropy (bit) | Reference |
|---------------------------------|---------|---------------|-----------|
| Face                            | 0.001   | 9.9658        | [12]      |
| Iris                            | 0.0001  | 13.2877       | [13]      |
| Fingerprint                     | 0.001   | 9.9658        | [13]      |
| Voice                           | 0.01    | 6.6439        | [14]      |
| Palm vein                       | 0.0001  | 13.2877       | [14]      |
| Keystroke                       | 0.01    | 6.6439        | [15]      |

However, when compared with other authentication methods, biometrics is unlikely to be exposed to remote attackers. According to Adler et al. [16], when computing the relative entropy using the mean of the population and the difference between individuals, the principal component analysis (PCA) feature of the face increases to 46.9 bits when combined with the independent component analysis (ICA) feature. Therefore, based on these results, we estimate that the entropy of biometric authentication, and the entropy of facial recognition authentication, is approximately 47 bits.

The security strength of an authentication method can be affected by the current situation in which CAMFA is being applied. The aforementioned previous studies have assumed the ideal environment and have thus theoretically proposed the best entropy for each authentication method. However, in the practical mobile environment, the security strength of an authentication method can decrease owing to the environmental constraints affecting the accuracy of the authentication method, as well as the security vulnerability of the authentication method. Consequently, the actual entropy associated with a particular authentication method may be lower in value than the corresponding theoretical entropy. For example, in the case of password-based authentication methods, a password that can be easily guessed by an attacker may possess a lower security strength than a random password of the same length. Furthermore, in the case of SMS-based authentication methods, if an attacker can steal the user's mobile device and view the SMS, the security strength becomes zero.

Based on the calculation of ideal entropy of an authentication method, the practical key space that reflects the security considerations of the current situation can be expressed as

$$SV_{current} = \sum_{i=0}^N (severity_i \times similarity_i) \quad (4)$$

$$K_{practical} = \begin{cases} 0, & SV_{current} \geq 1 \\ K_{theoretical} \times (1 - SV_{current}), & SV_{current} < 1 \end{cases} \quad (5)$$

Here,  $SV_{current}$  represents the security vulnerability of the current scenario and  $K_{theoretical}$  represents the theoretical key space of each type of authentication method that can be derived from Equations (2) and (3). In Equation (4),  $N$  indicates the number of security vulnerabilities that a particular authentication method should take into consideration for the current situation. The *severity* attribute indicates the impact of security vulnerability on the security strength of an authentication method and has a float value ranging from zero (no impact on security strength) to one (disablement of authentication method). The *similarity* attribute refers to the probability of occurrence of the vulnerability and can be expressed as a float value ranging from zero (not equal) to one (equal), thereby indicating the difference between the current situation and the situation in which the particular vulnerability could occur.

In Equation (5), the security vulnerability in current situation  $SV_{current}$  has been expressed as a float value greater than or equal to zero. If the  $SV_{current}$  has a value of zero, it indicates an environment that is safe from all security vulnerabilities in the current situation and the associated authentication method can provide complete theoretical entropy. However, if the  $SV_{current}$  has a value of greater than one, it implies a completely vulnerable environment that has security vulnerabilities in the current situation and therefore does not provide the authentication method's theoretical entropy at all. A security vulnerability with severity of value one and similarity of value one can also completely

disable the security strength of an authentication method in the current situation. In the case when there are no major security vulnerabilities, the existence of multiple vulnerabilities (i.e., several security vulnerabilities with both severity and similarity values being greater than zero and less than one) may weaken or disable the security strength of an authentication method. Since there can be various security vulnerabilities for each authentication method, it is necessary to analyze the security vulnerabilities considered in previous studies, as well as various issues that may arise in the future. It is beyond the scope of the proposed study to examine the said aspects in detail. Therefore, in the paper, the authors have assumed an ideal environment without any security vulnerabilities.

### 3.2. Grade-Up/Grade-Extend/Grade-Down of LOA

Users can increase their LOA (Grade-Up) by using additional authentication methods. In the case of explicit authentication, even if the user's current LOA is 0, the user moves to the corresponding LOA if the user passes an authentication method satisfying the entropy of the required LOA. In the case of implicit authentication, the entropy of the implicit authentication method is added to the authentication strength of the current user session. If the summed entropy exceeds the entropy required by the next LOA, the user's session will upgrade to the corresponding LOA.

For example, we can suppose a user is authenticated by PIN and implicit facial authentication. Let us assume that LOA-1 has entropy from 1 to 20, LOA-2 from 21 to 55, and LOA-3 from 55 and above. Initially, when the user has passed only PIN authentication ( $E_{pin} = 13$ ) they are at LOA-1. When they pass implicit facial recognition authentication ( $E_{implicit\_face} = 47$ ), the final entropy reaches 60 which is LOA-3 ( $13$  (entropy of the PIN) +  $47$  (entropy of the face) >  $55$  (required entropy of LOA-3)).

CAMFA maintains (Grade-Extend) or decreases (Grade-Down) the LOA of a user's session based on contextual factors. If a user is the owner of a mobile device, then once they have established a session, the LOA of the session is maintained. However, if the user does not own the mobile device, the LOA of the session will drop depending on the degree of risk that the mobile device will be stolen and exploited. CAMFA calculates the user's risk in the current situation based on the context of interest (COI) familiarity and the placement of the mobile device.

COI is an indicator of how familiar the current environment is to the user [17]. It uses probability based on how much time the user spends in the current place and how many fixed terminals are located nearby. A low COI familiarity means that there is a high probability that the user is at risk, while a high COI familiarity suggests the current environment is likely to be low risk because the user is familiar with the place. On the other hand, even if the place is familiar to the user, it is considered to be high risk if the terminals are fluctuating, which occurs in locations such as cafes or restaurants.

Placement is an indicator of how the user is keeping the mobile device. For example, the user may place a mobile device in his hand, pocket, or on the table. If the device is in his hand or pocket, CAMFA judges that the user owns the mobile device and maintains the LOA (Grade-Extend). Meanwhile, if the screen is turned off and the device is located on a table, CAMFA determines that the user and the mobile device are separated and drops the LOA (Grade-Down). Since the risk is proportional to the length of time the user and the mobile device are separated, CAMFA uses the timeout to gradually decrease the LOA of the user's session. The reduction rate of the LOA is also proportional to the risk from COI familiarity. When COI familiarity is low, the LOA reduces quickly because it means that user is away from a well-known place. By contrast, when COI familiarity is high, the user confidence grade reduces slowly because it means that the user is close to a well-known place. Equation 6 provides a formula for reducing the LOA of a user's session:

$$l_c = \text{floor} \left( l_c - \left( 2 \times \frac{(t_c - t_s)}{N} \right) \times \left( 0.5 + \frac{(1.0 - f_c)}{2} \right) \right) \quad (6)$$

where  $l_c$  is the LOA of the user's session,  $t_c$  is the current time,  $f_c$  is the COI familiarity value,  $t_s$  is the time when the risk is high, and  $N$  is the timeout of session.



### 3.3. Receive/Process/Reply of Service Provider's LOA Request

The user must satisfy the required LOA in order to request the service provider to perform a specific action (e.g., login the service or execute a specific transaction). The monitor module of CAMFA manages the LOA of the user's session, then receives and responds to the LOA request from the user's service provider. That is, as described in the previous section, CAMFA performs the Grade-Up as necessary to satisfy the LOA of the service provider, and the Grade-Extend or Grade-Down in accordance with the variation of environmental factors.

CAMFA manages the LOA of the user's session according to the characteristics of the authentication methods. Firstly, in the case of implicit authentication methods, CAMFA periodically executes the authentication methods during the time the user owns the mobile device. The entropy of the authentication method is used to update the LOA of the user's current session. When the service provider requests a specific LOA, if the LOA of the user's current session is satisfied, CAMFA passes the request without any additional authentication procedures. Implicit authentication methods require a certain period of time to confirm whether the user is the owner of mobile device, so this authentication method can only be utilized if it is completed in advance. However, since behavioral or environmental changes of the user must be reflected at the present time, the authentication that has been completed so far is not sufficient. When authentication is executed too often, the overhead of the mobile device becomes a problem. Therefore, during the time when the user owns the mobile device, the authentication procedure must be performed at a suitable period for each method.

Secondly, for explicit authentication methods, CAMFA requests the user for appropriate authentication methods to handle an LOA request from the service provider. Considering the LOA of user's current session, CAMFA chooses an authentication method with entropy that satisfies the required LOA. The larger the gap between the LOA of the user's current session and the request of service provider, the more complex (larger entropy) authentication method the user has to pass. Even if one authentication method is not available, CAMFA provides several authentication methods for the user to satisfy the entropy of the required LOA. Table 3 shows the type and overhead of the different authentication methods used by CAMFA.

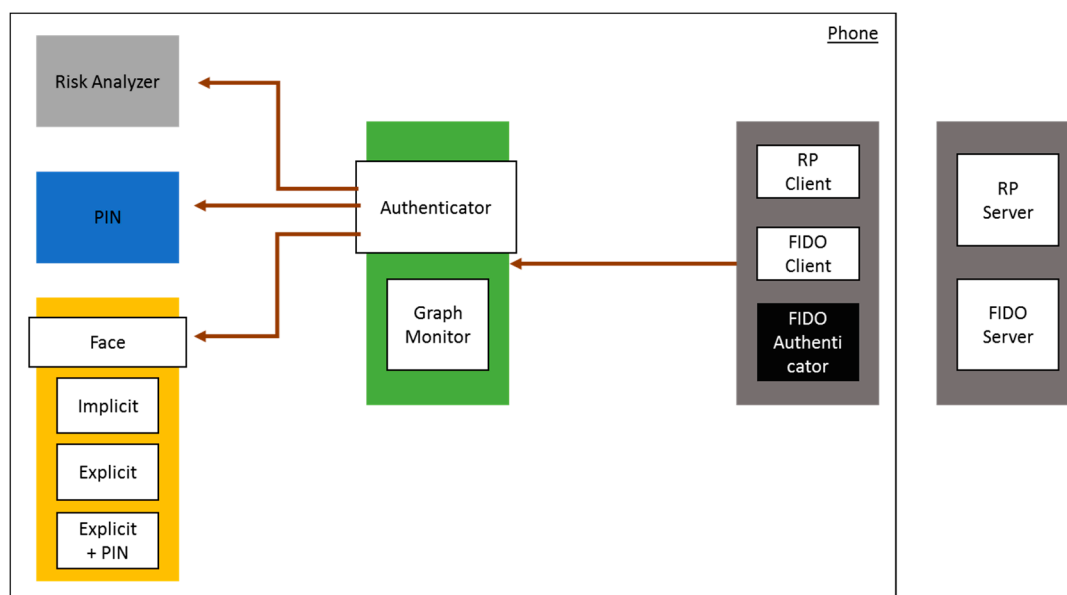
**Table 3.** The type and overhead of authentication methods used by CAMFA.

| Authentication Method | Type (Explicit/Implicit) | Overhead(Low/Mid/High) |
|-----------------------|--------------------------|------------------------|
| PIN                   | Explicit                 | Low                    |
| Password              | Explicit                 | Low                    |
| Keystroke             | Implicit                 | Mid                    |
| Placement             | Implicit                 | Mid                    |
| COI familiarity       | Implicit                 | Mid                    |
| Face                  | Explicit                 | Mid                    |
| Face                  | Implicit                 | High                   |

## 4. Implementation

We implemented CAMFA on the Android platform. For the entities related to the FIDO standard, we utilized one of our FIDO certified products that had passed the FIDO Interoperability test [4]. Using the concept of CAMFA, the FIDO authenticator applies the explicit/implicit authentication method available to our product. This section focuses on the part where CAMFA operates between the FIDO standard and the authentication methods.

Figure 3 shows the implementation block diagram of CAMFA. The entities related to the FIDO standard, such as FIDO server, RP server, RP client, and FIDO client, are the same as the existing ones. However, the RP's LOA is additionally specified in the parameter available as an extension in the FIDO protocol. As a FIDO authenticator, CAMFA receives an authentication request from the FIDO client; it then satisfies the RP's LOA using the available implicit/explicit authentication methods. CAMFA also continuously monitors the LOA of the user's current session based on the risk of the mobile device.



**Figure 3.** Implementation block diagram of CAMFA.

#### 4.1. Interaction between CAMFA and Authentication Methods

There are three ways for CAMFA to work with authentication methods. Firstly, CAMFA can ask each authentication method for the history of that technique. If the user authentication was successful within the valid period for that method, the result is applied to the LOA of the user's session. Secondly, CAMFA can ask the implicit authentication methods to authenticate the user. Among the authentication methods obtainable without the user's explicit intervention, CAMFA analyzes the sensor data to confirm whether the user is the owner of mobile device. Thirdly, CAMFA can request user authentication using the explicit authentication methods. If the LOA of the user's current session is not sufficient, CAMFA requests the user to pass explicit authentication methods that satisfy the RP's LOA. Table 4 shows the values that the authentication methods return to CAMFA according to each request type.

**Table 4.** Return values of each type and authentication method on CAMFA.

| Request Type | Authentication Method | Return Values   |
|--------------|-----------------------|---|
| History      | Face                  | List of authentication results (confidence, reliability, threshold) of a certain period (frequency, time) |
|              | Keystroke             | List of authentication results (confidence, reliability, threshold) of a certain period (frequency, time) |
|              | Risk                  | List of risk score of a certain period (frequency, time)  |
| Implicit     | Face                  | Current authentication result (confidence, reliability, threshold)  |
|              | Risk                  | Current risk score  |
| Explicit     | Face                  | Current authentication result (confidence, reliability, threshold)  |
|              | Keystroke             | Current authentication result (confidence, reliability, threshold)  |
|              | PIN                   | Current authentication result (pass or fail)  |

There are three points when CAMFA sends a request to the authentication methods. Firstly, CAMFA requests user authentication periodically. Implicit authentication methods require their procedures to collect and analyze sensor data in order to perform user authentication. For example, in the case of facial recognition authentication, time is required to initiate the camera and acquire an image of the user's partial face. Therefore, it is advantageous if the user authentication is performed

periodically within the valid period for the method, since the authentication method can then be utilized immediately when CAMFA receives a RP's LOA request. Secondly, CAMFA requests user authentication when a user begins to use the mobile device. A change in the LOA occurs because an explicit authentication is performed at the moment when the user unlocks the device. At this point, it is possible for CAMFA to update the LOA of the user's session by requesting the history of authentication methods, implicit authentications, and the risk of the current situation. Thirdly, CAMFA requests user authentication when the FIDO client sends an authentication request. If the LOA of the user's current session does not satisfy the RP's LOA, CAMFA performs the available implicit/explicit authentication methods that have enough entropy to meet the LOA required by the RP.

#### 4.2. Handling of FIDO Authentication Request on CAMFA

CAMFA checks the LOA of a user's session when the FIDO client sends a specific LOA requested by the service provider. Based on the history of the results of each authentication method, and from the available authentication methods, CAMFA calculates the LOA of the user's current session and the risk of the user in the current situation. If the authentication strength of the session satisfies the RP's LOA, a success response to the user authentication is transmitted to the FIDO server via the FIDO client. Otherwise, an implicit authentication is performed to attempt to increase the authentication strength of the session without user intervention. If the implicit authentication does not satisfy the RP's LOA, then the explicit authentication methods which are able to satisfy the RP's LOA are selected for the user to pass. Whenever the LOA is satisfied, CAMFA sends a success response to the user authentication. However, if the LOA is not satisfied at the end, it sends a fail response to user authentication. Figure 4 shows the operation flow of the CAMFA.

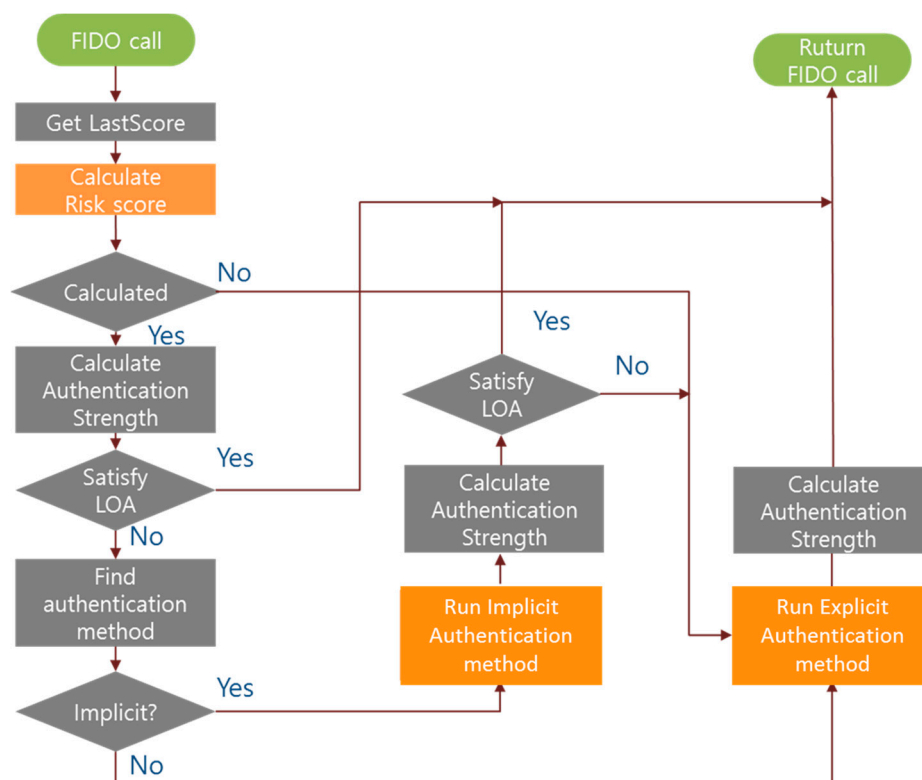


Figure 4. Operation flow of CAMFA.

Figure 5 shows a screenshot of the CAMFA operation process. On the right side of the figure is a FIDO client for verifying the operation of CAMFA, which sends an LOA when invoking CAMFA as a FIDO authenticator. The middle of the figure shows the CAMFA management and monitor screen,

which includes the current user's risk score, the authentication strength of the user session, and the evaluation result of each authentication method. The left side of the figure shows the risk calculator module and each explicit authentication method presented to the user.

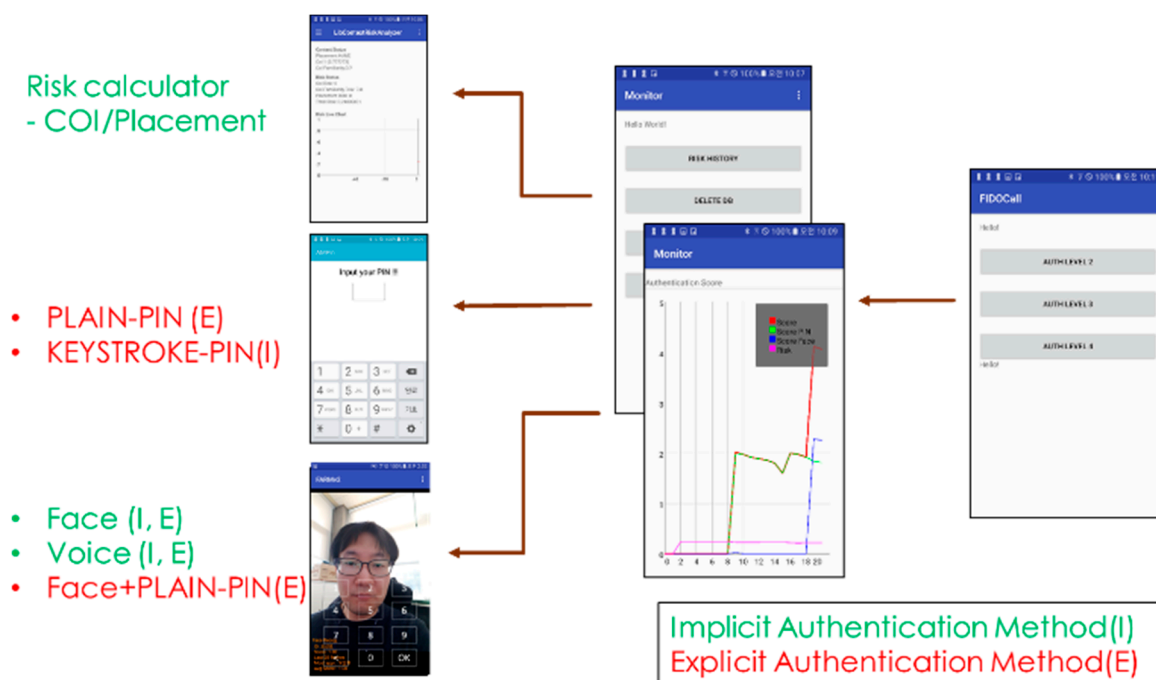


Figure 5. Screenshot of CAMFA.

In the current version of the implementation, to calculate the risk score, we evaluate the concept of COI by learning the Wi-Fi fingerprint pattern to measure how familiar the user is with their current location [17]. Also, by analyzing the status information of the mobile device, the risk is calculated according to whether the user is in possession of their mobile device (e.g., is it in their hand, pocket, or on the table). For the PIN-type authentication method, CAMFA provides a PLAIN-PIN for authenticating the user according to whether the numeric string submitted by the user matches the registered numeric string and a KEYSTROKE-PIN for matching the user's keystroke pattern. As an explicit/implicit biometric authentication device, a facial recognition module is included to acquire an image of the user with the front camera of a mobile device. It matches the acquired face image with a registered model of the user's face.

#### 4.3. Interaction between CAMFA and the FIDO Server

For interoperability with FIDO products, CAMFA was developed in compliance with the FIDO standard. In particular, in order to apply the LOA concept used in CAMFA to the FIDO standard, we extended the functions of the RP client, RP server, and FIDO server. Figure 6 shows the operational flow of CAMFA under the FIDO standard. The FIDO server predefines the RP's LOA for each service identified by the policyID (Step 0). The RP client generates a "UAFContext.RPContext" message specifying the policyID of a service, then passes a "UAFContext.FIDOContext" message to the FIDO server via the RP server (Steps 1–2). The FIDO server extracts the RP's LOA corresponding to the policyID (Step 3) and generates a "UAF AuthReq" message specifying the RP's LOA. When the FIDO client forwards the message to CAMFA (Step 4), which is one of the FIDO authenticators, CAMFA parses the "UAF AuthReq" (Step 5) and executes an authentication procedure to satisfy the RP's LOA (Step 6). The authentication result is included in the "UAF AuthResp" message and delivered to the FIDO server (Step 7). Next, the FIDO server generates the "ServerResp" message (Step 8) and

passes the message to the RP server through the RP client (Step 9). Finally, the RP server parses the “ServerResp” message and determines whether to provide the service (Steps 10–11).

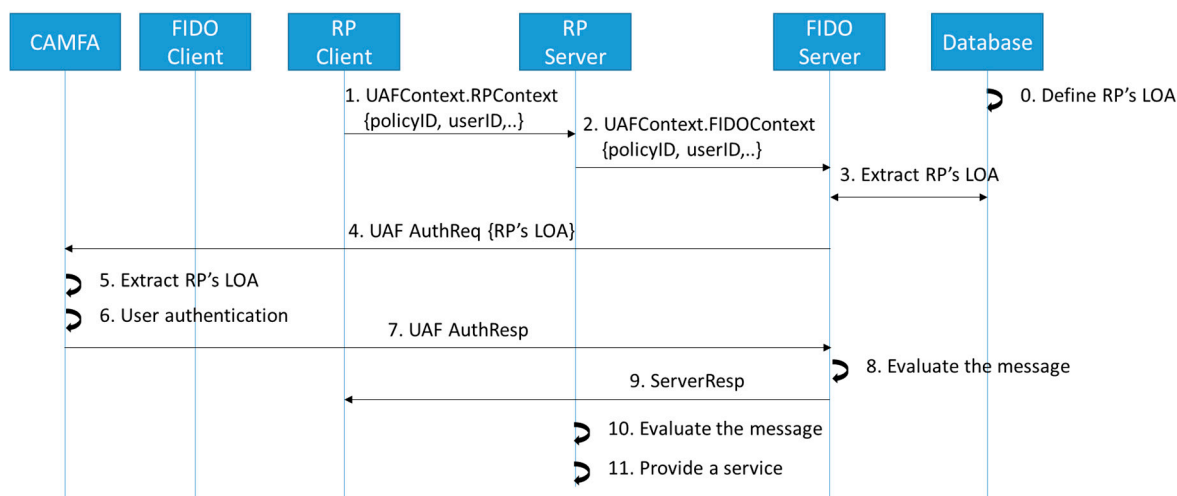


Figure 6. Operation flow of CAMFA under the FIDO standard.

Messages exchanged between each pair of FIDO entities are signed with asymmetric keys that are mutually shared at the registration, thus preventing a man-in-the-middle (MITM) attack by ensuring message integrity. The request message and the response message incorporate a challenge–response mechanism, thereby preventing a replay attack. Furthermore, the FIDO authenticator sets a public-key cryptography (PKC) attestation key while registering with the FIDO server. When the FIDO server requests the user for authentication, it sends a request message containing a challenge (i.e., UAF AuthReq message). In the case of message assertion that specifies the authentication result and the challenge value, the FIDO authenticator signs the response message with the attestation key (i.e., UAF AuthResp message) and returns it to the FIDO server. The FIDO server then verifies the assertion of the response message with the attestation key and thereby verifies the authentication result and challenge value for determining the authentication result.

To specify the RP’s LOA in the “UAF AuthReq” message, CAMFA uses the “Extension” field in the MatchCriteria attribute of the policy dictionary of the FIDO standard. Table 5 shows attribute names and the data required to construct this field, named Universal Level Extension.

Table 5. List of attributes in Universal Level Extension field.

| Name            | Type      | Value   |
|-----------------|-----------|---|
| Id              | DOMString | “extension.id.universal.level”  |
| Data            | DOMString | <ul style="list-style-type: none"> <li>Sets the LOA to the first byte of a 1-byte array. (e.g., Byte [] levels = {(byte) 0x03}); for LOA-3)</li> <li>Encodes the 1-byte array with Base64URL (e.g., String data = Base64URLHelper.encode(data);)</li> </ul> |
| Fail_if_unknown | Boolean   | False   |

In order for the FIDO client to invoke CAMFA, we define the activity implicit intent of CAMFA as shown in Figure 7. The authentication request message encoded in JSON (JavaScript Object Notation) is named ‘application/fido.verification.authenticator+json’.

```

<intent-filter>
  <action android:name="org.fidoalliance.intent.verification.universal" />
  <category android:name="android.intent.category.DEFAULT" />
  <data android:mimeType="application/fido.verification.authenticator+json"/ >
</intent-filter>

```

**Figure 7.** Activity Implicit Intent of CAMFA.

CAMFA adds the authentication result returned to the FIDO client to the extra area of the response Intent. Table 6 shows the format of CAMFA's authentication result.

**Table 6.** The format of CAMFA's authentication result.

| Name                     | Type    | Description  |
|--------------------------|---------|--|
| <b>User_cancel</b>       | Boolean | Whether a user cancel the authentication procedure |
| <b>Internal_error</b>    | Boolean | Whether an internal error has occurred             |
| <b>User_verification</b> | Boolean | Whether a user authentication has succeeded        |

## 5. User Study

In order to verify the utility of CAMFA in a practical mobile environment, we conducted a user study to collect a behavioral dataset of practical Android users. Then, we analyzed the utility of the multimodal and continuous authentication provided by CAMFA based on this behavioral dataset, which was collected over an average of 42 days for 22 participants. As a result, we confirmed that up to 48% of the explicit authentication overhead can be reduced by CAMFA.

### 5.1. Collection of Dataset from Practical Android Users

The data used in this paper was collected from 22 participants who used an Android mobile device over a period of approximately 42.5 days. Of these participants, 19 used a mobile device manufactured by Samsung, such as the Galaxy Note 5, Galaxy Note 8, and the Galaxy S7 models. Three participants used mobile devices manufactured by LG, namely the G5, V30, and X Screen models. Similar to the proposed study, various previous studies [18–20] have collected the sensor information of mobile devices and the number of participants was 9, 25, and 48, respectively. The corresponding average period of the user study was 1 h, 96 h, and 10 days, respectively. Based on the aforementioned information, it can be considered that 22 participants are enough in number for evaluating the effectiveness of CAMFA. Regarding the user study period, the authors collected the usage history of participants' mobile devices for a longer period than the previous studies, so as to demonstrate that the reduced overhead of users' authentication can persist in various situations for a long duration. Participants collected data on application usage, face confidence, mobile device placement, COI familiarity, and screen log, using a data collection application provided by us for an average 10 h per day. To protect the privacy of the participants, we received explicit consent from each participant before using our collection tool. We also avoided collecting sensitive information such as facial images and demographics.

To handle the facial recognition authentication, the collection tool collects a photograph of the user's face using the front camera of the mobile device every 10 s until 20 facial images have been collected. The collection tool then generates a model of the user's face using convolutional neural networks (CNN). The collection tool then deletes the user's facial images from the mobile device for privacy protection. At the time of facial authentication, the captured image is compared with the user's face model after extracting the feature points by calculating the Euclidean distance between the features. A detailed method for measuring face confidence is described in [21].



The collection tool collects values from sensors including the accelerometers, gyroscope, light, and orientation sensors in the mobile device each second. The tool then generates a classifier using a decision tree to determine the placement of the mobile device. The placement of the mobile device is classified as ‘HAND’, ‘POCKET’, and ‘TABLE’ by the classifier. The COI familiarity, which represents a similarity score with places where the user frequently spends time, is measured using Wi-Fi and Bluetooth sensors. A detailed method for measuring COI familiarity is described in [17]. The collection tool records application usage and screen log whenever an event occurs that is related to an application or the screen, respectively. Table 7 shows the format of the processed dataset in the user study.

**Table 7.** The format of processed dataset in the user study.

| Name            | Value                       | Description   |
|-----------------|-----------------------------|---|
| App log         | Package name of application | The name of the application or service that the user used (e.g., com.android.systemui)      |
| Face confidence | 0.0~1.0                     | Reliability of owner’s face   |
| Placement       | ‘HAND’/‘POCKET’/‘TABLE’     | Physical location of the mobile device  |
| COI familiarity | 0.0~1.0                     | A similarity score indicating whether the current location is similar to a trusted location |
| Screen log      | ‘ON’/‘OFF’                  | Screen status of the mobile device  |

## 5.2. Classification of Applications’ LOA

According to the dataset, the 22 participants used a total of 632 applications over approximately 42.5 days. We investigated the applications used by first finding them in the Google Play Store. We determined the LOA of each application according to the authentication method requested. When we did not both agree on the LOA of an application, it was determined using majority voting after another researcher determined the LOA of the application. Table 8 lists examples of applications with different LOAs.

**Table 8.** Four-step LOA according to the authentication method required by application.

| LOA | Authentication Method  | Applications                            |                       |                     |
|-----|--|---|-----------------------|---------------------|
|     |  | Type                                    | Number in the Dataset | Examples            |
| 4   | Strong Authentication (combination of PKI, OTP, biometrics, and so on) | requires a high level of authentication | 65                    | Banking, Stocks     |
| 3   | Password   | requires moderate authentication        | 226                   | Facebook, Instagram |
| 2   | PIN  | requires low level authentication       | 56                    | Contact list, SMS   |
| 1   | -  | requires no authentication              | 300                   | Weather, Calculator |

Based on the actual authentication method required by an application, we defined the level of authentication as follows. Firstly, LOA-0 represents the state where the user is not using the mobile device. LOA-1 represents applications that do not require any authentication method. LOA-2 represents applications that require a PIN and include some private information such as a personal schedule, SMS, and contact list. LOA-3 represents applications that require an ID and password, such as social network services, e-mail, and games. LOA-4 represents applications such as banking and stocks, which require certificate verification and biometric authentication, such as the fingerprint or iris of users (particularly in the Republic of Korea, certain applications, such as those for banking and stocks, require certificate verification of the user).

### 5.3. Analysis of Dataset According to Each Function of CAMFA

In this section, we describe experiments, which show how the proposed active authentication can reduce the number of explicit authentication requests. We performed simulation experiments after sorting the collected data by time. The experiments were performed by excluding applications with LOA-1 or LOA-4. For the case of LOA-1, explicit authentication is not required. For the case LOA-4, strong explicit authentication (public key certificate, one-time token, or biometrics) is required. In both of these cases, we do not count the number of explicit authentications. We also assumed that the user unconditionally performed an explicit authentication when the screen of the mobile device was switched on. In this case, we count the number of explicit authentications.

#### 5.3.1. Grade-Up by Face Confidence

Grade-Up determines whether the user confidence grade is to be increased, by comparing face confidence and the predefined threshold. Table 9 shows experimental results for Grade-Up depending on the threshold. The total number of explicit authentications was 89,116; from this, Grade-Up succeeded 3547, 609, and 64 times when the threshold was 0.5 [22], 0.65 [23], and 0.8 [24], respectively. The number of explicit authentication requests could be reduced by as much as the number of Grade-Up successes. In cases where the user confidence grade was less than the LOA required by the application, success rates of Grade-Up were recorded as 46.9%, 8.0%, and 0.8%, respectively. This result shows that the threshold value of facial recognition authentication greatly affects the success rate of implicit authentication.

**Table 9.** Ratio of Grade-Up by Face Confidence.

| Threshold | Total Number of Authentication | Number of Grade-Up | Ratio of Grade-Up |
|-----------|--------------------------------|--------------------|-------------------|
| 0.5       | 89,116                         | 3547               | 0.0398            |
| 0.65      |                                | 609                | 0.0068            |
| 0.8       |                                | 64                 | 0.0007            |

#### 5.3.2. Grade-Extend by Timeout

We experimented with Grade-Extend with the threshold fixed at 0.5, which had the highest reduction rate of explicit authentication. Timeout periods were set to 5 min [25], 15 min [26], and 30 min [27] based on existing works. Table 10 shows the experimental results for Grade-Extend depending on timeout period. Among the total number of authentications, Grade-Extend succeeded 38,935, 39,491, and 39,839 times when the timeout periods were 5, 15, and 30 min, respectively. When the user confidence grade is equal to or higher than the LOA of the application, the success rates of Grade-Extend were recorded as 91.1%, 89.8%, and 89.1%, respectively. When the user confidence grade is higher than the LOA of the application, the success rates of Grade-Down were recorded as 27.2%, 30.2%, and 32.0%, respectively.

**Table 10.** Ratio of Grade-Extend by Timeout.

| Timeout (minute) | The Total Number of Authentication | Number of Grade-Extend | Number of Grade-Down | Ratio of Grade-Extend |
|------------------|------------------------------------|------------------------|----------------------|-----------------------|
| 5                | 89,116                             | 3457                   | 35,478               | 0.437                 |
| 15               |                                    | 4013                   | 35,478               | 0.443                 |
| 30               |                                    | 4361                   | 35,478               | 0.447                 |

#### 5.3.3. Combined Grade-Up and Grade-Extend

Lastly, we measured the reduction rate of explicit authentication resulting from Grade-Up and Grade-Extend with various combinations of threshold and timeout periods. As Table 11 shows,

the rates of implicit authentication (Grade-Up and Grade-Extend) were measured as 48.68% when the threshold was 0.5 and timeout was 30 min, 44.99% when the threshold was 0.65 and the timeout was 15 min, and 43.69% when the threshold was 0.8 and timeout was 5 min.

**Table 11.** Ratio of explicit authentication according to the combination of face confidence threshold and session timeout period.

| Threshold of Face Confidence | Timeout (minute) | The Total Number of Authentications | Grade-Extend | Grade-Up | Ratio of Implicit Authentication (Extend+Grade-Up) | Ratio of Explicit Authentication |
|------------------------------|------------------|-------------------------------------|--------------|----------|--|----------------------------------|
| 0.5                          | 30               | 89,116                              | 0.4470       | 0.0398   | <b>0.4868</b>                                      | 0.5132                           |
| 0.65                         | 15               |                                     | 0.4431       | 0.0068   | 0.4499   | 0.5501                           |
| 0.8                          | 5                |                                     | 0.4369       | 0.0007   | 0.4376   | 0.5624                           |

## 6. Discussion

In this study, we applied a context-aware multimodal authentication method to the FIDO authenticator, called CAMFA. We described the details of CAMFA, performed an initial implementation, and analyzed the efficiency by conducting a user study. This shows that CAMFA can provide risk-based continuous authentication in the form of a FIDO authenticator. In this process, we derived various issues.

### 6.1. Issues Related with Implementation

The first issue is how to manage the LOA of a user's current session. Previously, a user could utilize the same LOA for a service without any further authentication procedures during the session, and the session would close when the user logged out the session or the validity time passed. Continuous authentication validates a user with the implicit authentication methods during the user's session. CAMFA can better manage the LOA of the session by adapting the point of authentication procedure, frequency, authentication methods, and validity time.

The second issue is how to revise the LOA of a user's current session according to the risk. CAMFA calculates the risk from the user's environmental factors and uses it to control how quickly the LOA of a session decreases over time. CAMFA can better calculate the risk by interpreting environmental factors in a different way. For example, it can adapt the entropy of each authentication method depending on the risk score.

The third issue is how to make a combined method for multimodal authentication. There is a need to discuss which criteria should be used to distinguish authentication methods that have different characteristics from each other, how to combine authentication methods based on these criteria, and how to use the result of combined authentication methods. CAMFA classifies the strength of each authentication method based on its entropy. According to the combination of the authentication methods, the authentication strength is only arithmetically added, and CAMFA derives an LOA for the user's session according to the final entropy. There are different ways in which CAMFA could better classify and combine the various authentication methods.

### 6.2. Issues Related with Analysis

In the analysis, we determined whether Grade-Up needs to be performed by comparing face confidence and a predefined threshold. With our proposed scheme as the reference, one can now ask the question, "Can facial recognition authentication replace passwords?" According to [28] and [16], the entropy of passwords is approximately 50 bits and the entropy of facial recognition is approximately 47 bits. Therefore, in theory, passwords cannot be replaced only by facial recognition authentication. We assumed that PIN must be authenticated when a user begins to use the mobile device. Because the entropy of PIN is approximately 13 bits [21], the combined entropy of face recognition and PIN is up to approximately 60 bits. Thus, we can conclude the password can be replaced by facial recognition authentication. CAMFA can upgrade the LOA of a user session using Grade-Up.

CAMFA determines whether Grade-Extend can be performed, considering COI familiarity, timeout time, and the placement of the mobile device. If the COI familiarity is high, either there is no attacker or the attacker is likely to be known by the user because the user is located in a reliable place. If the attacker is known to the user, the attacker can be quickly identified by the user. Thus, the security of the device is high when the user is in the COI. When the placement of the mobile device is 'HAND' or 'POCKET', the user is the owner of the mobile device. When the placement of the mobile device is 'TABLE', it is possible that the user has placed the mobile device on the table and left. In this case, an attacker can misuse the user's mobile device. Based on these assumptions, we reduce the LOA of the user's session by applying a timeout. The results of the analysis show that a timeout period of 30 [29] or 15 min [26] is reasonable.

CAMFA uses Grade-Up and Grade-Extend in order to enhance users' convenience. According to the analysis, the number of explicit authentication requests can be reduced by approximately 3.9% using Grade-Up and 44.7% using Grade-Extend. Therefore, CAMFA can reduce the number of explicit authentication requests by approximately 7% greater than that presented in [18].

In Section 5.3, we demonstrated that the success rates of Grade-Up and Grade-Extend were reduced by larger thresholds or lower timeout periods. When the measured face confidence is high, the success rate of Grade-Up would increase. However, the success rates were affected by 3 participants who had not measured face confidence and 10 participants who always show low face confidences (less than 0.7). Success rates of Grade-Up and Grade-Extend can be increased by lowering the threshold and increasing the timeout period. If CAMFA defines a lower threshold and higher timeout, the user's convenience would be enhanced but the security of the user's session would be decreased. To consider the trade-off between security and convenience, more analysis is needed by changing the parameters of CAMFA.

### 6.3. Threats to Validity

The first limitation of this study is that the configuration of CAMFA is limited to a specific domain. The risk, LOA, and each authentication method are based on references, but the configuration of these features may be different depending on the environment where CAMFA is applied. We assumed that the presence of fixed peripheral devices means low risk. In an environment with high risk, it is difficult to identify the identity of the attacker. However, at low risk, the identity of the attacker is easy to identify. Nevertheless, even in a reliable place such as a home or office, CAMFA does not reflect the case where a family member or a co-worker may misuse the user's mobile device. Although implicit authentication can handle this limitation by continuous authentication, the calculation of risk has to solve this limitation.

CAMFA uses the LOA by calculating the entropy of each authentication method based on only the size of the key space according to the related studies. Existing authentication methods have certain drawbacks, and solely entropy is difficult to reflect these drawbacks. For example, according to Table 1, the SMS-based authentication method has an entropy value ranging from 13.2877 to 19.9316. However, it cannot protect a user if an attacker possesses the user's device and thereby verifies the SMS. Table 2 shows the entropy of each biometric authentication method derived from the FMR of related studies. However, a particular authentication method can have different entropies for different implementation algorithms. The entropy can vary according to the accuracy (i.e., FMR) and the threshold criteria of the biometric authentication method that has been applied. In the case of a biometric authentication method that employs the same algorithm, variation of performance between explicit authentication and implicit authentication can occur, as observed from our user study results of facial recognition authentication.

In order to overcome the limitation of the entropy calculation of the previous studies, we presented the entropy formulas of the authentication method considering the security vulnerability in the current situation in Equations (4) and (5). However, the effectiveness of the equations is not verified because our user study assumed an ideal situation in which there is no security vulnerability. Instead,

from our user study performed in the practical environment, we could see that the facial recognition authentication did not reach the performance in the ideal environment. This confirms the need to consider security vulnerabilities in the current situation. In order to measure the practical security strength of authentication method in the current situation, it is necessary to investigate and analyze the security vulnerabilities of each authentication method, including not only the previous studies, but also various problems that may arise in the future. In addition, because this study is based on specific situations, it is necessary to set up specific settings for each domain based on basic settings that can be referred to. Therefore, it is necessary to study the extension of CAMFA for other domains and other factors, such as Beacon sensor [30].

The effectiveness of each authentication method may vary depending on the accuracy of the authentication method employed for CAMFA. Each authentication method mentioned in the manuscript can be applied to CAMFA. CAMFA does not rely on a particular authentication method. Depending on the specific authentication method actually applied at the time of implementing CAMFA, the corresponding algorithm and its effectiveness will thereby be determined. A detailed description of each authentication method has not been included in the manuscript because it is beyond the scope of CAMFA's contribution. The second limitation of this study is that the user study was performed under limited conditions. To accurately verify the utility of CAMFA, we should analyze the usage history of CAMFA after applying CAMFA to all applications installed on practical users' mobile devices. However, this can be difficult and there are technical issues when modifying every application. Therefore, after collecting the usage history of practical Android users' mobile devices for an extended period of time, we processed the risk, the LOA of the application, and the authentication methods by assuming that CAMFA was applied. Based on the results of the user study, we could identically analyze the performance of CAMFA. Rather, based on the collected dataset, additional analysis can be performed assuming the changed conditions such as the additional authentication methods, advance decision algorithms [31,32], or the modified LOA criteria. We have a plan to use this dataset to conduct further research to improve the performance of CAMFA.

## 7. Conclusions & Future Works

Existing sustainable IT services have several problems related to user authentication such as the inefficiency of managing the system security, low security, and low usability. In this paper, we proposed multimodal authentication with context awareness in the form of a FIDO authenticator. The proposed CAMFA overcomes the limitations of existing FIDO authentication devices which only provided explicit authentication, user authentication only at a specific time, and multifactor authentication. This reduces the user's explicit authentication burden and continually authenticates users at risk during the session. Moreover, it is able to respond to attacks such as the theft of the authentication method or session hijacking. To study the effectiveness of CAMFA, we ran a user study by collecting data from 22 participants over 42 days of activity on a practical Android platform. The result of the user study demonstrates that the number of explicit authentication requests could be reduced by half. Based on the results of this study, an advanced user authentication that provides multimodal and continuous authentication could be applied to sustainable IT services.

For future research, we will extend the CAMFA with various explicit/implicit authentication methods, study the calculation of LOA and risk, and investigate the combination of other authentication methods. This will improve the performance of CAMFA and expand it to other domains. We will also conduct further analysis based on the collected dataset to study advanced CAMFA for sustainable IT services.

**Author Contributions:** Se.-H.K.: Research for the related works, design the proposed model, and wrote the paper. D.C.: Perform and analyze user-study. So.-H.K.: review, comments, assessment of the paper. S.C.: Total supervision of the paperwork, K.-S.L.: Research for the related works, and readability, grammar, and spelling checks of the article.



**Acknowledgments:** This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2016-0-00097, Development of Biometrics-based Key Infrastructure Technology for On-line Identification)

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. FIDO Alliance. Available online: <https://fidoalliance.org/> (accessed on 6 April 2018).
2. Sampath, S. *Universal 2nd Factor (U2F) Overview*; FIDO Alliance Proposed Standard: Wakefield, MA, USA, 2015.
3. Sampath, S. *FIDO UAF Architectural Overview*; FIDO Alliance Proposed Standard: Wakefield, MA, USA, 2014.
4. FIDO Certified Product. Available online: <https://fidoalliance.org/certification/fido-certified-products/> (accessed on 6 April 2018).
5. Aetna's Next Generation Authentication. Available online: <https://news.aetna.com/2017/08/aetnas-next-generation-authentication/> (accessed on 6 April 2018).
6. Nag, A.K. An Adaptive Approach Towards the Selection of Authentication Factors in Multi-Factor Authentication (MFA) System. In Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa; 2015; pp. 7–10.
7. Crawford, H.; Renaud, K.; Storer, T. A framework for continuous, transparent mobile device authentication. *Comput. Secur.* **2013**, *39*, 127–136. [CrossRef]
8. Deutschmann, I.; Lindholm, J. Behavioral biometrics for darpa's active authentication program. In Proceedings of the 2013 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany; 2013; pp. 5–6.
9. Murmura, R.; Stavrou, A.; Barbar'a, D.; Fleck, D. Continuous Authentication on Mobile Devices Using Power Consumption, Touch Gestures and Physical Movement of Users. In *Research in Attacks, Intrusions, and Defenses*; Springer: Cham, Switzerland, 2015; pp. 405–424.
10. O'Gorman, L. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* **2013**, *91*, 2021–2040. [CrossRef]
11. Yeum, H. Authentication Levels Based on Trust Elevation Applicable to Financial Services. TTA.KO-12.0313. TTA. 2017. Available online: [http://committee.tta.or.kr/data/standard\\_view.jsp?by=asc&order=publish\\_date&nowPage=1571&pk\\_num=TTAK.KO-12.0313&nowSu=15708&rn=1](http://committee.tta.or.kr/data/standard_view.jsp?by=asc&order=publish_date&nowPage=1571&pk_num=TTAK.KO-12.0313&nowSu=15708&rn=1) (accessed on 21 May 2018).
12. Schroff, F.; Kalenichenko, D.; Philbin, J. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA; 2015; pp. 815–823.
13. Grother, P.; Salamon, W.; Chandramouli, R. Biometric Specifications for Personal Identity Verification. *NIST Spec. Publ.* **2013**, *800*, 76–82.
14. Silva, P. PalmSecure—A new level of Biometric Technology Solutions. *Fujitsu* **2013**. Available online: [http://www.fujitsu.com/pt/Images/Palm\\_Secure\\_tcm72-630557.pdf](http://www.fujitsu.com/pt/Images/Palm_Secure_tcm72-630557.pdf) (accessed on 21 May 2018).
15. Yampolskiy, R.V.; Govindaraju, V. Behavioural biometrics: A survey and classification. *Int. J. Biom.* **2008**, *1*, 81–113. [CrossRef]
16. Adler, A.; Youmaran, R.; Loyka, S. Towards a measure of biometric information. In Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCECE), Ottawa, ON, Canada; 2006; pp. 210–213.
17. Miettinen, M.; Heuser, S.; Kronz, W.; Sadeghi, A.-R.; Asokan, N. ConXsense: Automated context classification for context-aware access control. In Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, Kyoto, Japan; 2014; pp. 293–304.
18. Riva, O.; Qin, C.; Strauss, K.; Lymberopoulos, D. Progressive Authentication: Deciding When to Authenticate on Mobile Phones. In Proceedings of the 21st USENIX Security Symposium, Bellevue, WA, USA; 2012; pp. 301–316.
19. Clayton, S.; Rahmati, A.; Tossell, C.; Zhong, L.; Kortum, P. LiveLab: Measuring wireless networks and smartphone users in the field. *ACM SIGMETRICS Perform. Eval. Rev.* **2011**, *38*, 15–20.
20. Upal, M.; Sarkar, S.; Patel, V.M.; Chellappa, R. Active user authentication for smartphones: A challenge data set and benchmark results. In Proceedings of the 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA; 2016; pp. 1–8.



21. Oh, S.; Kim, S.; Lim, K. Compact deep learned feature-based face recognition for Visual Internet of Things. *J. Supercomput.* **2017**, *1*–13. [[CrossRef](#)]
22. Microsoft Face API V1.0 Default Threshold. Available online: <https://westus.dev.cognitive.microsoft.com/docs/services/563879b61984550e40cbb8d/operations/563879b61984550f30395239> (accessed on 6 April 2018).
23. IBK Knowledge Center Intelligent Video Analytics 2.0 Default Threshold. Available online: [https://www.ibm.com/support/knowledgecenter/en/SS88XH\\_2.0.0/iva/admin\\_alert\\_face\\_recognition.html](https://www.ibm.com/support/knowledgecenter/en/SS88XH_2.0.0/iva/admin_alert_face_recognition.html) (accessed on 6 April 2018).
24. KAIROS. Available online: <https://www.kairos.com/blog/three-steps-to-successful-facial-recognition> (accessed on 6 April 2018).
25. CJIS Advisory Policy. *Criminal Justice Information Services (CJIS) Security Policy*; CJISD-ITS-DOC-08140, Version 5.4; Criminal Justice Information Services Division: Washington, DC, USA, 2015.
26. Grassi, P.A.; Fenton, J.L.; Newton, E.M.; Perlner, R.A.; Regenscheid, A.R.; Burr, W.E.; Choong, Y.Y. *NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management*; NIST: Gaithersburg, MD, USA, 2017.
27. SSOCIRCLE. Available online: <https://www.ssocircle.com/en/2142/session-timeout-another-useless-security-brainchild/> (accessed on 6 April 2018).
28. Kim, J.; Sa, K.; Youm, H. Trust elevation method based on the user assurance level in financial sector. *Rev. Korea Inst. Inf. Secur. Cryptol. Bimon.* **2017**, *27*, 47–56.
29. Federal Bureau of Investigation. Available online: <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center> (accessed on 6 April 2018).
30. Kwak, J.; Sung, Y. Beacon-Based Indoor Location Measurement Method to Enhanced Common Chord-Based Trilateration. *J. Inf. Process. Syst.* **2017**, *13*, 1640–1651.
31. McNaughton, J.; Crick, T.; Hatch, A. Determining device position through minimal user input. *Hum. Cent. Comput. Inf. Sci.* **2017**, *7*, 36. [[CrossRef](#)]
32. Lee, J.-H.; Shin, B.-S. SensDeploy: Efficient sensor deployment strategy for real-time localization. *Hum. Cent. Comput. Inf. Sci.* **2017**, *7*, 37. [[CrossRef](#)]



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).