cryptography

Article

Multi-Factor Authentication: A Survey †

Aleksandr Ometov 1,*, Sergey Bezzateev 2, Niko Mäkitalo 3, Sergey Andreev 1, Tommi Mikkonen 3 and Yevgeni Koucheryavy 1

[1] Laboratory of Electronics and Communications Engineering, Tampere University of Technology, FI-33720 Tampere, Finland; sergey.andreev@tut.fi (S.A.); evgeni.kucheryavy@tut.fi (Y.K.)

[2] Department of Security of Cyberphysical Systems, ITMO University, St. Petersburg RU-197101, Russia; bsv@aanet.ru

[3] Department of Computer Science, University of Helsinki, FI-00014 Helsinki, Finland; niko.makitalo@helsinki.fi (N.M.); tommi.mikkonen@helsinki.fi (T.M.)

* Correspondence: aleksandr.ometov@tut.fi

† This manuscript is an extended version of work by A. Ometov and S. Bezzateev titled "Multi-factor Authentication: A Survey and Challenges in V2X Applications" presented at the 9th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT) on 6 November 2017.

Received: 30 November 2017; Accepted: 18 December 2017; Published: 5 January 2018

Abstract: Today, digitalization decisively penetrates all the sides of the modern society. One of the key enablers to maintain this process secure is authentication. It covers many different areas of a hyper-connected world, including online payments, communications, access right management, etc. This work sheds light on the evolution of authentication systems towards Multi-Factor Authentication (MFA) starting from Single-Factor Authentication (SFA) and through Two-Factor Authentication (2FA). Particularly, MFA is expected to be utilized for human-to-everything interactions by enabling fast, user-friendly, and reliable authentication when accessing a service. This paper surveys the already available and emerging sensors (factor providers) that allow for authenticating a user with the system directly or by involving the cloud. The corresponding challenges from the user as well as the service provider perspective are also reviewed. The MFA system based on *reversed* Lagrange polynomial within Shamir's Secret Sharing (SSS) scheme is further proposed to enable more flexible authentication. This solution covers the cases of authenticating the user even if some of the factors are mismatched or absent. Our framework allows for qualifying the missing factors by authenticating the user without disclosing sensitive biometric data to the verification entity. Finally, a vision of the future trends in MFA is discussed.

Keywords: survey; authentication; SFA; 2FA; MFA; evolution; vision

1. Introduction

The continuous growth in the numbers of smart devices and related connectivity loads has impacted mobile services seamlessly offered anywhere around the globe [1]. In such connected world, the enabler keeping the transmitted data secure is, in the first place, *authentication* [2–4].

According to the fundamental work in [5], authentication is a process where a "user identifies himself by sending x to the system; the system authenticates his identity by computing $F(x)$ and checking that it equals the stored value y". This definition has not changed significantly over time despite the fact that a simple password is no longer the only factor for validating the user from the information technology perspective [6].

Authentication remains a fundamental safeguard against illegitimate access to the device or any other sensitive application, whether offline or online [7–9] (see Figure 1). Back in time, the transactions were authenticated primarily by physical presence, i.e., for example, by applying the wax seal [10].

Closer to present days and with the advancement of our civilization, it was realized that the validation based on the sender identification *only* is not always adequate on the global scale [11].

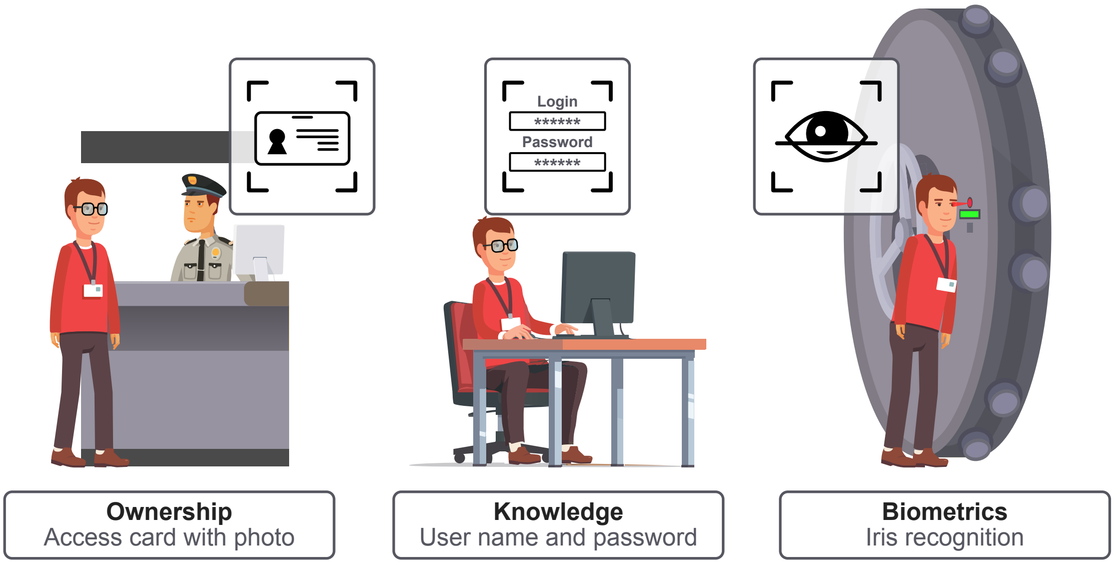

Figure 1. Conceptual authentication examples.

Initially, only one *factor* was utilized to authenticate the subject. By that time, Single-Factor Authentication (SFA) was mostly adopted by the community due to its simplicity and user friendliness [12,13]. As an example, the use of a password (or a PIN) to confirm the ownership of the user ID could be considered. Apparently, this is the weakest level of authentication [14,15]. By sharing the password, one can compromise the account immediately. Moreover, an unauthorized user can also attempt to gain access by utilizing the dictionary attack [16], rainbow table [17], or social engineering techniques [18]. Commonly, the minimum password complexity requirement is to be considered while utilizing this type of authentication [19].

Further, it was realized that authentication with just a single factor is not reliable to provide adequate protection due to a number of security threats [20]. As an intuitive step forward, Two-Factor Authentication (2FA) [21–23] was proposed that couples the representative data (username/password combination) with the factor of personal ownership, such as a smartcard or a phone [24,25].

Today, three types of factor groups are available to connect an individual with the established credentials [26]:

1. *Knowledge factor*—something the user knows, such as a password or, simply, a "secret";
2. *Ownership factor*—something the user has, such as cards, smartphones, or other tokens;
3. *Biometric factor*—something the user is, i.e., biometric data or behavior pattern.

Subsequently, Multi-Factor Authentication (MFA) was proposed to provide a higher level of safety and facilitate continuous protection of computing devices as well as other critical services from unauthorized access by using more than two categories of credentials [27–29]. For the most part, MFA is based on biometrics, which is automated recognition of individuals based on their behavioral [30,31] and biological characteristics [32]. This step offered an improved level of security as the users were required to present the evidence of their identity, which relies on two or more different factors [33]. The discussed evolution of authentication methods is shown in Figure 2.

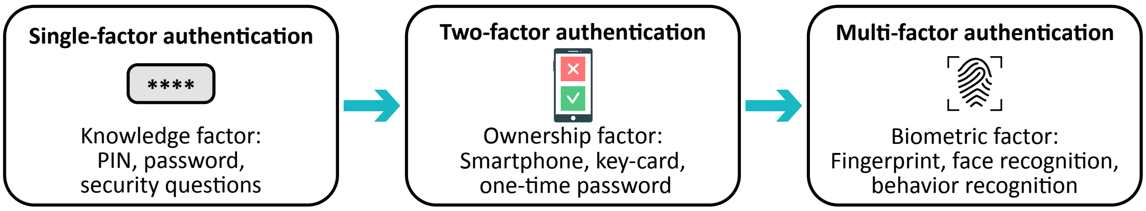

Figure 2. Evolution of authentication methods from SFA to MFA.

Today, MFA is expected to be utilized in scenarios where safety requirements are higher than usual [34,35]. According to SC Media UK, 68 percent of Europeans are willing to use biometric authentication for payments [36]. Consider the daily routine of ATM cash withdrawal [37,38]. Here, the user has to provide a physical token (a card) representing the ownership factor and support it with a PIN code representing the knowledge factor to be able to access a personal account and withdraw money.

This system could be easily made more complex by adding the second channel like, for example, a one-time password to be entered after both the card and the user password were presented [39,40]. In a more interesting scenario, it could be done with the facial recognition methods [41,42]. Moreover, a recent survey discovered that 30 percent of enterprises planned to implement the MFA solution in 2017, with 51 percent claiming that they already utilize MFA, and 38 percent saying that they utilize it in “some areas” of operation [43]. This evidence supports the MFA as an extremely promising direction of the authentication evolution.

As one of the interesting future trends, authentication between a vehicle and its owner or a temporary user may be considered. Based on the statistics [44], a vehicle is stolen every 45 s in the U.S. The current authentication method that allows for starting and using the vehicle is still an immobilizer key [45,46]. The MFA may significantly improve access to most of the electronic devices from both security and user experience perspectives [47,48].

Generally, MFA applications could be divided into three market-related groups: (i) commercial applications [49,50], i.e., account login, e-commerce, ATM, physical access control, etc.; (ii) governmental applications [51,52], i.e., identity documents, government ID, passport, driver’s license, social security, border control, etc.; and (iii) forensic applications [53,54], i.e., criminal investigation, missing children, corpse identification, etc. Generally, the number of scenarios related to authentication is indeed large. Today, MFA becomes an extremely critical factor for:

- Validating the identity of the user and the electronic device (or its system) [55,56];
- Validating the infrastructure connection [57];
- Validating the interconnected IoT devices, such as a smartphone, tablet, wearable device, or any other digital token (key dongle) [58].

Presently, one of the main MFA challenges is the absence of correlation between the user identity and the identities of smart sensors within the electronic device/system [59]. Regarding security, this relationship must be established so that only the legitimate operator, e.g., the one whose identity is authenticated in advance, can gain the access rights [60,61]. At the same time, the MFA process should be as user-friendly as possible, for example:

1. Customers first register and authenticate with the service provider to activate and manage services they are willing to access;
2. Once accessing the service, the user is required to pass a simple SFA with the fingerprint/token signed in advance by the service provider;
3. Once initially accepted by the system, the customer authenticates by logging in with the same username and password as setup previously in the customer portal (or social login).

For additional security, the managing platform can enable secondary authentication factors. Once the user has successfully passed all the tests, the framework automatically authenticates to the service platform;

4. The secondary authentication occurs automatically based on the biometric MFA, so the user would be requested to enter an additional code or provide a token password only in case the MFA fails.

Biometrics indeed significantly contribute to the MFA scheme and can dramatically improve identity proofing by pairing the knowledge factor with the multimodal biometric factors [62,63], thus making it much more difficult for a criminal to eavesdrop on a system while pretending to be another person. However, the utilization of biological factors has its challenges mainly related to the ease of use [64], which largely impacts the MFA system usability.

From the user experience perspective, fingerprint scanner already provides the most widely integrated biometric interface. This is mainly due to its adoption by smartphone vendors on the market [65]. On the other hand, it is not recommended to be utilized as a standalone authentication method [66]. However, the use of any biometrics often requires a set of separate sensing devices. The utilization of already integrated ones allows for reducing the authentication system costs and facilitate the adoption by end users. A fundamental trade-off between usability and security is one of the critical drivers when considering the authentication systems of today [67].

Another challenge is that the use of biometrics relies on a binary decision mechanism [68]. This was well studied over past decades in classical statistical decision theory from the authentication perspective [69,70]. There are various possible solutions to control a slight mismatch of the actual "measured" biometrics and the data stored in previously captured samples. The two widely utilized techniques are: false accept rate (FAR) [71] and false reject rate (FRR) [72]. Manipulations with the decision criteria allow adjusting the authentication framework based on the predefined cost, risks, and benefits. The MFA operation is highly dependent on FAR and FRR, since obtaining zero values for both of the metrics is almost infeasible. The evaluation of more than one biometric feature to establish the identity of an individual can improve the operation of the MFA system dramatically [73].

Since the currently available literature faces a lack of detailed MFA analysis suitable for non-specialists in the field, the main contributions of this work are as follows:

1. This work provides a detailed analysis of factors that are presently utilized for MFA with their corresponding operational requirements. Potential sensors to be utilized are surveyed based on the academic and industrial sources (Section 2);
2. The survey is followed by the challenges related to MFA adoption from both the user experience and the technological perspectives (Section 3);
3. Further, the framework based on the *reversed* Lagrange polynomial is proposed to allow for utilizing MFA in cases where some of the factors are missing (Section 4). A discussion on the potential evaluation methodology is also provided;
4. Finally, the vision of the future of MFA is discussed (Section 5).

2. State-of-the-Art and Potential MFA Sources

Presently, the authentication systems already utilize an enormous number of sensors that enable identification of a user. In this section, we elaborate on the MFA-suitable factors, corresponding market-available sensors, and related challenges. Furthermore, we provide additional details on the ones that are to be potentially deployed in the near future.

2.1. Widely Deployed MFA Sensors/Sources

Today, identification and authentication for accessing sensitive data are one of the primary use cases for MFA. We further list the factors already available for the MFA utilization without acquiring additional specialized equipment.

2.1.1. Password Protection

The conventional way to authenticate a user is to request a PIN code, password, etc. [74]. The secret pass-phrase traditionally represents a knowledge factor. It requires only a simple input device (at least one button) to authenticate the user.

2.1.2. Token Presence

The password could then be supplemented with a physical token—for example, a card, which is recommended as a second factor group—the ownership [75,76]. From the hardware perspective, a user may present a smartcard, phone, wearable device, etc., which are more complicated to delegate [77]. In this case, the system should be equipped with a radio interface allowing for two-way communication with the token [78,79]. On the other hand, the most widely known software token is one-time software generated password [80]. The main drawback of the above is the problem of uncontrollable duplication.

2.1.3. Voice Biometrics

Most of the contemporary smart electronic devices are equipped with a microphone that allows utilizing voice recognition as a factor for MFA [81,82]. At the same time, the technology advancement of tomorrow may allow special agencies not only to recognize the speakers but also to mimic their voices including the intonation, timbre, etc., which is a serious drawback of utilizing voice as a primary authentication method [83,84].

2.1.4. Facial Recognition

As the next step, facial recognition could be considered. At the beginning of its development, the technology was based on the landmark picture analysis, which was relatively simple to replicate by supplying the system with a photo [85]. The next phase was by enabling three-dimensional face recognition, i.e., by asking the user to move head during the authentication process in a specific manner [86,87]. Finally, the advancement of this system reached the point of recognizing the actual expressions of the user [88]. To enable facial recognition, it is required to equip the system with at least one output device and a camera [89].

2.1.5. Ocular-Based Methodology

The iris recognition techniques are on the market for more than 20 years [90]. This approach does not require the user to be close to the capture device while analyzing the color pattern of the human eye [91]. Retina analysis is another attractive technique [92]. Here, a thin tissue composed of neural cells that are located in the posterior portion of the eye is captured and analyzed. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The most prominent challenges in those methods are the need for high quality capture device and robust mathematical technique to analyze the image [93].

2.1.6. Hand Geometry

Some systems employ the analysis of the physical shape of a hand to authenticate the user. Initially, pegs were utilized to validate the subject, but the usability of such methods was low [94]. Further on, the flatbed scanner was used to obtain the image without the need to fix the user's hand in one specific position [95]. Today, some systems utilize conventional cameras not requiring close contact with the capture surface. This approach is, however, not very robust to the environment [96]. Some vendors apply so-called *photoplethysmography* (PPG) to determine whether a wearable device (e.g., a smartwatch) is currently on its user's wrist or not [97,98]. The process is similar to the one followed when measuring heart rate [99].

2.1.7. Vein Recognition

The advances in fingerprint scanners offer an opportunity to collect the vein picture of the finger as well [100]. More complicated devices utilize palm print recognition to acquire and store the shape/movement of the entire hand [101,102]. At the current stage of development, vein biometrics are still vulnerable to spoofing attacks [103,104].

2.1.8. Fingerprint Scanner

Utilizing fingerprint scanner as the primary authentication mechanism is currently being pushed by the majority of smartphone/personal computer vendors [105]. This solution is intuitive to use but remains extremely simple to fabricate—mainly due to the fact that our fingerprints could be obtained from almost anything we touch [106,107]. The integration potential of this method is indeed high [108], even though it is also not recommended to be used as a standalone authentication approach. Most of the smartphone vendors install an additional camera to obtain the fingerprint instead of more safe vein recognition.

2.1.9. Thermal Image Recognition

Similarly to vein recognition, thermal sensor is utilized to reconstruct the unique thermal image of one's body blood flow in proximity [109,110]. Many challenges with this authentication method may arise due to the user conditions: sickness or emotion may significantly influence the perceived figures [111].

2.1.10. Geographical Location

Utilizing the device's and user's geographical location to validate whether access to the device/service could be granted is a special case of location-based authentication [112,113]. Importantly, GPS signal could be easily jammed or considered faulty due to the propagation properties; thus, it is recommended to utilize at least two location sources, for example, GPS and wireless network cell ID [114]. A smartphone could be used to support MFA from the location acquisition perspective.

2.2. Future of MFA Integration

Accelerated adoption across many industries as well as increased availability of biometric services in a wide range of readily-available consumer products is pushing the concept of tight MFA integration. Currently, researchers and early technology adopters attempt to integrate new sensors to be utilized in MFA systems.

2.2.1. Behavior Detection

Back in time, behavior recognition was utilized to analyze military telegraph operator's typing rhythm to track the movement of the troops [115]. Today, gestures for authentication purposes may range from conventional to "hard-to-mimic" ones, since motor-programmed skill results in the movement being organized before the actual execution [116].

A modern example of such identification is the process of tapping the smartphone screen [117,118]. This approach could be easily combined with any text-input authentication methods as a typing pattern is unique for each person [119–121]. In case the MFA system is specifically developed for predefined gesture analysis [122], the user is required to replicate a previously learned movement while holding or wearing the sensing device [123–125].

A natural step of authentication for widely used handheld and wearable devices is the utilization of accelerometer fingerprinting [126,127]. For instance, each smartphone holder could be verified based on the gait pattern by continuously monitoring the accelerometer data that is almost impossible to fake by another individual [128].

For in-vehicle authentication, the integral system is expected to monitor the driver-specific features [129,130], which could be analyzed from two perspectives: (i) vehicle-specific behavior: steering angle sensor, speed sensor, brake pressure sensor, etc. [131,132]; and (ii) human factors: music played, calls made, presence of people in the car, etc. [133]. Another important *blocker*-factor is alcohol sensor. The engine start function could be blocked in case when the level of alcohol in the cabin is above an acceptable legal limit [134].

2.2.2. Beam-Forming Techniques

From the telecommunication perspective, Radio-frequency Identification (RFID) and Near-Field Communication (NFC) techniques have already observed widespread adoption and acceptance within the community [135]. Recent trends in physical-layer security claim that utilizing wireless Multiple-Input and Multiple-Output (MIMO) solutions to locate the source of the signal may become a significant breakthrough in validating the token on the user body [136–138].

2.2.3. Occupant Classification Systems (OCS)

Some vehicular systems already have the OCS solutions integrated in consumer cars [139]. A system of sensors can detect who is currently in the passenger/driver seat by utilizing, for example, weight or posture and automatically adjusting the vehicle to personal needs [140–142].

2.2.4. Electrocardiographic (ECG) Recognition

ECG data could be collected from the user's smart watch or activity tracker and compared with an individually stored pattern [143,144]. The main benefit of using this factor for authentication is that ECG signals emerge as a potential biometric modality with the advantage of being difficult (or close to impossible) to mimic. The only way is by utilizing the existing personal recording [145].

2.2.5. Electroencephalographic (EEG) Recognition

This solution is based on the brain waves analysis and could be considered from the fundamental philosophical proposition "Cogito ergo sum" by R. Descartes, or "I think, therefore I am" [146]. It allows for obtaining a unique sample of the person's brain activity pattern [147]. Formerly, EEG data capture could have been performed only in clinical settings by using invasive probes under the skull or wet-gel electrodes arrayed over the scalp. Today, the simple EEG collection is possible by utilizing market-available devices having the size of a headset [148].

2.2.6. DNA Recognition

Human cell lines are an essential resource for research, which is most frequently used in reverse genetic approaches or as in vitro models of human diseases [149]. It is also a source of unique DNA fingerprinting information [106]. Even though the process is time-consuming and expensive, it may be potentially utilized to pre-authorize the user to the highly secure facility along with other factors.

Subsequently, a comparison of the main indicators for the already deployed and emerging factors [150] is given in Table 1. The factors/sensors are evaluated based on the following parameters:

- *Universality* stands for the presence of factor in each person;
- *Uniqueness* indicates how well the factor differentiates one person from another;
- *Collectability* measures how easy it is to acquire data for processing;
- *Performance* indicates the achievable accuracy, speed, and robustness;
- *Acceptability* stands for the degree of acceptance of the technology by people in their daily life;
- *Spoofing* indicates the level of difficulty to capture and spoof the sample.

Table 1. Comparison of suitable factors for MFA: H—high; M—medium; L—low; n/a—unavailable.

Factor	Universality	Uniqueness	Collectability	Performance	Acceptability	Spoofing
Password	n/a	L	H	H	H	H
Token	n/a	M	H	H	H	H
Voice	M	L	M	L	H	H
Facial	H	L	M	L	H	M
Ocular-based	H	H	M	M	L	H
Fingerprint	M	H	M	H	M	H
Hand geometry	M	M	M	M	M	M
Location	n/a	L	M	H	M	H
Vein	M	M	M	M	M	M
Thermal image	H	H	L	M	H	H
Behavior	H	H	L	L	L	L
Beam-forming	n/a	M	L	L	L	H
OCS	n/a	L	L	L	L	M
ECG	L	H	L	M	M	L
EEG	L	H	L	M	L	L
DNA	H	H	L	H	L	L

However, many other issues are to be addressed while integrating the MFA for the end users. In the following section, we elaborate on those challenges and formalize the recommendations for improved ease of integration.

3. MFA Operation Challenges

An integration of novel solutions has always been a major challenge for both developers and managers. The key challenges are presented in Figure 3. In the first place, user acceptance is a critical aspect for the adoption of strong identity and multi-factor authentication. While adopting and deploying MFA solutions, it is required to follow a careful and thorough approach—where most challenges arise from opportunities and potential benefits [151].

3.1. Usability

The main usability challenges emerging in the authentication process could be characterized from three perspectives [152]:

- *Task efficiency*—time to register and time to authenticate with the system;
- *Task effectiveness*—the number login attempts to authenticate with the system;
- *User preference*—whether the user prefers a particular authentication scheme over another.

In addition to the approaches discussed previously, researchers have already started an investigation of more specific effects in the authentication procedures based on a variety of human factors. The authors of [153] provided a study on how the user age affects the task efficiency in cases of PIN and graphic access mechanisms. It is concluded that younger generation can spend up to 50 percent less time to pass the authentication procedure in both cases. Interestingly, the authors of [154] have shown that gender, in the same case, does not affect the results.

Another direction in the authentication mechanisms usability is related to cognitive properties of the selected human [155]. The work in [156] offered an overview on how to make the passwords memorable while keeping them relatively usable and secure at the same time. Paper by Belk et al. [157] delivered a research on the task completion efficiency and effectiveness among the conventional passwords and the realistic ones. The results revealed that, for most of the participants, the utilization of graphic passwords requires more time than for the textual ones. However, cognitive differences between users, i.e., being Verbal or Imager [152], affect the task completion significantly. Here, Verbals complete the text-based tasks faster than Imagers and vice versa. The work by Ma et al. [158] studied the impact of disability (Down syndrome) in the same two scenarios. It was once again confirmed that textual passwords are utilized better compared to the graphical ones.

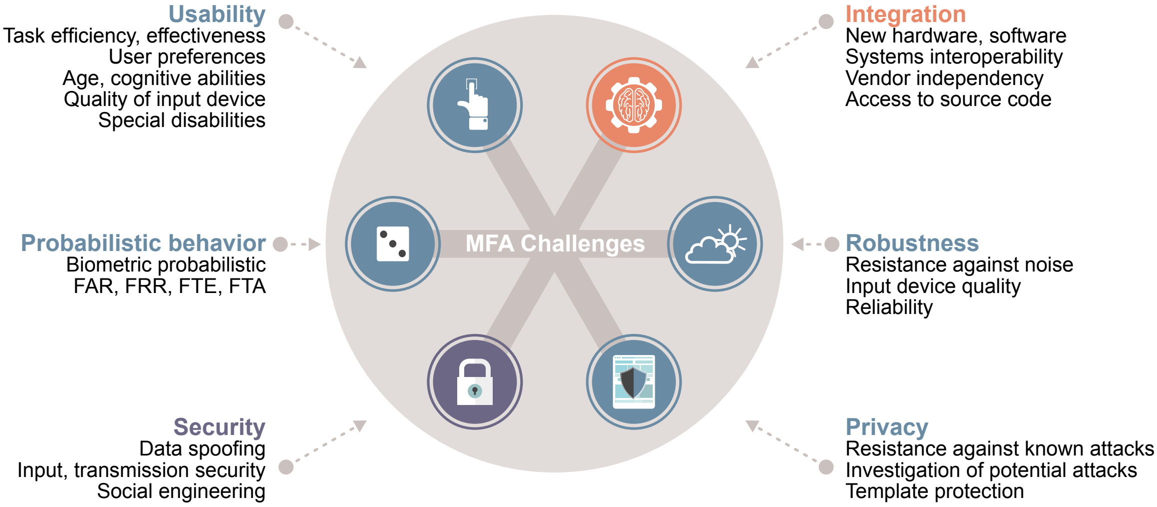

Figure 3. Main operational challenges of MFA.

In addition, the properties of the authentication device play a major role in this process. The authors of [159] investigated the usability of textual passwords on mobile devices. It was proven that using a smartphone or other keyboardless equipment for creating a password suffers from poor usability as compared to conventional personal computers. Another work [160] confirmed the same theory from a task efficiency perspective.

Today, most of the online authentication services are knowledge-based [161], i.e., depend on the username and password combination. More complex systems require the user to interact with additional tokens (one-time passwords, code generators, phones, etc.). Complementing traditional authentication strategies, MFA is not feasible without biometrics. From this perspective, the work in [62] provided an analysis on how gamification and joy can positively impact the adoption of new technology. The gesture-related user experience research conducted in [162] showed that security and user experience do not necessarily need to contradict one other. This work also promoted pleasure as the best way for fast technology adoption. The reference [163] addressed the usability of the ECG solution for authentication, and it was concluded that the application of ECG is not yet suitable for dynamic real-life scenarios.

Many researchers promoted the utilization of personal handheld devices to be utilized during the MFA procedure. Michelin et al. [164] proposed using the smartphone's camera for facial and iris recognition while keeping the decision-making in the cloud. Another work on biometric authentication for an Android device [165] demonstrated an increased level of satisfaction related to higher task efficiency achieved with the MFA solution. Reference [166] studied the usability and practicality of biometric authentication in the workplace. It was concluded that the ease of technology utilization and its environmental context play a vital role—the integration and the adoption will always incur additional and unexpected resource costs.

An extremely important problem of MFA usability roots in the fact that "not all users can use any given biometric system" [167]. People who have lost their limb due to an accident may not be able to authenticate using a fingerprint. Visually impaired people may have difficulties using the iris-based authentication techniques.

Biometric authentication requires an integration of new services and devices that results in the need for additional education during adoption, which becomes more complicated for seniors and due to related *understandability* concerns. One fact is clear—user experience plays a prominent role in successful MFA adoption; some say, "user comes first" [168]. Today, research in usable security for knowledge-based user authentication is in the process of finding a viable compromise between the usability and security—many challenges remain be addressed and will arise soon.

3.2. Integration

Even if all the usability challenges are resolved during the development phase, integration brings further problems from both technological and human perspectives.

Most of the consumer MFA solutions remain hardware-based [52]. Generally, "integrating physical and IT security can reap considerable benefits for an organization, including enhanced efficiency and compliance plus improved security" [169]. However, convergence is not so simple. Related challenges include bringing the physical and the IT security teams together, combining heterogeneous system components, and upgrading the physical access systems.

While developing the MFA system, biometrics independence should be considered carefully, i.e., assurance of interoperability criteria should be met [170]. The framework needs to have functionality to handle the biometric data from sensors other than the initially deployed ones [171]. The utilization of multi-biometrics, that is, simultaneous usage of more than one factor should also be taken into account [172].

Another major interoperability concern is vendor dependency [173]. Enterprise solutions are commonly developed as stand-alone isolated systems that offer an extremely low level of flexibility. Integration of newly introduced to the market sensors would require complicated and costly updates, which most probably will not be considered soon.

Further, it should be noted that most of the currently available MFA solutions are not fully/partially open source. This introduces the questions of trustworthiness and reliability to the third party service providers. The available level of transparency delivered by both hardware and software vendors should be taken into consideration while selecting the MFA framework in the first place.

3.3. Security and Privacy

Any MFA framework is a digital system composed of critical components, such as sensors, data storage, processing devices, and communication channels [174]. All of those are typically vulnerable to a variety of attacks at entirely different levels, ranging from replay attempts to adversary attacks [175]. Security is thus a necessary tool to enable and maintain privacy. Therefore, we begin with the attacks executed on the input device itself [176]. Letting only the legitimate controller access and process sensitive personal data exposes the community to the main risks related to MFA security that are listed further.

The first of the key risks is related to data spoofing that would be successfully accepted by the MFA system [177]. Notably, due to biometrics being used by a variety of MFA frameworks, a glaring opportunity for the attacker to analyze both the technology underlying the sensor and the sensor itself results in revealing the most suitable spoofing materials. The main goal of the system and hardware architects is to provide either a secure environment or, in case it is not possible, to consider the related spoofing possibilities in advance. A risk of capturing either physical or electronic patterns and reproducing them within the MFA system should be addressed carefully.

Conventionally, the safeguard to protect against electronic replay attacks requires utilization of a timestamp [178]. Unfortunately, a biometric spoofing attack is fairly simple to execute [179]. Even though biometrics can improve the performance of the MFA system, they can also increase the number of vulnerabilities that can be exploited by an intruder. Further risk is sensitive data theft during the transmission between the sensor and the processing/storage unit. Such theft may primarily occur due to insecure transmission from the input device through extraction and matching blocks to the database, and there is potential for an attack [180]. The required levels of data safety should be guaranteed to resist against this risk type [181,182].

Another opportunity to attack the MFA system is by capturing the secret data sample [183]. For knowledge factors, the system would be immediately compromised in case zero-knowledge solutions are not utilized [184]. Specific interest is dedicated to capturing a biometric sample that could not be updated or changed over time [185]. Hence, protection of the biometric data requires a higher level of security during capture, transmission, storage, and processing phases [186].

The following risk is related to the theft from the data storage. Conventionally, databases are stored in a centralized manner, which offers a single point of failure [187,188]. At the same time, some of the remote systems contacting the database are not always legitimately authorized to access the personal data stored. High level of isolation is required to protect the data from theft in addition to utilizing irreversible encryption [189]. Subsequent risk is related to location-related attacks. The GPS signal could be vulnerable to position lock (jamming) or to feeding the receiver with false information, so that it computes an erroneous time or location (spoofing) [190,191]. Similar techniques may be applied to cellular- and WLAN-based location services [192,193].

Finally, being an information technology system, MFA framework should deliver relatively high levels of "throughput" [194], which reflects the capability of a system to meet the needs of its users in terms of the number of input attempts per time period [195]. Even if the biometrics are considered suitable in every other aspect, but the system can only perform, e.g., one biometrics-based match per hour, whereas it is required to operate at 100 samples per hour, such a solution should not be considered as feasible. The recommendation here is to select appropriate processing hardware for the server/capture side.

The MFA security framework should also support a penetration testing panel to assess its potential weaknesses. Today, the developers are often conducting external audit to evaluate the risks and act based on such evaluation for more careful planning. The MFA system should thus be assessed to deliver a more secure environment.

3.4. Robustness to Operating Environment

Even if the security and privacy aspects are fully resolved, the biometric systems, mainly fingerprinting, were falling short of fulfilling the "robustness" requirement since the very beginning of their journey [196]. This was mainly due to the operational trials being conducted in the laboratory environment instead of the field tests. One distinct example is voice recognition, which was highly reliable in a silent room but failed to verify the user in urban landscapes.

A similar problem applies to early facial recognition techniques, which failed to operate without adequate light support, quality camera, etc. [197]. The flip side of the coin was the need for continuous supervision of the examined subject. Even today, there are either bits of advice on where to look/place fingers, or there is visual aid available during the security check. The lack of experience in machine-to-human interaction is commonly analyzed with Failure to Enroll (FTE) as well as Failure to Acquire (FTA) rates [198]. They both depend on the users themselves as well as the additive environmental noise.

Since a significant part of MFA is highly dependent on biometry, it could be classified as inherently probabilistic due to such nature [199]. The base of the biometric authentication lies in the field of pattern matching, which in turn relies on approximation. Approximate matching is a critical consideration in any MFA system, since difference between users could be crucial due to a variety of factors and uncertainty. The image captured during a fingerprint scan would be different every time it is observed because of the presentation angle, pressure, dirt, moisture, or differentiation of sensors even if taken of the same person.

Two important error rates used to quantify the performance of a biometric authentication system are FAR and FRR. FAR is the percentage of impostors inaccurately allowed as genuine users. It is defined as the ratio of the *number of false matches* to the *total number of impostor match attempts*. FRR is the number of genuine users rejected from using the system, which is defined as the ratio of the *number of false rejections* to the *total number of genuine match attempts*.

Literature further recommends the utilization of the Crossover Error Rate (CER) in addition to the previously discussed metrics [200]. This parameter is defined as the probability of the system being in a state where FAR equals to FRR. The lower this value is, the better the system performs. According to [201], "Higher FAR is preferred in systems where security is not of prime importance, whereas higher FRR is preferred in high-security applications". The point of equality between FAR and FRR is referred to as Equal Error Rate (EER) [202]. Based on the above, it could be once again concluded that a system utilizing solely biometrics may not be considered as a preferred MFA framework.

By analyzing the above listed challenges, it is possible to evaluate and assess the entire MFA system. In what follows, we propose an approach to enable MFA for vehicular integration based on the availability of a large number of sensors in modern vehicles.

4. Enabling Flexible MFA Operation

In this work, we offer a new authentication scheme that focuses on the vehicle-to-everything (V2X) scenarios, since cars of today are already equipped with multiple sensors that could potentially be utilized for MFA. Conventionally, the user has a username/password/PIN/token [203] and will additionally be asked to utilize a biometric factor, such as facial features or fingerprints. The general overview supported by a follow-up discussion is given in Figure 4. If the authentication procedure fails to establish trust by using this combination of factors, then the user will be prompted to authenticate by utilizing another previously registered factor or a set of those. This MFA system may not only verify the accuracy of the user input but also determine how the user interacts with the devices, i.e., analyze the *behavior*. The more the user interacts with the biometric system, the more accurate its operation becomes.

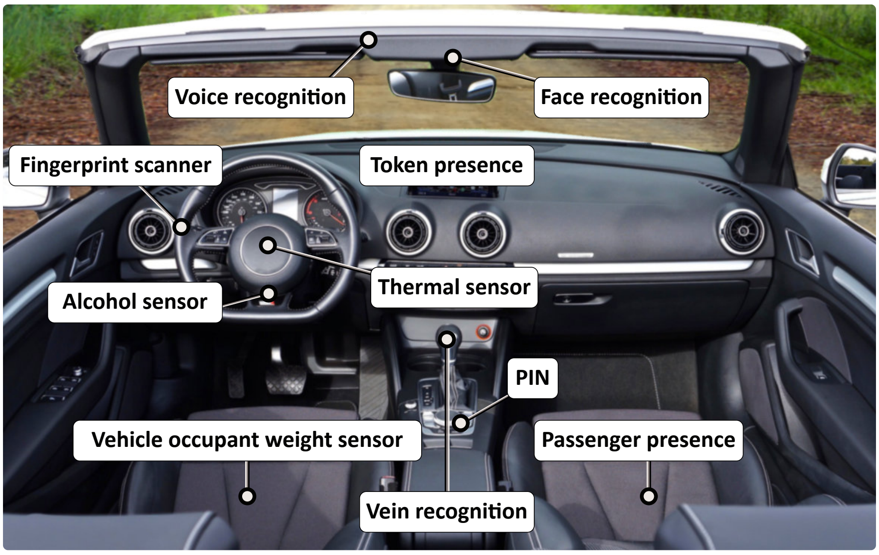

Figure 4. Current and emerging MFA sensors for vehicles.

Another feature of the discussed scenario is the actual sensor usability in case of interaction with a car [204]. If a sensor (e.g., a fingerprint reader) is being utilized and that device is not available from where the user is attempting to log in or gain access—the user experience becomes inadequate. Having a dual-purpose device—smartphone or smartwatch (suitable for executing the information security primitives [205]), which the user already has in his or her possession—as an additional MFA factor (not only as a token) makes both the system costs and usability much more reasonable [206].

The presence of large amounts of sensor data brings us to the logical next step of its application in MFA. We further envision potential utilization of the corresponding factors to authenticate the user without implementing a dedicated "verifier" with the actual biometric data except for the one collected in real time.

4.1. Conventional Approach

One of the approaches considered within the scope of this work is based on utilizing Lagrange polynomials for secret sharing [207]. The system secret S is usually "split" and distributed among a set of key holders. It could be recovered later on, as described in [208–210] and numerous other works, as

$$\begin{aligned} f(x) &= S + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}, \\ f(0) &= S, \end{aligned} \tag{1}$$

where a_i are the generated polynomial indexes and x is a unique identification factor F_i. In such systems, every key holder with a factor ID obtains its own unique key share $S_{ID} = f(ID)$.

In conventional systems, it is required to collect any l shares $\{S_{ID_1}, S_{ID_2}, \dots, S_{ID_l}\}$ of the initial secret to unlock the system, while the curve may offer $n > l$ points, as it is shown in Figure 5. The basic principle behind this approach is to specify the secret S and use the generated curve based on the random coefficients a_i to produce the secret shares S_i. This methodology is successfully utilized in many secret sharing systems that employ the Lagrange interpolation formula [211,212].

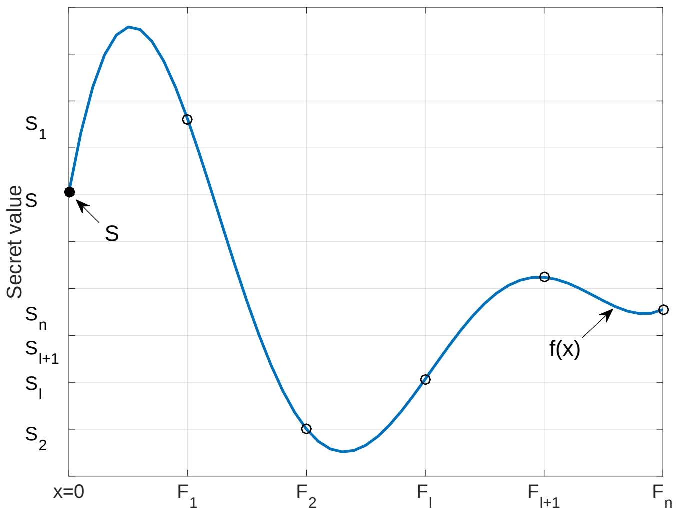

Figure 5. Lagrange secret sharing scheme.

Unfortunately, this approach may not be applied for the MFA scenario directly [213], since the biometric parameters are already in place, i.e., we can neither assign a new S_i to a user nor modify them. On the one hand, the user may set some of the personal factors, such as password, PIN-code, etc. On the other hand, some of them may be unchangeable (biometric parameters and behavior attributes). In this case, an inverse task where the shares of the secret S_{ID_i} are known as factor values S_i is to be solved. Basically, S_i are fixed and become unique $\{S_1, S_2, \dots, S_l\}$ when set for a user. In this case, S is the secret for accessing the system and should be acquired with the user factor values. A possible solution based on the *reversed* Lagrange interpolation formula is proposed in the following subsection.

4.2. Proposed Reversed Methodology

In this work, we consider the MFA system with explicit l factors F. Each factor F_i has a unique secret S_i obtained with the corresponding procedure (PIN, fingerprint, etc.) from the user. In the worst case, it is related to the biometric data—the probability that it changes over time is low. The corresponding factors and secrets could then be represented as

$$\begin{aligned} &F_1 : S_1, \\ &F_2 : S_2, \\ &\ldots \\ &F_l : S_L, \\ &F_{l+1} : T, \end{aligned} \tag{2}$$

where S_i is the secret value obtained from the sensor (factor), l is the number of factors required to reconstruct the secret, and F_{l+1} is a timestamp collected at time instant T.

It is important to note that providing the actual secrets to the verifier is not an option, especially in case of sensitive biometric data, because a fingerprint is typically an unchangeable factor. Hence, letting even a trusted instance obtain the corresponding data is a questionable step to make. Conversely, compared to the method considered in Section 4.1, the *modified algorithm implies that S_i are obtained from the factors* (only one polynomial describes the corresponding curve), as it is shown in Figure 5. In other words, the proposed methodology produces the system secret S based on the collected factor values S_i instead of assigning them in the first place.

A system of equations connected to the Lagrange interpolation formula with the factors, their values, and the secret for the system access is

$$\begin{cases} S_1 = \overline{S} + a_1 F_1 + a_2 F_1^2 + \cdots + a_{l-1} F_1^{l-1} + a_l F_1^l, \\ S_2 = \overline{S} + a_1 F_2 + a_2 F_2^2 + \cdots + a_{l-1} F_2^{l-1} + a_l F_2^l, \\ \ldots \\ S_l = \overline{S} + a_1 F_l + a_2 F_l^2 + \cdots + a_{l-1} F_l^{l-1} + a_l F_l^l, \\ T = \overline{S} + a_1 T + a_2 T^2 + \cdots + a_{l-1} T^{l-1} + a_l T^l, \end{cases} \tag{3}$$

where a_i are the corresponding generated coefficients, $f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}$, and $f(0) = S$. The system in Equation (3) has only one solution for S and it is well known from the Lagrange interpolation formula.

Lemma 1. *One and only one polynomial curve $f(x)$ of degree $l-1$ could be described by l points on the plane $(x_1, y_1), (x_2, y_2), \ldots, (x_l, y_l)$*

$$f_x = a_0 + a_1 x + \ldots + a_{l-1} x^{l-1}, \{f(x_i) = y_i\}_{i=1}^{l}.$$

Hence, the system secret S may be recovered based on l collected shares as given by the conventional Lagrange interpolation formula without the need to transfer the *original* factor secrets S_i to the verifier. Hence, the sensitive person-related data is kept private, as

$$S = (-1)^l \sum_{i=1}^{l+1} S_i \prod_{j=1, j \neq i}^{l+1} \frac{F_j}{F_i - F_j}, \tag{4}$$

where $F_{l+1} = T$. The proposed modifications are required to assure the uniqueness of the acquired data, see Figure 6.

Due to the properties of the Lagrange formulation, there can only be one curve described by the corresponding polynomial (Lemma 1); therefore, each set of $\overline{[F_i : S_i]}$ will produce its unique $\overline{S}$. However, if the biometric data collected by MFA has not been changed over time, the secret will always remain the same, which is an obvious vulnerability of the considered system. On the other hand, a simple addition of the timestamp should always produce a unique curve, as it is shown in Figure 6 for T, T_1, and T_2.

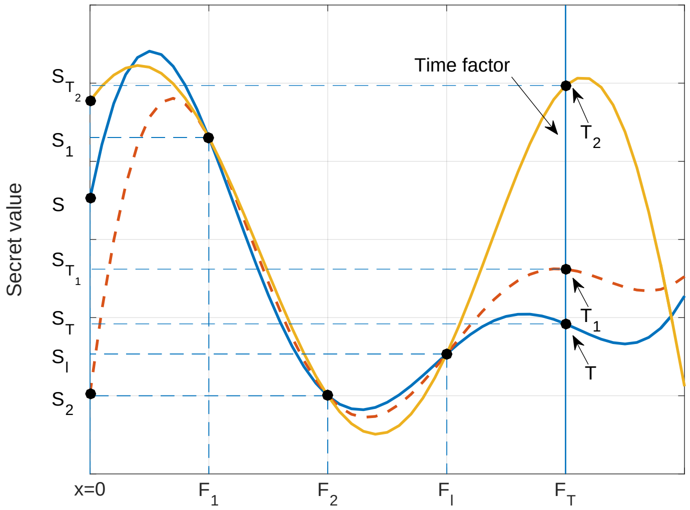

Figure 6. Reversed method based on the Lagrange polynomial.

The proposed solution provides robustness against the case where all S_i remain unchanged over time. This is achieved by adding a unique factor of time T, which enables the presence of F_l with the corresponding secret. It is necessary to mention that the considered threshold scheme based on the Lagrange interpolation formula utilizes Rivest–Shamir–Adleman (RSA) mechanism or ElGamal encryption/decryption algorithm for authentication during the final step. In this case, it is proven that we obtain a secure threshold scheme related to secrets S_i in [214].

4.3. *Proposed MFA Solution for V2X Applications*

Indeed, our proposed solution may operate out-of-the-box in case where all l factors are present. The system may thus provide a possibility to identify and report any outdated factor information—for example, weight fluctuation [215]. Access to a service could be automated when some of the factors are not present [216]. We further elaborate on this feature in the current subsection.

4.3.1. Factor Mismatch

Assuming that the number of factors in our system is $l = 4$, the system secret S can be represented in a simplified way as a group of

$$S \leftarrow \begin{bmatrix} F_1 & F_2 & F_3 & F_4 \end{bmatrix}.$$

Here, if any of S_i are modified—the secret recovery mechanism would fail. An improvement to this algorithm is delivered by providing separate system solutions $\overline{S_i}$ for a lower number of factors collected. Basically, for $\bar{l} = 3$, the number of possible combinations of factors with one missing is equal to four, as follows

$$\begin{aligned} \overline{S_1} &\leftarrow \begin{bmatrix} F_1 & F_2 & F_3 \end{bmatrix}, \\ \overline{S_2} &\leftarrow \begin{bmatrix} F_1 & F_3 & F_4 \end{bmatrix}, \\ \overline{S_3} &\leftarrow \begin{bmatrix} F_1 & F_2 & F_4 \end{bmatrix}, \\ \overline{S_3} &\leftarrow \begin{bmatrix} F_2 & F_3 & F_4 \end{bmatrix}. \end{aligned} \quad (5)$$

The device may thus grant access based on a predefined risk function policy. As the second benefit, it can inform the user (or the authority) that a particular factor F_i has to be updated based on the failed S_i combination. Indeed, this modification brings only marginal transmission overheads, but, on the other hand, enables higher flexibility in authentication and missing factor validation.

4.3.2. Cloud Assistance

Another important scenario for MFA is potential assistance of the trusted authority in $F_i : S_i$ mismatch or loss. In case when the user fails to present a sufficient number of factors, the trusted authority can be requested to provide the temporary factor keys, as it is demonstrated in Figure 7.

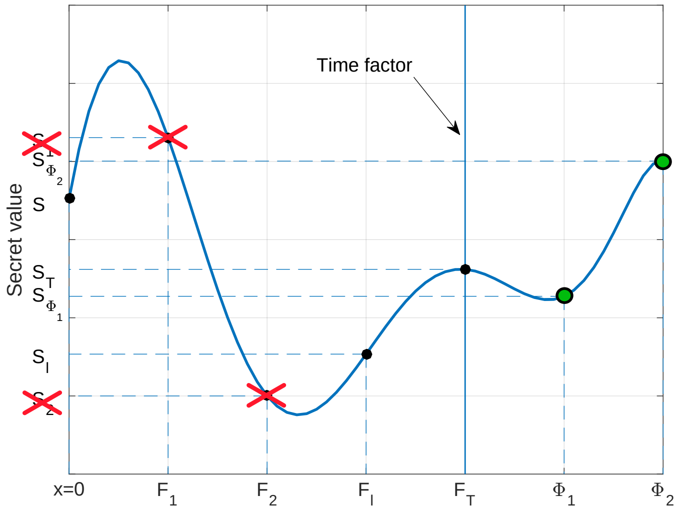

Figure 7. Trusted authority assistance in authentication when user is missing two factors.

For example, assume that the user forgot or lost two factors F_2 and F_3 with the corresponding keys $S_1 = f(F_1)$ and $S_2 = f(F_2)$. The trusted authority is willing to assist in authentication—two temporary keys $S_{\Phi_1} = f(\Phi_1)$ and $S_{\Phi_2} = f(\Phi_2)$ are thus generated and sent to the user via a secure channel. Obtaining these keys and applying the Lagrange interpolation formula with RSA or ElGamal encryption/decryption-based threshold authentication procedure involves the following factors and keys

$$\begin{aligned} &F_1 : S_1, \\ &F_2 : S_2, \\ &\ldots \\ &F_l : S_L, \\ &F_{l+1} : T, \\ &\Phi_1 : S_{\Phi_1}, \\ &\Phi_2 : S_{\Phi_2}, \end{aligned} \tag{6}$$

as described in [214]. This allows for gaining access to the device.

The proposed solution is designed explicitly to complete the MFA step of the authentication, that is, its usage for SFA and 2FA is not recommended. This is mainly due to the features of the Lagrange interpolation formula. Basically, in the SFA case and without the $F_{l+1} : T$ factor, the equation at hand can be simply represented as $S_1 = S + b_1F_1$, i.e., it will become 'a point'. Even adding a random timestamp factor will not provide any valuable level of biometric data protection, since an eavesdropper could be able to immediately recover the factor secret.

The above is not suitable for the 2FA either, since providing two factors allows the curve to have linear behavior, i.e., the eavesdropper is required two attempts to recover the secrets. However, adding a timestamp factor here allows for providing the necessary level of safety with three actual factors, as discussed below.

4.4. Potential Evaluation Techniques

Conventionally, authentication systems utilizing only the knowledge of ownership factors operate in pass/fail mode, i.e., the input data is either correct or incorrect. When it comes to using biometrics, the system faces potential errors during the biometric sample capturing, which was discussed previously in Section 3.4. We further elaborate on our proposed methodology from the crucial FAR/FRR perspective.

Typically, the FAR/FRR parameters of a sensor are provided by vendors based on the statistically collected data [217]. For the MFA framework, we assume two possible decisions made during the user authentication phase, as it is displayed in Figure 8: (i) H_0—the user is not legitimate; or (ii) H_1—the user is legitimate. These form the entire sample space of $P(H_0) + P(H_1) = 1$. The risk policy is assumed to be handled by the authentication system owner who also sets up the distributions of $P(H_0)$ and $P(H_1)$.

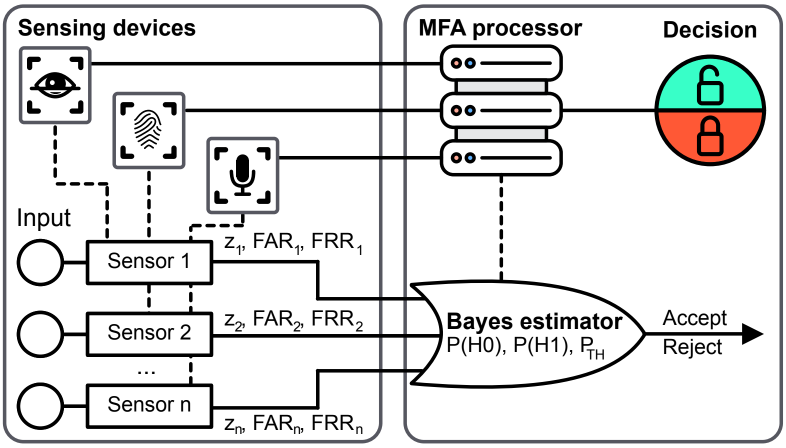

Figure 8. MFA system mode. P_{TH} is the selected threshold.

Generalizing, there might be n biometric sensors collecting the user input data. Each individual sensor measurement from the set $Z = \{z_1, \ldots, z_n\}$ is distributed within $[0, 1]$, and this set is further analyzed under the conditions of two previously considered hypotheses. The measurements delivered from the sensors could be processed in two different ways as introduced in the sequel.

4.4.1. Strict Decision Methodology

Each sensor decides whether the user is legitimate or not by returning either *accept* or *reject*. The MFA system then combines the collected results and provides a group decision based on the resulting vector. Hence, it is possible to utilize the threshold decision functions or weighted threshold functions depending on the reliability of the sensor.

For the first case, the sensor will return the value $z_i, z_i = [0; 1]$, which could be interpreted as either *YES* or *NO*. Then, the conditional probabilities $P\left(z_i \left| H_0 \right.\right)$ and $P\left(z_i \left| H_1 \right.\right)$ are defined by FAR_i and FRR_i values, respectively, for i-th sensor. Here, FAR_i and FRR_i are taken at the CER/EER point, e.g., z_i is selected at the point where $FAR_i = FRR_i$. Generally, this methodology reflects the scenarios of ownership or knowledge factors from the biometric perspective.

4.4.2. Probabilistic Decision Methodology

The sensor responds with a result of its measurements as well as a probabilistic characteristics. Further, the data is merged before the final decision is made. Therefore, the entire set of the measured data could be utilized when making a group decision and, accordingly, a common result might be established based on the set collected from all sensors.

In the second case, the sensor returns a result of the measurements as well as the template comparison in the form of a match score z_i $(0 \leq z_i \leq 1)$. For each of the values z_i, the conditional probability $P\left(z_i \left| H_0\right.\right)$ is calculated based on the FAR_i values at z_i. In addition, the conditional probability $P\left(z_i \left| H_1\right.\right)$ is determined by FRR_i values at z_i.

This approach offers an opportunity to consider the strict decision methodology as a simplified model of the probabilistic one for the case where FAR_i and FRR_i are given only in one point. Here, the measurement result can only take two values, i.e., higher or lower than the selected threshold.

4.4.3. Evaluation

In this work, we consider a more general case of the probabilistic decision-making methodology, while a combination of the measurement results for the individual sensors is made similarly to the previous works by using the Bayes estimator [218]. Since the outcomes of measurements have a probabilistic nature, the decision function is suitable for the maximum a posteriori probability solution.

In more detail, the decision function may be described as follows. At the input, it requires a conditional probability of the measured value from each sensor $P\left(z_i \left| H_0\right.\right)$ and $P\left(z_i \left| H_1\right.\right)$ together with a priori probabilities of the hypotheses $P(H_0)$ and $P(H_1)$. The latter values could be a part of the company's risk policy as they determine the degree of confidence for specific users. Then, the decision function evaluates the a posteriori probability of the hypothesis $P\left(H_1 \left| Z\right.\right)$ and validates that the corresponding probability is higher than a given threshold P_{TH}.

The measurement-related conditional probabilities can be considered as independent random variables; hence, the general conditional probability is as follows:

$$P\left(Z \left| H_J\right.\right) = \prod_{z_i \in Z} P\left(z_i \left| H_J\right.\right), J \in \{0;1\}\,. \tag{7}$$

Further, the total probability $P(Z)$ is calculated as

$$P(Z) = \prod_{z_i \in Z} P\left(z_i \left| H_0\right.\right) P(H_0) + \prod_{z_i \in Z} P\left(z_i \left| H_1\right.\right) P(H_1), \tag{8}$$

where $P\left(z_i \left| H_J\right.\right), J \in \{0;1\}$ are known from the sensor characteristics, while $P(H_0)$ and $P(H_1)$ are a priori probabilities of the hypotheses (a part of the company's risk policy).

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

$$P\left(H_1 \left| Z\right.\right) = \frac{\prod_{z_i \in Z} P\left(z_i \left| H_1\right.\right) P(H_1)}{P(Z)}. \tag{9}$$

For a comprehensive decision over the entire set of sensors, the following rule applies

$$P\left(H_1 \left| Z\right.\right) > P_{TH} \Rightarrow \{Accept\}, \text{else } \{Reject\}. \tag{10}$$

As a result, the decision may be correct or may lead to an error. The FAR and FRR values could then be utilized for selecting the appropriate threshold P_{TH} based on all of the involved sensors.

5. Discussion and Future Prospects

Today, authentication matters more than ever before. In the digital era, most users will rely on biometrics in matters concerning systems security and authorization to complement the conventional passwords. Even though privacy, security, usability, and accuracy concerns are still in place, MFA becomes a system that promises the security and ease of use needed for modern users while acquiring access to sensitive data.

Without a doubt, biometrics are one of the key layers to enable the future of MFA. This functionality is often regarded not standalone but as a supplement to traditional authentication approaches like passwords, smart cards, and PINs. Combining two or more authentication mechanisms is expected to provide a higher level of security when verifying the user. The expected evolution towards MFA is rooted in the synergistic biometric systems that allow for significantly improved user experience and MFA system throughput, which would be beneficial for various applications (see Figure 9). Such systems will intelligently couple all three factor types, namely, knowledge, biometrics, and ownership.

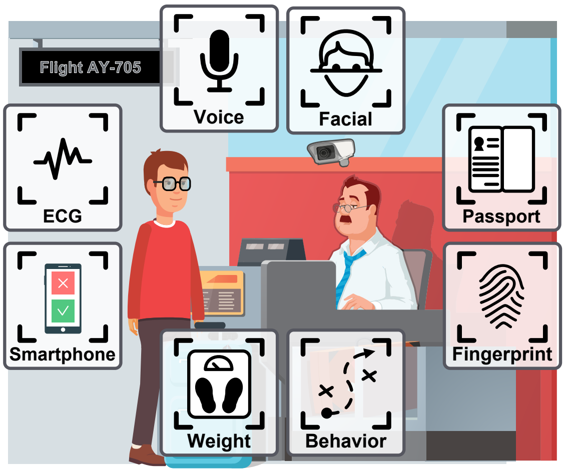

Figure 9. Biometric MFA for the airport scenario.

Since conventional single-factor systems of today are based on only one parameter (unimodality property), if its acquisition is affected in any way (be it noise or disruption), the overall accuracy will degrade. As a reminder, collecting a single type of non-knowledge related data, e.g., biometrics, could exclude part of the user population when particular disabilities are present. Moreover, spoofing this only factor is a relatively simple task.

One of the most promising directions in MFA is behavior-based biometrics providing entirely new ways of authenticating the users. The solutions that are based on muscular memory, e.g., writing or gestures, coupled with machine learning become more prominent examples. Already today, software can extrapolate user handwriting and reach the confidence levels of above 99.97 percent [219]. More forward-looking MFA sources to be utilized in the nearest future are heart and brain [220]. The attractive area of ECG and EEG analysis is also expected to provide unique identification samples for each subject.

Another military-inspired research activity already shows the capability to identify the users based on the way they interact with computer [221]. This approach takes into consideration the typing speed, typical spelling mistakes, writing rhythm, and other factors [222]. The appropriate terminology is not settled yet, and some call this methodology Passive Biometrics [223], while others name it Continuous Authentication [224]. It results in having a unique fingerprint of the user–computer interaction pattern, which is extremely difficult to replicate.

All of the discussed MFA scenarios require significant memory resources to statistically analyze the input data and store the biometric samples even if utilizing different optimization techniques [225,226]. A very promising direction of the MFA development is therefore in the area of *neural networks* and *Big Data* [227]. Here, many successful applications have been known to the community for more than a decade. Examples could be found in [228–230] where conventional factors, such as iris, retina, fingerprints, etc., are considered. Utilizing neural networks for the next-generation biometrics is the most likely way to proceed due to presently high levels of the analysis complexity [231,232].

In summary, biometric technology is a prominent direction driven by the mobile device market. The number of smartphones to be sold only in the US is expected to reach 175 million units by 2018 with the corresponding market to exceed $50.6B in revenues by 2022 [233,234]. It is believed that a strong push towards the utilization of biometrics in many areas of life is imminent, since most of the flagman devices are already equipped with the fingerprint scanner and facial recognition technology in addition to convention PIN codes.

This work provided a systematic overview of the state-of-the-art in both technical and usability issues, as well as the major challenges in currently available MFA systems. In this study, we discussed the evolution of authentication from single- through two- and towards multi-factor systems. Primarily, we focused on the MFA factors constituting the state-of-the-art, future possible directions, respective challenges, and promising solutions. We also proposed an MFA solution based on the reversed Lagrange polynomial as an extension of Shamir's Secret Sharing scheme, which covers the cases of authenticating the user even if some of the factors are mismatched or absent. It also helps qualify the missing factors without disclosing the sensitive data to the verifier.

Acknowledgments: The work of the second author is supported by the Academy of Finland.

Author Contributions: A.O. prepared the state-of-the-art; N.M. and T.M. conducted the analysis of challenges; S.B. designed the flexible MFA solution; A.O., S.B., N.M., S.A., T.M, and Y.K. wrote the paper.

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

Abbreviations

MFA	Multi-Factor Authentication
SFA	Single-Factor Authentication
2FA	Two-Factor Authentication
SSS	Shamir's Secret Sharing
PIN	Personal Identification Number
ID	Identification Number
ATM	Automated Teller Machine
FAR	False Accept Rate
FRR	False Reject Rate
PPG	Photoplethysmography
RFID	Radio-Frequency Identification
NFC	Near-Field Communication
OCS	Occupant Classification Systems
ECG	Electrocardiography
EEG	Electroencephalography
GPS	Global Positioning System
FTE	Failure to Enroll
FTA	Failure to Acquire
CER	Crossover Error Rate
EER	Equal Error Rate
V2X	Vehicle-to-Everything
IAM	Identity and Access Management

References

1. VNI Cisco Global Mobile Data Traffic Forecast 2016–2021. White Paper, 2017. Available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf (accessed on 4 January 2018).
2. Roy, S.; Khatwani, C. Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols. *Cryptography* **2017**, *1*, 9.

3. Dworkin, M.J. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. Special Publication (NIST SP)-800-38B 2016. Available online: https://www.nist.gov/publications/recommendation-block-cipher-modes-operation-cmac-mode-authentication-0 (accessed on 4 January 2018).
4. Alomar, N.; Alsaleh, M.; Alarifi, A. Social authentication applications, attacks, defense strategies and future research directions: A systematic review. *IEEE Commun. Surv. Tutor.* **2017**, doi:10.1109/COMST.2017.2651741.
5. Lamport, L. Password authentication with insecure communication. *Commun. ACM* **1981**, *24*, 770–772.
6. Benarous, L.; Kadri, B.; Bouridane, A. A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions. In *Biometric Security and Privacy*; Springer: Berlin, Germany, 2017; pp. 371–411.
7. Boyd, C.; Mathuria, A. *Protocols for Authentication and Key Establishment*; Springer: Berlin, Germany, 2013.
8. Mohsin, J.; Han, L.; Hammoudeh, M.; Hegarty, R. Two Factor vs. Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; ACM: New York, NY, USA, 2017; p. 39.
9. Pathan, A.S.K. *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*; CRC Press: Boca Raton, FL, USA, 2016.
10. Balloon, A.M. From Wax Seals to Hypertext: Electronic Signatures, Contract Formation, and a New Model for Consumer Protection in Internet Transactions. *Emory Law J.* **2001**, *50*, 905.
11. Danny T. MFA (Multi-Factor Authentication) with Biometrics. 2017. Available online: https://www.bayometric.com/mfa-multi-factor-authentication-biometrics/ (accessed on 4 Jaurnay 2018).
12. Konoth, R.K.; van der Veen, V.; Bos, H. How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany, 2016; pp. 405–421.
13. Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. *J. Inf. Process. Syst.* **2011**, *7*, 187–198.
14. Dasgupta, D.; Roy, A.; Nag, A. Toward the design of adaptive selection strategies for multi-factor authentication. *Comput. Secur.* **2016**, *63*, 85–116.
15. Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F. Passwords and the evolution of imperfect authentication. *Commun. ACM* **2015**, *58*, 78–87.
16. Wang, D.; Wang, P. Offline dictionary attack on password authentication schemes using smart cards. In *Information Security*; Springer: Berlin, Germany, 2015; pp. 221–237.
17. Ah Kioon, M.C.; Wang, Z.S.; Deb Das, S. Security analysis of MD5 algorithm in password storage. *Appl. Mech. Mater.* **2013**, *347*, 2706–2711.
18. Heartfield, R.; Loukas, G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Comput. Surv. (CSUR)* **2016**, *48*, 37.
19. Grassi, P.A.; Fenton, J.L.; Newton, E.M.; Perlner, R.A.; Regenscheid, A.R.; Burr, W.E.; Richer, J.P.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; et al. *NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.
20. Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Comput. Secur.* **2011**, *30*, 208–220.
21. Schneier, B. Two-factor authentication: Too little, too late. *Commun. ACM* **2005**, *48*, 136.
22. Petsas, T.; Tsirantonakis, G.; Athanasopoulos, E.; Ioannidis, S. Two-factor authentication: Is the world ready?: Quantifying 2FA adoption. In Proceedings of the 8th European Workshop on System Security, Bordeaux, France, 21 April 2015; ACM: New York, NY, USA, 2015; p. 4.
23. Wang, D.; He, D.; Wang, P.; Chu, C.H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 428–442.
24. Sun, J.; Zhang, R.; Zhang, J.; Zhang, Y. Touchin: Sightless two-factor authentication on multi-touch mobile devices. In Proceedings of the Conference on Communications and Network Security (CNS), San Francisco, CA, USA, 29–31 October 2014; pp. 436–444.
25. Bruun, A.; Jensen, K.; Kristensen, D. Usability of Single- and Multi-factor Authentication Methods on Tabletops: A Comparative Study. In Proceedings of the International Conference on Human-Centred Software Engineering, Paderborn, Germany, 16–18 September 2014; Springer: Berlin, Germany, 2014; pp. 299–306.

26. Harini, N.; Padmanabhan, T.R. 2CAuth: A new two factor authentication scheme using QR-code. *Int. J. Eng. Technol.* **2013**, *5*, 1087–1094.
27. Scheidt, E.M.; Domangue, E. Multiple Factor-Based User Identification and Authentication. U.S. Patent 7,131,009, 31 October 2006.
28. Bhargav-Spantzel, A.; Squicciarini, A.C.; Modi, S.; Young, M.; Bertino, E.; Elliott, S.J. Privacy preserving multi-factor authentication with biometrics. *J. Comput. Secur.* **2007**, *15*, 529–560.
29. Banyal, R.K.; Jain, P.; Jain, V.K. Multi-factor authentication framework for cloud computing. In Proceedings of the Fifth International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), Seoul, Korea, 24–25 September 2013; pp. 105–110.
30. Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 136–148.
31. Jorgensen, Z.; Yu, T. On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; ACM: New York, NY, USA, 2011; pp. 476–482.
32. National Research Council; Whither Biometrics Committee. *Biometric Recognition: Challenges and Opportunities*; National Academies Press: Washington, DC, USA, 2010.
33. Huang, X.; Xiang, Y.; Bertino, E.; Zhou, J.; Xu, L. Robust multi-factor authentication for fragile communications. *IEEE Trans. Dependable Secur. Comput.* **2014**, *11*, 568–581.
34. Tahir, H.; Tahir, R. BioFIM: Multifactor Authentication for Defeating Vehicle Theft. In Proceedings of the World Congress on Engineering, London, UK, 2–4 July 2008; Volume 1, pp. 1–3.
35. Coventry, L.; De Angeli, A.; Johnson, G. Usability and biometric verification at the ATM interface. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, FL, USA, 5–10 April 2003; ACM: New York, NY, USA, 2003; pp. 153–160.
36. SC Media UK. 68% of Europeans Want to Use Biometric Authentication for Payments. 2016. Available online: https://www.scmagazineuk.com/68-of-europeans-want-to-use-biometric-authentication-for-payments/article/530818/ (accessed on 4 January 2018).
37. Khan, R.; Hasan, R.; Xu, J. SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices. In Proceedings of the 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco, CA, USA, 30 March–3 April 2015; pp. 41–50.
38. Adeoye, O.S. Evaluating the performance of two-factor authentication solution in the banking sector. *Int. J. Comput. Sci.* **2012**, *9*, 457–462.
39. Aloul, F.; Zahidi, S.; El-Hajj, W. Two factor authentication using mobile phones. In Proceedings of the International Conference on Computer Systems and Applications, Rabat, Morocco, 10–13 May 2009; pp. 641–644.
40. Ometov, A.; Bezzateev, S.; Kannisto, J.; Harju, J.; Andreev, S.; Koucheryavy, Y. Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things. *IEEE Internet Things J.* **2017**, *4*, 843–854, doi:10.1109/JIOT.2016.2593898.
41. Parmar, D.N.; Mehta, B.B. Face recognition methods & applications. *arXiv* **2014**, arXiv:1403.0485.
42. Sunehra, D. Fingerprint based biometric ATM authentication system. *Int. J. Eng. Invent.* **2014**, *3*, 22–28.
43. Security Intelligence. The Move to Multifactor Authentication: Are Passwords Past Their Prime? 2016. Available online: https://securityintelligence.com/news/the-move-to-multifactor-authentication-are-passwords-past-their-prime/ (accessed on 4 January 2018).
44. National Highway Traffic Safety Administration. Learn How to Protect Your Car. 2016. Available online: https://www.nhtsa.gov/vehicle-theft-prevention (accessed on 4 January 2018).
45. Garcia, F.D.; Oswald, D.; Kasper, T.; Pavlidès, P. Lock It and Still Lose It-on the (in) Security of Automotive Remote Keyless Entry Systems. In Proceedings of the USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016.
46. Verdult, R.; Garcia, F.D.; Ege, B. Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer. In Proceedings of the USENIX Security Symposium, Washington, DC, USA, 14–16 August 2013; pp. 703–718.
47. Symeonidis, I.; Mustafa, M.A.; Preneel, B. Keyless car sharing system: A security and privacy analysis. In Proceedings of the IEEE International Smart Cities Conference (ISC2), Trento, Italy, 12–15 September 2016; pp. 1–7.

48. Dmitrienko, A.; Plappert, C. Secure free-floating car sharing for offline cars. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, Scottsdale, AZ, USA, 22–24 March 2017; ACM: New York, NY, USA, 2017; pp. 349–360.
49. Neha; Chatterjee, K. Authentication techniques for e-commerce applications: A review. In Proceedings of the International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016; pp. 693–698.
50. Fan, K.; Ge, N.; Gong, Y.; Li, H.; Su, R.; Yang, Y. An ultra-lightweight RFID authentication scheme for mobile commerce. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 368–376.
51. Nor, N.A.; Narayana Samy, G.; Ahmad, R.; Ibrahim, R.; Maarop, N. The Proposed Public Key Infrastructure Authentication Framework (PKIAF) for Malaysian Government Agencies. *Adv. Sci. Lett.* **2015**, *21*, 3161–3164.
52. Labati, R.D.; Genovese, A.; Muñoz, E.; Piuri, V.; Scotti, F.; Sforza, G. Biometric recognition in automated border control: A survey. *ACM Comput. Surv. (CSUR)* **2016**, *49*, 24.
53. Grigoras, C. Applications of ENF analysis in forensic authentication of digital audio and video recordings. *J. Audio Eng. Soc.* **2009**, *57*, 643–661.
54. Gill, P.; Jeffreys, A.J.; Werrett, D.J. Forensic application of DNA 'fingerprints'. *Nature* **1985**, *318*, 577–579.
55. Han, K.; Potluri, S.D.; Shin, K.G. On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. In Proceedings of the International Conference on Cyber-Physical Systems (ICCPS), Philadelphia, PA, USA, 8–11 April 2013; pp. 160–169.
56. Ishtiaq Roufa, R.M.; Mustafaa, H.; Travis Taylora, S.O.; Xua, W.; Gruteserb, M.; Trappeb, W.; Seskarb, I. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In Proceedings of the 19th USENIX Security Symposium, Washington, DC, USA, 11–13 August 2010; pp. 11–13.
57. Chaurasia, B.K.; Verma, S. Infrastructure based authentication in VANETs. *Int. J. Multimed. Ubiquitous Eng.* **2011**, *6*, 41–54.
58. Rossi, B. Connected car security: why identity should be in the driving seat. 2016. Available online: http://www.information-age.com/connected-car-security-why-identity-should-be-driving-seat-123461078/ (accessed on 4 January 2018).
59. Kleberger, P.; Olovsson, T.; Jonsson, E. Security aspects of the in-vehicle network in the connected car. In Proceedings of the Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 5–9 June 2011; pp. 528–533.
60. Calandriello, G.; Papadimitratos, P.; Hubaux, J.P.; Lioy, A. Efficient and robust pseudonymous authentication in VANET. In Proceedings of the 4th International Workshop on Vehicular ad hoc Networks, Montreal, QC, Canada, 9–14 September 2007; ACM: New York, NY, USA, 2007; pp. 19–28.
61. Yang, Y.; Wei, Z.; Zhang, Y.; Lu, H.; Choo, K.K.R.; Cai, H. V2X security: A case study of anonymous authentication. *Pervasive Mob. Comput.* **2017**, *41*, 259–269.
62. De Luca, A.; Hang, A.; Von Zezschwitz, E.; Hussmann, H. I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; ACM: New York, NY, USA, 2015; pp. 1411–1414.
63. Clarke, N. *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling*; Springer: Berlin, Germany, 2011.
64. Rane, S.; Wang, Y.; Draper, S.C.; Ishwar, P. Secure biometrics: Concepts, authentication architectures, and challenges. *IEEE Signal Process. Mag.* **2013**, *30*, 51–64.
65. Bhagavatula, C.; Ur, B.; Iacovino, K.; Kywe, S.M.; Cranor, L.F.; Savvides, M. Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption. In Proceedings of the Usable Security (USEC), San Diego, CA, USA, 21 February 2016; pp. 1–10.
66. Wimberly, H.; Liebrock, L.M. Using fingerprint authentication to reduce system security: An empirical study. In Proceedings of the Symposium on Security and Privacy (SP), Berkeley, CA, USA, 22–25 May 2011; pp. 32–46.
67. De Cristofaro, E.; Du, H.; Freudiger, J.; Norcie, G. A comparative usability study of two-factor authentication. *arXiv* **2013**, arXiv:1309.5344.
68. Jin, A.T.B.; Ling, D.N.C.; Goh, A. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognit.* **2004**, *37*, 2245–2255.

69. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **2001**, *40*, 614–634.
70. Jain, A.K.; Ross, A. Multibiometric systems. *Commun. ACM* **2004**, *47*, 34–40.
71. Schroff, F.; Kalenichenko, D.; Philbin, J. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the Conference on Computer Vision and Pattern Recognition, Boston, MA, USA, 7–12 June 2015; pp. 815–823.
72. Feng, T.; Liu, Z.; Kwon, K.A.; Shi, W.; Carbunar, B.; Jiang, Y.; Nguyen, N. Continuous mobile authentication using touchscreen gestures. In Proceedings of the Technologies for Homeland Security (HST) Conference, Waltham, MA, USA, 13–15 November 2012; pp. 451–456.
73. Ross, A.; Jain, A. Information fusion in biometrics. *Pattern Recognit. Lett.* **2003**, *24*, 2115–2125.
74. Kun, A.L.; Royer, T.; Leone, A. Using tap sequences to authenticate drivers. In Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, Eindhoven, The Netherlands, 28–30 October 2013; ACM: New York, NY, USA, 2013; pp. 228–231.
75. Hwang, M.S.; Li, L.H. A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2000**, *46*, 28–30.
76. Khan, S.H.; Akbar, M.A.; Shahzad, F.; Farooq, M.; Khan, Z. Secure biometric template generation for multi-factor authentication. *Pattern Recognit.* **2015**, *48*, 458–472.
77. Busold, C.; Taha, A.; Wachsmann, C.; Dmitrienko, A.; Seudié, H.; Sobhani, M.; Sadeghi, A.R. Smart keys for cyber-cars: Secure smartphone-based NFC-enabled car immobilizer. In Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 18–20 February 2013; ACM: New York, NY, USA, 2013; pp. 233–242.
78. Urien, P.; Piramuthu, S. Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks. *Decis. Support Syst.* **2014**, *59*, 28–36.
79. Fan, K.; Gong, Y.; Liang, C.; Li, H.; Yang, Y. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. *Secur. Commun. Netw.* **2016**, *9*, 3095–3104.
80. Acharya, S.; Polawar, A.; Pawar, P. Two factor authentication using smartphone generated one time password. *J. Comput. Eng. (IOSR-JCE)* **2013**, *11*, 85–90.
81. Lee, J.D.; Caven, B.; Haake, S.; Brown, T.L. Speech-based interaction with in-vehicle computers: The effect of speech-based e-mail on drivers' attention to the roadway. *Hum. Factors* **2001**, *43*, 631–640.
82. Thullier, F.; Bouchard, B.; Menelas, B.A.J. A Text-Independent Speaker Authentication System for Mobile Devices. *Cryptography* **2017**, *1*, 16.
83. Hautamäki, R.G.; Kinnunen, T.; Hautamäki, V.; Laukkanen, A.M. Automatic versus human speaker verification: The case of voice mimicry. *Speech Commun.* **2015**, *72*, 13–31.
84. Hautamäki, R.G.; Kinnunen, T.; Hautamäki, V.; Leino, T.; Laukkanen, A.M. I-vectors meet imitators: On vulnerability of speaker verification systems against voice mimicry. In Proceedings of the Interspeech, Lyon, France, 25–29 August 2013; pp. 930–934.
85. Ahonen, T.; Hadid, A.; Pietikainen, M. Face description with local binary patterns: Application to face recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* **2006**, *28*, 2037–2041.
86. Zhao, W.; Chellappa, R.; Phillips, P.J.; Rosenfeld, A. Face recognition: A literature survey. *ACM Comput. Surv. (CSUR)* **2003**, *35*, 399–458.
87. Smeets, D.; Claes, P.; Vandermeulen, D.; Clement, J.G. Objective 3D face recognition: Evolution, approaches and challenges. *Forensic Sci. Int.* **2010**, *201*, 125–132.
88. Kakadiaris, I.A.; Passalis, G.; Toderici, G.; Murtuza, M.N.; Lu, Y.; Karampatziakis, N.; Theoharis, T. Three-dimensional face recognition in the presence of facial expressions: An annotated deformable model approach. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 640–649.
89. Wójtowicz, W.; Ogiela, M.R. Biometric watermarks based on face recognition methods for authentication of digital images. *Secur. Commun. Netw.* **2015**, *8*, 1672–1687.
90. Wildes, R.P. Iris recognition: An emerging biometric technology. *Proc. IEEE* **1997**, *85*, 1348–1363.
91. Tan, T.; He, Z.; Sun, Z. Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition. *Image Vis. Comput.* **2010**, *28*, 223–230.
92. Bhattacharyya, D.; Ranjan, R.; Alisherov, F.; Choi, M. Biometric authentication: A review. *Int. J. u- e-Serv. Sci. Technol.* **2009**, *2*, 13–28.
93. Bowyer, K.W.; Burge, M.J. *Handbook of Iris Recognition*; Springer: Berlin, Germany, 2016.

94. Wong, A.L.; Shi, P. Peg-Free Hand Geometry Recognition Using Hierarchical Geometry and Shape Matching. In *MVA*; Citeseer: Hong Kong, China, 2002; pp. 281–284.
95. Zheng, G.; Wang, C.J.; Boult, T.E. Application of projective invariants in hand geometry biometrics. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 758–768.
96. Guo, J.M.; Liu, Y.F.; Chu, M.H.; Wu, C.C.; Le, T.N. Contact-free hand geometry identification system. In Proceedings of the 18th IEEE International Conference on Image Processing (ICIP), Brussels, Belgium, 11–14 September 2011; pp. 3185–3188.
97. Phan, D.; Siong, L.Y.; Pathirana, P.N.; Seneviratne, A. Smartwatch: Performance evaluation for long-term heart rate monitoring. In Proceedings of the International Symposium on Bioelectronics and Bioinformatics (ISBB), Beijing, China, 14–17 October 2015; pp. 144–147.
98. Zhang, Z. Photoplethysmography-based heart rate monitoring in physical activities via joint sparse spectrum reconstruction. *IEEE Trans. Biomed. Eng.* **2015**, *62*, 1902–1910.
99. Lu, S.; Zhao, H.; Ju, K.; Shin, K.; Lee, M.; Shelley, K.; Chon, K.H. Can photoplethysmography variability serve as an alternative approach to obtain heart rate variability information? *J. Clin. Monit. Comput.* **2008**, *22*, 23–29.
100. Kumar, A.; Hanmandlu, M.; Madasu, V.K.; Lovell, B.C. Biometric authentication based on infrared thermal hand vein patterns. In Proceedings of the Digital Image Computing: Techniques and Applications (DICTA'09), Melbourne, Australia, 1–3 December 2009; pp. 331–338.
101. Kang, W.; Wu, Q. Contactless palm vein recognition using a mutual foreground-based local binary pattern. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1974–1985.
102. Piekarczyk, M.; Ogiela, M.R. Touch-Less Personal Verification Using Palm and Fingers Movements Tracking. In *New Trends in Analysis and Interdisciplinary Applications*; Springer: Berlin, Germany, 2017; pp. 603–609.
103. Tome, P.; Vanoni, M.; Marcel, S. On the vulnerability of finger vein recognition to spoofing. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10–12 September 2014; pp. 1–10.
104. Tome, P.; Marcel, S. On the vulnerability of palm vein recognition to spoofing attacks. In Proceedings of the International Conference on Biometrics (ICB), Phuket, Thailand, 9–22 May 2015; pp. 319–325.
105. Titcomb, J. Why Your Smartphone's Fingerprint Scanner Isn't as Secure as You Might Think. 2017. Available online: http://www.telegraph.co.uk/technology/2017/04/11/smartphone-fingerprint-scanners-could-easily-fooled-fake-prints/ (accessed on 4 January 2018).
106. Jain, A.; Bolle, R.; Pankanti, S. *Biometrics: Personal Identification in Networked Society*; Springer: Berlin, Germany, 2006; Volume 479.
107. Maltoni, D.; Maio, D.; Jain, A.; Prabhakar, S. *Handbook of Fingerprint Recognition*; Springer: Berlin, Germany, 2009.
108. De Luca, A.; Lindqvist, J. Is secure and usable smartphone authentication asking too much? *Computer* **2015**, *48*, 64–68.
109. Kong, S.G.; Heo, J.; Boughorbel, F.; Zheng, Y.; Abidi, B.R.; Koschan, A.; Yi, M.; Abidi, M.A. Multiscale fusion of visible and thermal IR images for illumination-invariant face recognition. *Int. J. Comput. Vis.* **2007**, *71*, 215–233.
110. Guzman, A.M.; Goryawala, M.; Wang, J.; Barreto, A.; Andrian, J.; Rishe, N.; Adjouadi, M. Thermal imaging as a biometrics approach to facial signature authentication. *IEEE J. Biomed. Health Inform.* **2013**, *17*, 214–222.
111. Hu, S.; Choi, J.; Chan, A.L.; Schwartz, W.R. Thermal-to-visible face recognition using partial least squares. *JOSA A* **2015**, *32*, 431–442.
112. Denning, D.E.; MacDoran, P.F. Location-based authentication: Grounding cyberspace for better security. *Comput. Fraud Secur.* **1996**, *1996*, 12–16.
113. Fridman, L.; Weber, S.; Greenstadt, R.; Kam, M. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Syst. J.* **2017**, *11*, 513–521.
114. Hammad, A.; Faith, P. Location Based Authentication. U.S. Patent 9,721,250, 1 August 2017.
115. Vacca, J.R. *Biometric Technologies and Verification Systems*; Butterworth-Heinemann: Oxford, UK, 2007.
116. Banerjee, S.P.; Woodard, D.L. Biometric authentication and identification using keystroke dynamics: A survey. *J. Pattern Recognit. Res.* **2012**, *7*, 116–139.

117. Shrestha, B.; Mohamed, M.; Tamrakar, S.; Saxena, N. Theft-resilient mobile wallets: Transparently authenticating NFC users with tapping gesture biometrics. In Proceedings of the 32nd Annual Conference on Computer Security Applications, Los Angeles, CA, USA, 5–9 December 2016; ACM: New York, NY, USA, 2016; pp. 265–276.
118. Gascon, H.; Uellenbeck, S.; Wolf, C.; Rieck, K. Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior. In Proceedings of the Conference "Sicherheit", Sicherheit, Schutz und Verlässlichkeit, 19–21 March 2014; pp. 1–12.
119. Buschek, D.; De Luca, A.; Alt, F. Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; ACM: New York, NY, USA, 2015; pp. 1393–1402.
120. Meng, W.; Wong, D.S.; Furnell, S.; Zhou, J. Surveying the development of biometric user authentication on mobile phones. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1268–1293.
121. Buriro, A.; Crispo, B.; Del Frari, F.; Wrona, K. Touchstroke: Smartphone user authentication based on touch-typing biometrics. In Proceedings of the International Conference on Image Analysis and Processing, Niagara Falls, ON, Canada, 22–24 July 2015; Springer: Berlin, Germany, 2015; pp. 27–34.
122. Sae-Bae, N.; Ahmed, K.; Isbister, K.; Memon, N. Biometric-rich gestures: A novel approach to authentication on multi-touch devices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 22–27 April 2006; ACM: New York, NY, USA, 2012; pp. 977–986.
123. Lee, W.H.; Lee, R.B. Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning. In Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, 26–29 June 2017; pp. 297–308.
124. Burgbacher, U.; Hinrichs, K. An implicit author verification system for text messages based on gesture typing biometrics. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, oronto, ON, Canada, 26 April 26–1 May 2014; ACM: New York, NY, USA, 2014; pp. 2951–2954.
125. Hachaj, T.T.; Ogiela, M.R.; Baraniewicz, D. Evaluation of Gesture Description Language in the role of touchless interface for virtual reality environment. *Prz. Elektrotech.* **2017**, *93*, 57–66.
126. Van Goethem, T.; Scheepers, W.; Preuveneers, D.; Joosen, W. Accelerometer-based device fingerprinting for multi-factor mobile authentication. In Proceedings of the International Symposium on Engineering Secure Software and Systems, London, UK, 6–8 April 2016; Springer: Berlin, Germany, 2016; pp. 106–121.
127. Figueira, C.; Matias, R.; Gamboa, H. Body Location Independent Activity Monitoring. In Proceedings of the International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSIGNALS), Rome, Italy, 21–23 February 2016; pp. 190–197.
128. Grankin, M.; Khavkina, E.; Ometov, A. Research of MEMS accelerometers features in mobile phone. In Proceedings of the 12th Conference of Open Innovations Association FRUCT, Oulu, Finland, 5–9 November 2012; pp. 31–36.
129. Wang, W.; Xi, J.; Chen, H. Modeling and recognizing driver behavior based on driving data: A survey. *Math. Prob. Eng.* **2014**, *2014*.
130. Igarashi, K.; Miyajima, C.; Itou, K.; Takeda, K.; Itakura, F.; Abut, H. Biometric identification using driving behavioral signals. In Proceedings of the International Conference on Multimedia and Expo, Taipei, Taiwan, 27–30 June 2004; Volume 1, pp. 65–68.
131. McCall, J.C.; Trivedi, M.M. Driver behavior and situation aware brake assistance for intelligent vehicles. *Proc. IEEE* **2007**, *95*, 374–387.
132. Oliver, N.; Pentland, A.P. Driver behavior recognition and prediction in a SmartCar. In Proceedings of the International Society for Optics and Photonics Meeting, Orlando, FL, USA, 24–28 April 2000; Volume 4023, pp. 280–290.
133. Shi, E.; Niu, Y.; Jakobsson, M.; Chow, R. Implicit Authentication through Learning User Behavior. In Proceedings of the 13th International Conference, ISC 2010, Boca Raton, FL, USA, 25–28 October 2010; Springer: Berlin, Germany, 2010; Volume 6531, pp. 99–113.
134. Nothacker, K.H.; Basaran, P.A.; Rettus, S.I.; Strasser, M.J.; Aziz, I.; Walton, J.P.; Saul, Z.M.; Faykus, C.T. Method and System for Monitoring Intoxication. U.S. Patent 9,192,334, 24 November 2015.
135. He, D.; Zeadally, S. An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography. *IEEE Internet Things J.* **2015**, *2*, 72–83.

136. Xiao, L.; Chen, T.; Han, G.; Zhuang, W.; Sun, L. Channel-Based Authentication Game in MIMO Systems. In Proceedings of the Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 Decembe 2016; pp. 1–6.
137. Zhao, N.; Zhang, Z.; Rehman, M.U.; Ren, A.; Yang, X.; Zhao, J.; Zhao, W.; Dong, B. Authentication in Millimeter-Wave Body-Centric Networks through Wireless Channel Characterization. *IEEE Trans. Antennas Propag.* **2017**, *65*, 6616–6623.
138. Gapeyenko, M.; Samuylov, A.; Gerasimenko, M.; Moltchanov, D.; Singh, S.; Aryafar, E.; Yeh, S.P.; Himayat, N.; Andreev, S.; Koucheryavy, Y. Analysis of human-body blockage in urban millimeter-wave cellular communications. In Proceedings of the International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–7.
139. Mercedes-Benz SUV Operation Manual. Occupant Classification System (OCS). 2017. Available online: http://www.mersuv.com/mbread-149.html (accessed on 4 January 2018).
140. Farmer, M.E.; Jain, A.K. Occupant classification system for automotive airbag suppression. In Proceedings of the Computer Society Conference on Computer Vision and Pattern Recognition, Madison, WI, USA, 18–20 June 2003; Volume 1.
141. Mehney, M.A.; McCarthy, M.C.; Fullerton, M.G.; Malecke, F.J. Vehicle Occupant Weight Sensor Apparatus. U.S. Patent 6,039,344, 6 July 2000.
142. Ferro, M.; Pioggia, G.; Tognetti, A.; Carbonaro, N.; De Rossi, D. A sensing seat for human authentication. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 451–459.
143. Silva, H.; Lourenço, A.; Fred, A. In-vehicle driver recognition based on hand ECG signals. In Proceedings of the International conference on Intelligent User Interfaces, Lisbon, Portugal, 14–17 February 2012; ACM: New York, NY, USA, 2012; pp. 25–28.
144. Pham, T.; Ma, W.; Tran, D.; Nguyen, P.; Phung, D. Multi-factor EEG-based user authentication. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Beijing, China, 6–11 July 2014; pp. 4029–4034.
145. Paranjape, R.; Mahovsky, J.; Benedicenti, L.; Koles, Z. The electroencephalogram as a biometric. In Proceedings of the Canadian Conference on Electrical and Computer Engineering, Toronto, ON, Canada, 13–16 May 2001; Volume 2, pp. 1363–1366.
146. Chuang, J.; Nguyen, H.; Wang, C.; Johnson, B. I think, therefore I am: Usability and security of authentication using brainwaves. In Proceedings of the International Conference on Financial Cryptography and Data Security, Okinawa, Japan, 1 April 2013; Springer: Berlin, Germany, 2013; pp. 1–16.
147. Mohanchandra, K.; Lingaraju, G.; Kambli, P.; Krishnamurthy, V. Using brain waves as new biometric feature for authenticating a computer user in real-time. *Int. J. Biom. Bioinform. (IJBB)* **2013**, *7*, 49.
148. Siswoyo, A.; Arief, Z.; Sulistijono, I.A. Application of Artificial Neural Networks in Modeling Direction Wheelchairs Using Neurosky Mindset Mobile (EEG) Device. *EMITTER Int. J. Eng. Technol.* **2017**, *5*, 170–191.
149. Reid, Y.; Storts, D.; Riss, T.; Minor, L. Authentication of Human Cell Lines by STR DNA Profiling Analysis. Eli Lilly & Company and the National Center for Advancing Translational Sciences, 2013. Available online: https://www.ncbi.nlm.nih.gov/books/NBK144066/ (accessed on 4 January 2018).
150. Yun, Y.W. The '123' of biometric technology. *Synth. J.* **2002**, *3*, 83–96.
151. Kraus, L.; Antons, J.N.; Kaiser, F.; Möller, S. User experience in authentication research: A Survey. In Proceedings of the PQS 2016, Berlin, Germany, 29–31 August 2016; pp. 54–58.
152. Katsini, C.; Belk, M.; Fidas, C.; Avouris, N.; Samaras, G. Security and Usability in Knowledge-based User Authentication: A Review. In Proceedings of the 20th Pan-Hellenic Conference on Informatics, Patras, Greece, 10–12 November 2016; ACM: New York, NY, USA, 2016; p. 63.
153. Nicholson, J.; Coventry, L.; Briggs, P. Age-related performance issues for PIN and face-based authentication systems. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris, France, 27 April–2 May 2013; ACM: New York, NY, USA, 2013; pp. 323–332.
154. Harby, F.; Qahwaji, R.; Kamala, M. End-Users' Acceptance of Biometrics Authentication to Secure E-Commerce within the Context of Saudi Culture: Applying the UTAUT Model. In *Globalization, Technology Diffusion and Gender Disparity: Social Impacts of ICTs*; Information Science Reference: Hershey, PA, USA, 2012; pp. 225–246.

155. Ogiela, M.R.; Ogiela, L. Behavioral Keys in Cryptography and Security Systems. In Proceedings of the International Conference on Intelligent Networking and Collaborative Systems, Toronto, ON, Canada, 24–26 August 2017; Springer: Berlin, Germany, 2017; pp. 296–300.
156. Al-Ameen, M.N.; Wright, M.; Scielzo, S. Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; ACM: New York, NY, USA, 2015; pp. 2315–2324.
157. Belk, M.; Fidas, C.; Germanakos, P.; Samaras, G. The interplay between humans, technology and user authentication: A cognitive processing perspective. *Comput. Hum. Behav.* **2017**, *76*, 184–200.
158. Ma, Y.; Feng, J.; Kumin, L.; Lazar, J. Investigating user behavior for authentication methods: A comparison between individuals with down syndrome and neurotypical users. *ACM Trans. Access. Comput. (TACCESS)* **2013**, *4*, 15.
159. Melicher, W.; Kurilova, D.; Segreti, S.M.; Kalvani, P.; Shay, R.; Ur, B.; Bauer, L.; Christin, N.; Cranor, L.F.; Mazurek, M.L. Usability and security of text passwords on mobile devices. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016; ACM: New York, NY, USA, 2016; pp. 527–539.
160. Von Zezschwitz, E.; De Luca, A.; Hussmann, H. Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. In Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, Helsinki, Finland, 26–30 October 2014; ACM: New York, NY, USA, 2014; pp. 461–470.
161. Fathi, R.; Salehi, M.A.; Leiss, E.L. User-friendly and secure architecture (UFSA) for authentication of cloud services. In Proceedings of the 8th International Conference on Cloud Computing (CLOUD), New York, NY, USA, 27 June–2 July 2015; pp. 516–523.
162. Aumi, M.T.I.; Kratz, S. AirAuth: Evaluating in-air hand gestures for authentication. In Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services, Toronto, ON, Canada, 23–26 September 2014; ACM: New York, NY, USA, 2014; pp. 309–318.
163. Da Silva, H.P.; Fred, A.; Lourenço, A.; Jain, A.K. Finger ECG signal for user authentication: Usability and performance. In Proceedings of the 6th International Conference on Biometrics: Theory, Applications and Systems, Arlington, VA, USA, 29 September–2 October 2013; pp. 1–8.
164. Michelin, R.A.; Zorzo, A.F.; Campos, M.B.; Neu, C.V.; Orozco, A.M. Smartphone as a biometric service for web authentication. In Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016; pp. 405–408.
165. Conti, V.; Collotta, M.; Pau, G.; Vitabile, S. Usability Analysis of a Novel Biometric Authentication Approach for Android-Based Mobile Devices. *J. Telecommun. Inf. Technol.* **2014**, *4*, 34–43.
166. Maple, C.; Norrington, P. The usability and practicality of biometric authentication in the workplace. In Proceedings of the First International Conference on Availability, Reliability and Security, Vienna, Austria, 20–22 April 2006; pp. 1–7.
167. Matyáš, V.; Říha, Z. Biometric authentication–security and usability. In *Advanced Communications and Multimedia Security*; Springer: Berlin, Germany, 2002; pp. 227–239.
168. NetworkWorld. Solving the Challenge of Multi-Factor Authentication Adoption. 2017. Available online: https://www.networkworld.com/article/3197096/lan-wan/solving-the-challenge-of-multi-factor-authentication-adoption.html (accessed on 4 January 2018).
169. TechTarget. Logical, Physical Security Integration Challenges. 2017. Available online: http://searchsecurity.techtarget.com/magazineContent/Logical-physical-security-integration-challenges (accessed on 4 January 2018).
170. Tolosana, R.; Vera-Rodriguez, R.; Ortega-Garcia, J.; Fierrez, J. Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification. *IEEE Access* **2015**, *3*, 478–489.
171. Galbally, J.; Satta, R. Biometric Sensor Interoperability: A Case Study in 3D Face Recognition. In Proceedings of the ICPRAM, Rome, Italy, 24–26 February 2016; pp. 199–204.
172. Alonso-Fernandez, F.; Fierrez, J.; Ramos, D.; Gonzalez-Rodriguez, J. Quality-based conditional processing in multi-biometrics: application to sensor interoperability. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2010**, *40*, 1168–1179.

173. Bandara, H.; De Silva, S.R.P.; Weerasinghe, P.D. The universal biometric system. In Proceedings of the International Conference on Advances in ICT for Emerging Regions, Colombo, Sri Lanka, 24–26 August 2015; pp. 1–6.
174. Jain, A.K.; Nandakumar, K. Biometric Authentication: System Security and User Privacy. *IEEE Comput.* **2012**, *45*, 87–92.
175. Biggio, B.; Akhtar, Z.; Fumera, G.; Marcialis, G.L.; Roli, F. Security evaluation of biometric authentication systems under real spoofing attacks. *IET Biom.* **2012**, *1*, 11–24.
176. Marcel, S.; Nixon, M.S.; Li, S.Z. *Handbook of Biometric Anti-Spoofing*; Springer: Berlin, Germany, 2014; Volume 1.
177. Uludag, U.; Jain, A.K. Attacks on biometric systems: A case study in fingerprints. In Proceedings of the SPIE, San Jose, CA, USA, 19–22 January 2004; Volume 5306, pp. 622–633.
178. He, D.; Zeadally, S. Authentication protocol for an ambient assisted living system. *IEEE Commun. Mag.* **2015**, *53*, 71–77.
179. Rodrigues, R.N.; Kamat, N.; Govindaraju, V. Evaluation of biometric spoofing in a multimodal system. In Proceedings of the 4th IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), Washington, DC, USA, 27–29 September 2010; pp. 1–5.
180. Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric template security. *EURASIP J. Adv. Signal Process.* **2008**, *2008*, 113.
181. Andreev, S.; Hosek, J.; Olsson, T.; Johnsson, K.; Pyattaev, A.; Ometov, A.; Olshannikova, E.; Gerasimenko, M.; Masek, P.; Koucheryavy, Y.; et al. A unifying perspective on proximity-based cellular-assisted mobile social networking. *IEEE Commun. Mag.* **2016**, *54*, 108–116.
182. Ometov, A.; Zhidanov, K.; Bezzateev, S.; Florea, R.; Andreev, S.; Koucheryavy, Y. Securing network-assisted direct communication: The case of unreliable cellular connectivity. In Proceedings of the Trustcom/ BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; Volume 1, pp. 826–833.
183. Chingovska, I.; Anjos, A.; Marcel, S. On the effectiveness of local binary patterns in face anti-spoofing. In Proceedings of the International Conference of theBiometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6–7 September 2012; pp. 1–7.
184. Vaidya, B.; Makrakis, D.; Mouftah, H.T. Improved two-factor user authentication in wireless sensor networks. In Proceedings of the 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Niagara Falls, NU, Canada, 11–13 October 2010; pp. 600–606.
185. Rathgeb, C.; Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. *J. Inf. Secur. (EURASIP)* **2011**, doi:10.1186/1687-417X-2011-3.
186. Chen, B.; Chandran, V. Biometric template security using higher order spectra. In Proceedings of the International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, USA, 14–19 March 2010; pp. 1730–1733.
187. Fierrez, J.; Ortega-Garcia, J.; Toledano, D.T.; Gonzalez-Rodriguez, J. BioSec baseline corpus: A multimodal biometric database. *Pattern Recognit.* **2007**, *40*, 1389–1392.
188. Fierrez, J.; Galbally, J.; Ortega-Garcia, J.; Freire, M.R.; Alonso-Fernandez, F.; Ramos, D.; Toledano, D.T.; Gonzalez-Rodriguez, J.; Siguenza, J.A.; Garrido-Salas, J.; et al. BiosecurID: A multimodal biometric database. *Pattern Anal. Appl.* **2010**, *13*, 235–246.
189. Gomez-Barrero, M.; Rathgeb, C.; Galbally, J.; Busch, C.; Fierrez, J. Unlinkable and irreversible biometric template protection based on bloom filters. *Inf. Sci.* **2016**, *370*, 18–32.
190. Fan, Y.; Zhang, Z.; Trinkle, M.; Dimitrovski, A.D.; Song, J.B.; Li, H. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids. *IEEE Trans. Smart Grid* **2015**, *6*, 2659–2668.
191. Heng, L.; Work, D.B.; Gao, G.X. GPS signal authentication from cooperative peers. *IEEE Trans. Intell. Trans. Syst.* **2015**, *16*, 1794–1805.
192. Lichtman, M.; Jover, R.P.; Labib, M.; Rao, R.; Marojevic, V.; Reed, J.H. LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation. *IEEE Commun. Mag.* **2016**, *54*, 54–61.
193. Sheng, Y.; Tan, K.; Chen, G.; Kotz, D.; Campbell, A. Detecting 802.11 MAC layer spoofing using received signal strength. In Proceedings of the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1768–1776.

194. Wayman, J.; Jain, A.; Maltoni, D.; Maio, D. An introduction to biometric authentication systems. *Biom. Syst.* **2005**, 1–20, doi:10.1007/1-84628-064-8_1.
195. Benchmark. Deploying Fingerprint Biometrics. 2017. Available online: http://benchmarkmagazine.com/deploying-fingerprint-biometrics/ (accessed on 1 January 2017).
196. Ratha, N.; Bolle, R. *Automatic Fingerprint Recognition Systems*; Springer: Berlin, Germany, 2007.
197. Sariyanidi, E.; Gunes, H.; Cavallaro, A. Automatic analysis of facial affect: A survey of registration, representation, and recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* **2015**, *37*, 1113–1133.
198. Raja, K.B.; Raghavendra, R.; Stokkenes, M.; Busch, C. Multi-modal authentication system for smartphones using face, iris and periocular. In Proceedings of the International Conference on Biometrics (ICB), Phuket, Thailand, 19–22 May 2015; pp. 143–150.
199. Golfarelli, M.; Maio, D.; Malton, D. On the error-reject trade-off in biometric verification systems. *IEEE Trans. Pattern Anal. Mach. Intell.* **1997**, *19*, 786–796.
200. Sanmorino, A.; Yazid, S. A survey for handwritten signature verification. In Proceedings of the 2nd International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE), Jalarta, Indonesia, 14–15 August 2012; pp. 54–57.
201. Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 4–20.
202. Kholmatov, A.; Yanikoglu, B. Identity authentication using improved online signature verification method. *Pattern Recognit. Lett.* **2005**, *26*, 2400–2408.
203. Utter, T.; Proefke, D.; Baillargeon, R. Multiple Vehicle Authentication for Entry and Starting Systems. U.S. Patent 20070001805, 4 January 2007.
204. Cranor, L.F.; Garfinkel, S. *Security and Usability: Designing Secure Systems that People Can Use*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2005.
205. Ometov, A.; Masek, P.; Malina, L.; Florea, R.; Hosek, J.; Andreev, S.; Hajny, J.; Niutanen, J.; Koucheryavy, Y. Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices. In Proceedings of the International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, Australia, 14–18 March 2016; pp. 1–6.
206. SC Media UK. Making the Case for the Use of Biometrics in Multi-Factor Authentication. 2016. Available online: https://www.scmagazineuk.com/making-the-case-for-the-use-of-biometrics-in-multi-factor-authentication/article/545395/ (accessed on 1 January 2018).
207. Lai, C.P.; Ding, C. Several generalizations of Shamir's secret sharing scheme. *Int. J. Found. Comput. Sci.* **2004**, *15*, 445–458.
208. Ometov, A.; Orsino, A.; Militano, L.; Araniti, G.; Moltchanov, D.; Andreev, S. A novel security-centric framework for D2D connectivity based on spatial and social proximity. *Comput. Netw.* **2016**, *107*, 327–338.
209. Yang, C.C.; Chang, T.Y.; Hwang, M.S. A(t,n) multi-secret sharing scheme. *Appl. Math. Comput.* **2004**, *151*, 483–490.
210. Dehkordi, M.H.; Mashhadi, S. An efficient threshold verifiable multi-secret sharing. *Comput. Stand. Interfaces* **2008**, *30*, 187–190.
211. Smart, N.P. Secret Sharing Schemes. In *Cryptography Made Simple*; Springer: Berlin, Germany, 2016; pp. 403–416.
212. Harn, L.; Lin, C. Strong (n, t, n) verifiable secret sharing scheme. *Inf. Sci.* **2010**, *180*, 3059–3064.
213. Ogiela, L.; Ogiela, M.R.; Takizawa, M. Safety and Standardization of Data Sharing Techniques and Protocols for Management of Strategic Data. In Proceedings of the 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 1076–1081.
214. Kaya, K.; Selçuk, A.A. Threshold cryptography based on Asmuth–Bloom secret sharing. *Inf. Sci.* **2007**, *177*, 4148–4160.
215. Niinuma, K. Biometric Authentication Device, Biometric Authentication Method and Computer Readable, Non-Transitory Medium. U.S. Patent 9,542,543, 10 January 2017.
216. Koved, L. *Usable Multi-Factor Authentication and Risk-Based Authorization*; Technical Report; International Business Machines Corp: Yorktown Heights, NY, USA, 2015.
217. Thakkar, D. False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics. 2017. Available online: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/ (accessed on 4 January 2018).

218. Castanedo, F. A review of data fusion techniques. *Sci. World J.* **2013**, *2013*, 704504.
219. Biometric Signature ID. Biometric signature ID Scores an Outstanding 99.97% Accuracy against Identity Fraud from Tolly Group. 2017. Available online: https://www.biosig-id.com/news-and-events/press-releases/193-biometric-signature-id-scores-an-outstanding-99-97-accuracy-against-identity-fraud-from-tolly-group (accessed on 4 January 2018).
220. Weiner, S. The Future of Biometrics Could Be Your Heart. 2017. Available online: http://www.popularmechanics.com/technology/security/a28443/biometric-heart-scanner/ (accessed on 4 January 2018).
221. O'Neal, M.; Balagani, K.; Phoha, V.; Rosenberg, A.; Serwadda, A.; Karim, M.E. *Context-Aware Active Authentication using Touch Gestures, Typing Patterns and Body Movement*; Technical Report; Louisiana Technical University: Ruston, LA, USA, 2016.
222. NSTC Subcommittee on Biometrics & Identity Management. *Biometrics Metrics Report v0.3*; Technical Report; U.S. Military Academy: New York, NY, USA, 2012.
223. Townsend, K. Passive Authentication May Be the Future for User Authentication, and It's Just Beginning to Appear. 2016. Available online: http://www.securityweek.com/passive-authentication-future-user-authentication (accessed on 4 January 2018).
224. Walters, R. Continuous Authentication: The Future of Identity and Access Management (IAM). 2016. Available online: https://www.networkworld.com/article/3121240/security/continuous-authentication-the-future-of-identity-and-access-management-iam.html (accessed on 4 January 2018).
225. Bartlett, M.S.; Movellan, J.R.; Sejnowski, T.J. Face recognition by independent component analysis. *IEEE Trans. Neural Netw.* **2002**, *13*, 1450–1464.
226. Wright, J.; Yang, A.Y.; Ganesh, A.; Sastry, S.S.; Ma, Y. Robust face recognition via sparse representation. *IEEE Trans. Pattern Anal. Mach. Intell.* **2009**, *31*, 210–227.
227. Berry, P. Biometrics and Artificial Neural Networks: How Big Data Collection Works in Your Favor. 2014. Available online: http://chicagopolicyreview.org/2014/03/04/biometrics-and-artificial-neural-networks-how-big-data-collection-works-in-your-favor/ (accessed on 4 January 2018)
228. Sadikoglu, F.; Uzelaltinbulat, S. Biometric Retina Identification Based on Neural Network. *Procedia Comput. Sci.* **2016**, *102*, 26–33.
229. Yao, Y.; Marcialis, G.L.; Pontil, M.; Frasconi, P.; Roli, F. Combining flat and structured representations for fingerprint classification with recursive neural networks and support vector machines. *Pattern Recognit.* **2003**, *36*, 397–406.
230. Derakhshani, R.; Ross, A. A texture-based neural network classifier for biometric identification using ocular surface vasculature. In Proceedings of the International Joint Conference on Neural Networks, Orlando, FL, USA, 12–17 August 2007; pp. 2982–2987.
231. Zhang, X.; Yao, L.; Kanhere, S.S.; Liu, Y.; Gu, T.; Chen, K. MindID: Person Identification from Brain Waves through Attention-based Recurrent Neural Network. *arXiv* **2017**, arXiv:1711.06149.
232. Salloum, R.; Kuo, C.C.J. ECG-based biometrics using recurrent neural networks. In Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017; pp. 2062–2066.
233. Biometrics Research Group, Inc. Mobile Biometric Applications. 2017. Available online: http://chicagopolicyreview.org/2014/03/04/biometrics-and-artificial-neural-networks-how-big-data-collection-works-in-your-favor/ (accessed on 4 January 2018).
234. Acuity Market Intelligence. The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy. 2016. Available online: http://www.acuity-mi.com/GBMR_Report.php (accessed on 4 January 2018).