

# A Matrix for Systematic Selection of Authentication Mechanisms in Challenging Healthcare related Environments

Michael Grabatin

Michael Steinke

Daniela Pöhn

Wolfgang Hommel

michael.grabatin@unibw.de

michael.steinke@unibw.de

daniela.poehn@unibw.de

wolfgang.hommel@unibw.de

Universität der Bundeswehr München, Research Institute CODE  
Munich, Germany

## ABSTRACT

Passwords continue to dominate the authentication landscape, while One Time Passwords (OTPs) provided by apps are increasingly used as second factor. Even though several alternatives are developed, very few regard usability. Even fewer alternatives consider special conditions of authentication, like disabilities and other input restrictions, typical for healthcare workers. In this paper, we show shortcomings by the example of different stages within the care cycle. Generalized requirements are used to evaluate existing authentication mechanisms. These findings result in the design of a matrix showing different authentication methods and requirements. The matrix can be used to identify the best fitting authentication mechanisms based on the needs of the scenario. Not only the first factor can be identified, but the matrix also helps to select additional well-fitting authentication mechanism for a specific scenario. The designed matrix is practically underlined by applying it to the care cycle with different cyber-physical systems (CPS).

## CCS CONCEPTS

• **Security and privacy** → **Authentication**; *Biometrics*; *Graphical / visual passwords*; *Multi-factor authentication*.

## KEYWORDS

Authentication; Identity Management; Access Management; Systems Security

## ACM Reference Format:

Michael Grabatin, Michael Steinke, Daniela Pöhn, and Wolfgang Hommel. 2021. A Matrix for Systematic Selection of Authentication Mechanisms in Challenging Healthcare related Environments. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-physical Systems*

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

SAT-CPS'21, April 28, 2021, Virtual Event, USA

© 2021 Association for Computing Machinery.

ACM ISBN 978-1-4503-8319-6/21/04...\$15.00

<https://doi.org/10.1145/3445969.3450424>

(SAT-CPS'21), April 28, 2021, Virtual Event, USA. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3445969.3450424>

## 1 INTRODUCTION

Digital technology is an opportunity to be part of today's society in the daily life. People look for a home or a new job online. Healthcare and administrative procedures are accessible online in many countries as well as appointments at doctors can be made. Therefore, digital identities, such as eIDs, are required for digitalization. The management of digital identities, including details of user information, referred to as attributes, is called identity management. Different home organizations, like companies, universities or online networks provide identity management for their users. Besides management of the identities themselves, they provide means for authentication. Authentication is the act of proving an identity via different mechanisms. Identity management can and should be a mean for inclusion. At the same time access is also one key success factor for digital inclusion. This means connectivity, affordability, and accessibility are key success factors for digital identities and, consequently, authentication. Authentication should be usable for different persons in different, sometimes challenging situations. But is this the case?

We especially focus on multiple interrelated situations in the healthcare cycle with special conditions for authentication and their requirements, due to a necessary trade-off of usability and security for these complex systems. By addressing gathered challenges, we receive a better overview. The aim of this work is to provide a matrix serving as a tool for decision-making for suitable authentication mechanisms. We explicitly focus on covering aspects arising from special and challenging conditions. The proposed matrix allows to systematically select authentication mechanisms, combinations, and fallbacks. By providing suitable authentication methods, the acceptance rate of the users can be increased.

Our main contribution is decision matrix itself as well as its systematic derivation, which may help persons in charge, e.g., in hospitals, with identifying adequate authentication mechanisms. To our knowledge no such decision matrix is currently available.

The rest of the paper is organized as follows: Section 2 highlights authentication challenges in four associated situations in

the context of a scenario in the healthcare cycle. Based on the scenario, requirements are gathered, which are generalized in Section 3. These generalized requirements are contrasted in the following Section 4 with related approaches. The findings lead to the conception of the matrix for authentication in Section 5. Section 6 discusses the concept and applies it to the four real-world scenarios. Section 7 concludes the paper and gives future directions.

## 2 SCENARIO: AUTHENTICATION CHALLENGES IN THE CARE CYCLE

According to Verbeek and Lord [40], the care cycle includes the activities of promotion & prevention, diagnosis, treatment, management and rehabilitation. Within these activities, we identified four heavily IT-supported situations with each having its own IT-environment (especially different highly specialized CPS – e. g. for patient monitoring) and fit authentication mechanisms:

- (1) Emergency care and vehicle services (*management*).
- (2) Medical care in hospitals (*diagnosis and treatment*).
- (3) (Mass) Testing and Contact (*prevention and diagnosis*).
- (4) Patients' physical and mental handicaps (*rehabilitation*).

For these situations, we highlight authentication challenges and make assumptions about how authentication is done. Especially with regard to MFA, authentication methods are usually grouped in four categories [2]:

- **Something you know:** Knowledge.
- **Something you have:** Possession.
- **Something you are:** Inherent or biometric characteristics.
- **Something you do or how you do something:** Actions.

While each authentication method has its own unique difficulties, it is generally assumed that authentication methods work equally well for everybody with the exception for certain disabilities. Yet, environments that restrict the usefulness of some authentication methods are plentiful. The following sections describe a selection of those *a)* from the perspective of emergency services, *b)* at the hospital, *c)* during testing for prevention or diagnosis, and *d)* persons affected by disabilities. All four scenarios are related to healthcare, but have a different angle. They are derived from our insides gained from projects and private engagements. Based on these different scenarios, the most urgent requirements are gathered.

### 2.1 Emergency Care and Vehicle Services

Blue light organizations in Germany often have tablets and other devices in their vehicles. As information has to be available immediately, even with changing persons, either no authentication or a simple code is used. Voluntary fire brigades in Munich and other cities have tablets with detailed information about the place of action from the control room, calculating the route to an emergency location. Especially in voluntary fire brigades, the groups are mixed at each alarm and even guests from other brigades can participate under conditions. The devices are placed in the front row, therefore, only the driver or the group leader can interact. These persons are typically higher up in the hierarchy and have no or only fewer disabilities. Everyone is alerted and things have to go quickly. The group leader still has to mentally prepare for the operation and

give instructions to the team. Therefore, the authentication is either simple, using trivial passwords like “1234”, or none at all. The NIDApad, an emergency information and documentation assistant for ambulances even goes one step beyond. The tablet is used for documentation and pre-informing hospitals. Personal sensitive information is handled, requiring the use of secure authentication. As the crew is changing, they use one four number digit code in Bavaria. Additionally, the NIDApad has a touchpad, though the professionals from the rescue service wear disposable gloves. Based on this scenario, the following requirements can be gathered:

- **REQ1:** Time-saving, reliable methods.
- **REQ2:** Easy to handle when under pressure.
- **REQ3:** Multi-user-devices.
- **REQ4:** Protection of sensitive information.
- **REQ5:** Usable with disposable gloves.
- **REQ6:** Suitable for mobile devices.
- **REQ7:** Consideration of advanced hygiene aspects.

### 2.2 Hospitalization and Care

Further challenges appear at the subsequent situation: the hospitalization and care. In fact, every medical process is nowadays augmented by and dependent on a sophisticated IT-infrastructure and services like a hospital information system (HIS), which organizes the treatments of all patients. Physicians record patients' health conditions or medical treatments from common stationary client PCs or even mobile devices. These devices are often shared between multiple individuals – for instance, consider doctors' visit in different hospital wards or treatment rooms where multiple physicians as well as nurses work with the same systems. As a result of hospitals and healthcare institutions being very popular targets for data theft and malware infects, typical deficiencies like collective user accounts must be avoided and medical staff must lock client sessions as soon as they leave a client system unattended. Password authentication is by far prevalent in common hospital environments, yet – especially using strong password phrases – it is time-consuming and consequently impedes medical operations as well as frustrates users that consequently bypass lock-screen policies. Just like in emergency vehicles, personnel often wears disposable gloves, work in hectic surroundings and must comply with very strict hygiene regulations. Additionally, users can have restrictions as described in the following scenario. Requirements for authentication methods in this scenario encompass the following:

- **REQ1:** Time-saving, reliable methods, cf. Scenario (S) 1.
- **REQ5:** Usable with disposable gloves, cf. S 1.
- **REQ6:** Suitable for mobile devices, cf. S 1.
- **REQ7:** Consideration of advanced hygiene aspects, cf. S 1.
- **REQ8:** Usability.

### 2.3 (Mass) Testing and Communication

With the recent COVID-19 crisis the need to be able to test many people in short time frames has been highlighted. The problems associated with this range from organizing the testing itself, e. g., scheduling who will be tested where and when, to notifying the tested persons about their result in a timely manner. All while protecting the patients' private information and ensuring that results are not accidentally associated with the wrong person. In theory,

approaches like electronic health records and government issued eID could be suitable to provide the necessary infrastructure. Both systems are, however, at the moment not fully in place in Germany, and requiring computer and Internet access to retrieve results is still not feasible for many, especially, the older generations or homeless persons. Additionally, even if they were and everybody could use them, there is still the need to be able to test and inform hundreds of thousands of tourists, visitors, and other non-residents. The fast spread of a pandemic and the large volume of potential patients mandates especially quick enrollment times, as to not tie up already sparse resources with registering and setting up patients identities. Although the setup should be quick, it should be protected against errors, which would prevent the patient from accessing the results. Another considerable aspect is the cost of the authentication method. Handing out smart cards or access tokens can probably increase security but would also rise costs immensely. Additionally, those devices may not be sufficiently available at the time.

This scenario is also applicable outside of large scale pandemics, where it could free up capacities. From the description of this scenario the following requirements for authenticating patients to labs have been gathered:

- **REQ9:** Readily available, independent of nationality, age, or permanent residence.
- **REQ10:** (Mass) availability of authentication tools.
- **REQ11:** Quick but error resistant enrollment.
- **REQ12:** Low cost per identity.

## 2.4 Patients' Physical and Mental Handicaps

Sometimes it may not only be the environment that increases the difficulty of performing an authentication according to a specific method. Disabilities – even if only temporary (e.g., wound dressings or injuries during or after hospitalization) – affect a substantial percentage of the population at least once in their lifetime, as such, this scenario describes the effects of common disabilities on authentication methods. Due to mental handicaps, knowing something may be more difficult, e.g., with respect to remembering secure passwords or passphrases. This for instance affects many people with learning disabilities, Alzheimer's, or dementia. As affected persons cannot reliably remember passwords, personal identification numbers (PIN) codes, or passphrases – which they may need to access their computer, smartphone, or apartment/rooms – they must rely on other approaches, that ideally do not degrade security. Quite the contrary: The authentication methods should be more secure to prevent others taking advantage of the affected persons.

Besides mental handicaps, other categories of disabilities exist. A physical handicap may impede having or effectively using something you have, like controlling a smartphone or smart card. Similarly, certain body parts may not conform to expected properties hindering people with physical handicaps to show something they are, e.g., provide a fingerprint or iris scan. Last but not least, the way interfaces are interacted with and how a user with some kind of handicap does it can also vary widely from non-handicapped users, e.g., using a Braille keyboard.

This list of potential difficulties with authentication methods is not exhaustive – and due to the diversity of conditions probably

never can be – but provides an idea for facets that have to be regarded when designing an authentication workflow. As a result and regardless of the existence or severity of disabilities of the users, a good authentication system should allow to substitute one authentication method with another as a user's choice. Most smartphones already do a pretty good job in this regard, as they usually offer authentication via PIN, pattern, fingerprint, face recognition, location, or proximity of other devices. The security of the different methods obviously differs and has to be taken into consideration when allowing a user to choose their preferred authentication method. This results into the following requirements:

- **REQ13:** User-substitutable authentication methods.
- **REQ14:** Wide range of authentication methods from different categories.
- **REQ15:** Use a combination of methods to mediate effects of weaker authentication methods.
- **REQ16:** Preferred authentication method has to be treated as personal information.

## 2.5 Requirements based on Use-Cases

Based on the healthcare related scenarios described in the sections above, the following requirements can be gathered:

- **REQ1:** Time-saving, reliable methods.
- **REQ2:** Easy to handle when under pressure.
- **REQ3:** Multi-user-devices.
- **REQ4:** Protection of sensitive information.
- **REQ5:** Usable with disposable gloves.
- **REQ6:** Suitable for mobile devices.
- **REQ7:** Consideration of advanced hygiene aspects.
- **REQ8:** Usability.
- **REQ9:** Readily available, independent of nationality, age, or permanent residence.
- **REQ10:** (Mass) availability of authentication tools.
- **REQ11:** Quick but error resistant enrollment.
- **REQ12:** Low cost per identity.
- **REQ13:** User-substitutable authentication methods.
- **REQ14:** Wide range of authentication methods from different categories.
- **REQ15:** Use a combination of methods to mediate effects of weaker authentication methods.
- **REQ16:** Preferred authentication method has to be treated as personal information.

Table 1 shows that scenarios S 1 and S 2 share most requirements, while scenarios S 3 and S 4 are rather unique. The diversity of requirements makes it harder to find a common approach.

## 3 GENERALIZATION OF CHALLENGING CONDITIONS

In favor of providing a general overview of challenging conditions for authentication in scenarios from Section 2, we could identify several groups of important aspects. We identified *six superordinate groups* in which requirements, as some of them have been described in the previous section, can be assigned to. These six superordinate groups are the following:

**Table 1: Overview of requirements in the use-cases**

Situations	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6	REQ7	REQ8	REQ9	REQ10	REQ11	REQ12	REQ13	REQ14	REQ15	REQ16
Emergency Care and Vehicle Services	x	x	x	x	x	x	x									
Hospitalization and Care	x				x	x	x	x								
(Mass) Testing and Communication									x	x	x	x				
Physical and Mental Handicaps													x	x	x	x

**Reliability:** First of all, for some scenarios requirements regarding reliability are very important, e. g., false-negatives in user authentication hinders medical personnel in performing one's duty. Further factors are, e. g., online and offline usage, ease of recovery, and fast authentication.

**Security:** Second, the security of an authentication mechanism is very important, since false-positives may lead to the violation of confidentiality, integrity or availability of protected data. Security relates to, e. g., different attack vectors, either towards the method, the implementation, the person using it, or the underlying hardware, and the replacement of compromised authentication material.

**Usability:** Third, usability and adequacy, e. g., for handicapped people, also affects a lot of scenarios as disregarding user-friendly methods leads to bypassing authentication mechanisms, e. g., by not sticking to lock-screen-policies. Factors are, for example, time consumption and error prone.

**Environmental Requirements:** Another related group of requirements can be described as environmental requirements, i. e., requirements that stem from special circumstances of a device's usage, e. g., shared devices and frequent user switching. Further environmental requirements relate to restrictions, e. g., input, physical, operational, and legal restrictions. Input restrictions describe that users cannot access or operate input devices, e. g., due to protective clothing like gloves. The environment is not suitable for specific technologies, e. g., high humidity or electromagnetic interference, when having physical restrictions. In order to ensure work is done as planned, some methods may be hindering, e. g., time constraints. Specific protections are required or prohibited legally, e. g., requiring smart cards and prohibiting facial recognition. This group of challenging conditions for instance also covers hygiene aspects and cleansing, as we mentioned especially in Scenario 1 and 2. Costs for methods can fall into this category, but it depends on the actual planned implementation as well as on the status quo.

**Data Protection and Privacy:** Even though we did not explicitly address these groups in our scenarios, further challenging conditions may appear in the matter of data protection and privacy. For instance, considering online voting and special health conditions, e. g., being HIV positive. Requirements range from personal information to anonymous identification.

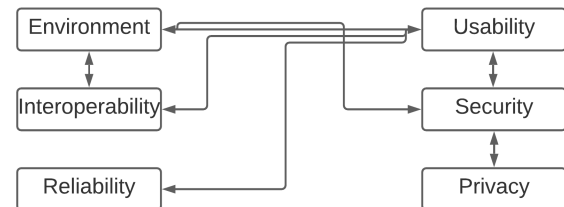
**Interoperability:** Interoperability is especially important regarding authentication mechanisms that depend on other devices, e. g., smart card or USB-stick-based mechanisms. We

generalize this requirement with interoperability towards software and hardware. It also relates to usability.

Interoperability impacts the usability. The same applies for reliability and usability, as many false-negatives affect usability. Furthermore, privacy requires security. Though security can be maintained, while privacy is lacking. This is the case if, e. g., a bank sells personal information to a marketer. Also, security and usability can contradict each other. A system, which is shutdown, is secure, but not usable anymore. Nevertheless, if a system is not usable anymore, then the users tend to find ways around it, which can again affect the security. Environmental requirements can have effects on other requirements, like interoperability, usability, and security. The dependencies between the requirements can be seen in Figure 1. Table 2 shows how the requirements we deduced from our scenarios in Section 2 can be classified according to the six groups we stated in this section.

#### 4 OVERVIEW OF EXISTING AUTHENTICATION MECHANISMS

General security issues for components of cyber-physical systems related to healthcare have been described in detail by [33]. The focus *user authentication* of this work is often times not considered. Common mechanisms are based on something you know, something you have, something you are, and something you do. According to Kizza [18], authentication can be based on the following user items: username, password, retina images, fingerprints, physical location, and identity cards. The author describes voice recognition and hand geometry as further biometric methods. Besides something you know, we categorize the authentication mechanisms into physical means for authentication and biometric authentication mechanisms. Biometrics are further divided into physiological and behavioral. In the following, we describe authentication for these categories, prior to approaches related to the three scenarios described in Section 2.

**Figure 1: Dependencies between the requirements.**

**Table 2: General categories of the scenarios' requirements**

Group	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6	REQ7	REQ8	REQ9	REQ10	REQ11	REQ12	REQ13	REQ14	REQ15	REQ16
Reliability	x									x			x			
Security				x						x	x				x	
Data Protection and Privacy			x	x							x					x
Usability	x	x			x	x		x	x	x	x		x			
Environmental requirements	x	x	x		x		x	x		x		x				x
Interoperability									x	x			x	x		

#### 4.1 Knowledge-based Authentication Mechanisms

Typical knowledge mechanisms are passwords, PINs, and transaction numbers (TANs). Raza et al. [31] see graphical passwords as another pattern and suggest combining authentication methods. Nevertheless, they are not unique and can be guessed or attacked. If they are forgotten, it is important not to rely on questions, where the answer can be guessed or googled. As pictures are typically easier to remember than passwords, Xiaoyuan Suo et al. [37] propose graphical passwords.

#### 4.2 Possession-based Authentication Mechanisms

Something you have is widely used with MFA. A physical item can be, e. g., a security key, USB token, smart card, radio-frequency identification (RFID) or near-field communication (NFC) chip or Bluetooth. Physical mechanisms can be blocked, broken, forgotten, getting stolen or otherwise fail. Therefore, it is important to have a backup strategy. Sportiello [36] analyzes different attack vectors on smart cards. The authors of [6] present a lightweight authentication scheme for wearable devices and mobile terminals using bit-wise exclusive-OR and hash function operations.

#### 4.3 Behavioral Biometric Authentication Mechanisms

Several approaches for behavioral biometric authentication are developed. Specially designed for cyber-physical systems used in healthcare, the authors of [1] describe methods for body sensors to authenticate the user based on body movement (e. g., depending on the location of the device hand or head movement) or sensor data (e. g., electroencephalogram, EEG). The authors of [28] include voice recognition, signature recognition, gait recognition, behavior profiling, keystroke dynamics, and touch dynamics into behavioral biometric authentication. They assume behavioral biometrics as not so accurate and stable, but as continuous and transparent authentication. Foot gestures may result in behavior profiling. Lopes et al. [24] use a set of multi-modal interactions combining hand and foot input for supporting contactless 3D manipulation tasks. Drivers are authenticated by tap sequences in the approach of Kun et al. [21]. The authors of [9] designed an approach based on dynamic audio token on android operating system. Kumar and Rauthan [20] analyze typing patterns. Mainali et al. [25] improve privacy-enhancing context authentication from location-sensitive data.

#### 4.4 Physiological Biometric Authentication Mechanisms

Ruoti et al. [32] analyze the usability of different web authentication systems. Physiological biometrics appears to be user-friendly and innovative. Meng et al. [28] present a taxonomy for existing biometric authentication on mobile phones. They describe physiological biometric authentication including fingerprint, face, iris, retina and hand just as palm recognition. Physiological biometrics are unique, but can be modified, e. g., by cuts, lacks accuracy, and need additional hardware. Both subdivision of biometric authentication, physiological and behavioral, have false-negative and false-positive rates. This is also depending on the implementation. For instance, the authors in [25] relate to error rates up to 10% for contextual authentication schemes. Last but not least, the authors and Spolaor et al. [35] outline potential attack vectors, i. e., side-channel analysis. Sebastian [34] compares different biometric methods with security level, user acceptance, ease of use, costs, errors, and hardware. Weissenfeld et al. [41] describe the advantage of 4-fingerprint authentication versus 1-fingerprint authentication for border control. Their approach is contactless, using mobile phones. In contrast, Marattukalam and Abdulla [26] suggest the use of deep learning algorithms for decision-making related to palm veins as contactless method. Physiological biometric mechanisms can be combined, cf. Herbadji et al. [16], where iris and major finger knuckles are used.

#### 4.5 Existing Approaches Related to the Care Cycle

The authors of [39] describe a RFID based secure mobile communication framework for emergency response management. This approach could be used for S 1. Other approaches related to blue light organizations concentrate on fleet management though.

With respect to S 2, authentication challenges in a hospital environment, only little research work has been undertaken with these special issue. In a rather recent publication by Ehrler et al. [8], the authors issue challenges with and solutions for suitable authentication methods for shared mobile devices in hospitals. Key problems are, for instance, that mobile devices like smartphones usually do not provide a proper management of multiple identities and possibilities to reduce costs and expenses by the introduction of BYOD (bring your own device) for personal devices while opening new security vulnerabilities. Based on a theoretical evaluation of seven authentication mechanisms, i. e., password, pattern-based passwords, certificates, smart cards, hardware tokens, biometrics

and proximity, the authors propose using a combination of proximity and password-based authentication. However, as the authors state themselves, not only the process but especially human factors need to be evaluated in a more detailed manner. Another very important authentication issue in a hospital environment is addressed in [14]: Single Sign On (SSO) solutions. In their paper, the authors especially discuss privacy concerns implicated by SSO, which they evaluated in the context of a field study in a larger hospital. On the one hand, SSO is highly desirable from the perspective of usability while, on the other hand, SSO may entail security holes. Furthermore, according to the authors, SSO also involves potentially major changes, e. g., the replacement of generic user identities with unique user ids (which is appropriate due to a number of reasons, e. g., regarding privacy regulations and traceability). Their concerns with respect to allowing the surveillance of employees can rather be seen as a problem that is not directly attached to SSO. Kyriacou et al. [22] and Gai et al. [10] consider authentication in pandemics like COVID-19 with focus is on the fleet management. Nevertheless, other large-scale environments can be compared, like online banking or voting.

Regarding our fourth scenario, the influence of disabilities on how authentication can be done has been researched by various authors. In [19], Kowtko describes the effects of aging just as aging-related physiological changes and diseases on biometric authentication methods. They range from general usability problems with the unstructured and frequently changing environment of the Internet through the inability of fingerprint recognition systems to recognize users because of physiological changes associated with heart failure to problems of iris and facial recognition systems because of cataracts or similar diseases. In another example, Helkala [15] analyzes the effects of Parkinson's, dyslexia, visual impairment, and upper extremity disabilities on common authentication methods like PINs, passwords, and one-time codes. The author shows that most regarded disabilities lower the security of most authentication methods and increase the time it takes for the user to authenticate. Similarly, but focusing only on the aspect of visual impairment, i. e., blindness or low vision, Dosono et al. [7] gather the main challenges for vision impaired users when using common online services like email, social media, or banking applications. The results show that the main problems are due to usability and accessibility problems, like finding the login fields or waiting for screen reading software to finish reading the pages. An advanced method of authenticating users via an EEG is described by the authors of [13]. Their research explores the feasibility of authenticating a user based on data recorded by an EEG when the user is presented with a series of pictograms from which the user mentally selects one. The results of their study indicate that a highly secure "neuroauthenticator" could be built, not only for disabled people but also for environments that require very high security.

## 5 SUITABILITY OF AUTHENTICATION MECHANISMS

As shown in the previous section, there are plenty of authentication mechanisms from various categories – knowledge, physical, behavioral, or physiological means. In the following sections, we want to align these authentication methods with challenges we

condensed into six general groups in special environmental or situational conditions, cf. Section 3. As a result, we strive to provide a conceptual assistance structure for decision-making in regard to choosing a proper authentication mechanism for special conditions, also considering MFA.

### 5.1 Reliability

Both classical mechanisms for authentication, password and pattern, are reliable, as both can be checked offline and there can neither be false negatives nor positives. The speed is comparably slow, while phishing and other attacks exist. Dependent on the physical authentication mechanisms and the implementation, the reliability is medium to high. Due to different difficulties, it is important to have a backup strategy. As biometrics are unique, they are more reliable in verifying a claimed identity, see approaches in Section 4.4. Especially physiological authentication mechanisms might fail after accidents and other changing actions, e. g., wearing masks while using face recognition. Therefore, a backup mechanism is important. The speed of physiological authentication mechanisms tends to be higher than of behavior authentication mechanisms.

### 5.2 Security

Besides the following issues, compromised servers and social engineering are attack vectors. In terms of security, classical authentication mechanisms tend to be compromisable if an attacker has access to the hardware or is nearby for shoulder surfing [17]. Additionally, passwords can be phished or cracked in the worst case. Passwords, patterns, and PINs can be guessed in the worst case, e. g., from heat traces [23] and smudges [4] or simple trial and error [27]. The top 20 probable patterns unlock up to 32.55% [5].

Physical authentication mechanisms are often used as a second factor in order to improve security. The device cannot be "guessed" and phishing is only possible face to face. If a physical device being the single factor gets stolen, the security is not given anymore. Also, the implementation can have security bugs, see smart cards [36] and older products, e. g. by MIFARE [11], as well as the transmission.

As described in terms of reliability concerns, biometric authentication mechanisms are not as accurate as other mechanisms [34]. In addition to the mechanism, the security depends on the implementation [3, 38]. Since the behavior is harder to mimic, the security of behavioral biometric authentication is higher in comparison. If the biometric information in the database is stolen, it may have a large privacy impact, depending on the way the information is stored.

### 5.3 Data Protection and Privacy

With respect to data protection and privacy, classical password pattern authentication is a rather decent approach. Using a password-based approach allows you to use pseudonyms as it is already good practice in many organizations. Thus, an attacker has to guess your ID and password. A similar method regarding privacy-protecting knowledge-based authentication is described in [29] where the authors propose a ticket-based approach for e-voting. A comparison of different approaches is conducted in [12], indicating that privacy may benefit from novel paradigms such as Blockchain.

Also, the physical authentication mechanisms can be good with regard to data protection. They can similarly be used for a privacy-conserving authentication approach, since they are not necessarily bound to a specific person's entity.

The third group of authentication mechanisms, biometric mechanisms, however, is usually rather inappropriate with respect to data protection and privacy. They are closely bound to a specific person and cannot be handed over to others (which is very desirable in terms of security and reliability, however not in terms of privacy).

## 5.4 Usability

Considering the mentioned approaches in terms of usability, password-based authentication usually performs very bad, especially as soon as passwords comply with suitable password policies regarding their strength, length and changing cycles of several weeks to month, as well as related policies like locking one's displays as soon as she leaves the device. Password-based authentication is usually very time-consuming and error-prone, minimizing usability especially considering potential user's disabilities or hectic environments. Considering PINs, blacklisting improves the security, if the list is large, while it has at the same time an effect on the usability. According to [27], blacklisting 10% is the ideal ratio.

Physical authentication mechanisms usually perform way better in this respect. Especially security keys, USB tokens, smart cards or NFC-based authentication mechanisms can overcome the mentioned drawbacks of password-based authentication. Mobile authentication, for instance using Bluetooth-based presence-indicating approaches, however, are very dependent from the specific scenario surroundings. In crowded environments with shared IT-systems, these mechanisms will probably rise to problems since an authentication of users cannot be pursued unambiguously.

Biometric authentication mechanisms usually provide very good usability, especially in terms of authentication with disabilities, since these approaches do not require something you need to know, nor something you need to have, but something you are. Due to the existence of many of suitable approaches in this area, they can be suitably selected according to a specific scenario.

## 5.5 Environmental Requirements

The environment, in which an authentication method should be primarily used, influences the choice of suitable options immensely. Especially knowledge-based authentication, i. e., passwords or PINs, are often error-prone and too slow with regard to most of the mentioned limitations in healthcare environments. Possession-based authentication, i. e., smart cards or USB/RFID/NFC/Bluetooth tokens, may also be affected by some limitations as protective clothing, potentially hindering personnel carrying electronic devices. Biometric authentication systems – i. e., for fingerprint, face/iris recognition – can also likewise be limited by the environment (e. g., face masks). Additionally, biometric authentication may fail or be unreliable in freezing or hot and humid conditions, due to the body's reaction.

## 5.6 Interoperability

A key component when selecting authentication methods is sufficient interoperability with the system that needs to be protected, the people using it, and the environment it is used in. This aspect is

one of the most challenging ones, as meeting all three conditions is particularly hard. Password-based authentication is basically a de facto standard that is implemented in almost every system, but it is also impossible or cumbersome to use in many situations. Authentication based on biometrics and to some extent also tokens can be used with far fewer systems. Only very few systems allow for interchangeable authentication methods based on users' needs and current environmental factors. Consequently, careful planning in advance is required if less common authentication methods seem more suitable.

## 5.7 Matrix for Systematic Decision-Making

In the previous sections, we analyzed different authentication mechanisms based on the derived generic requirements and resulting sub-requirements. In order to be able to choose a mechanism, a scoring scheme is applied. Based on sub-requirements discussed in text in the previous section and the average weight by independent experts, the sub-requirements receive weights. Three points provide are accurate enough while being easy to handle. Requirements and sub-requirements, which are completely fulfilled, count with a weight of 2 points, while half-fulfilled score 1 point, and non-fulfilled with 0 points. This method is done per requirement, shown in Figure 2 for environmental requirements. Environmental requirements are divided into input restrictions, physical restrictions, operational restrictions, and legal restrictions.

In order to reduce the complexity, each requirement is condensed to an average scoring per requirement and authentication mechanism, as shown in Figure 3. If sub-requirements should weight differently, it is though necessary to take this into account for the final decision. To use our decision matrix, the weighting  $W1$  to  $W6$  of the individual group must be adapted to a corresponding use-case. Then, for each row representing a different authentication scheme, the evaluated value must be multiplied to the corresponding weights. The granularity is left to the user of the decision matrix: She may choose to use integer or floating weights numbers between 1 and 3. It has to be noted that the decision matrix depicted in Figure 3 is biased towards the possession-based authentication methods. No matter how the individual aspects are weighted, due to the consistent high scores for possession-based methods, they will always come out on top. The other authentication methods, however, can be influenced by the weighting. This inherent bias in the matrix is not necessarily a flaw in the design, but rather the result of possession-based authentication methods being fairly flexible and easy to use in general. Additionally, in order to take into account strict impossibilities with respect to one of the authentication mechanisms groups (e. g., knowledge-based authentication for people with mental disabilities may sometimes be highly impractical), one or more groups can be disregarded.

## 6 DISCUSSION OF THE DECISION MATRIX

To choose the best-fitting authentication mechanism for a specific situation in the healthcare cycle, the requirements should be weighted by the responsible persons and in dependence on a certain use-case. In order to evaluate our approach, we apply the selection of suitable authentication mechanism to our scenario with its multiple challenging situations described in Section 2. The weights are

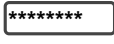



Environmental Requirements	Knowledge 	Possession 	Behaviour 	Biometric 
Input restrictions	0	1	2	1
Physical restrictions	1	1	1	1
Operational restrictions	0	2	2	1
Legal restrictions	2	2	1	1

Figure 2: Matrix for environmental requirements.

the result of the average weights gained by the authors after further discussions with experts. The outcomes were the basis for additional discussions with administrators, and end users in the related areas. Due to restrictions caused by COVID-19 we did not carry out a full user study. It though may already help persons in charge, e. g., in hospitals with identifying adequate authentication mechanisms. We plan a two-stage user study for future work, divided into technical assessment by administrators and user experience by end users.

### 6.1 Emergency Care and Emergency Vehicle Services

With the need for fast available information, even with changing persons, the reliability is weighted high with W1 3 points. Even though sensitive data is handled, security can be seen as lower in comparison, using W2 with 2 points. The same applies for data protection and privacy W3. This is especially the case, as the vehicles are typically not open for foreigners and passengers are nearby or inside the vehicle. Additionally, the focus of intruders is typically not personal information. Usability W4 and environment requirements W5 are further problems in this use-case, resulting in 3 points each. The need for interoperability is considered low, leading to W6 of 1 point. By weighting the requirements, the following result can be gained, shown in Figure 4.

As a result, possession authentication mechanisms with 2 points in average and a sum of 28 points should be chosen. Smartcards, tokens, and keys are fast, easy to use (even with disposable clothes and cleaned with disinfection liquids). Therefore, they are highly suitable. In order to determine a concrete method, further investigation is needed. Knowledge, behavior, and biometric are similarly good as second factor or fallback with 14 points.

### 6.2 Hospitalization and Care

In the situation of hospitalization and care, the decision matrix can be applied as follows: Reliability is very important in medical scenarios in order to provide reliable treatments, resulting in W1 of 3 points. Security can also be considered quite high with 2 points for W2, since hospitals are open to public. Privacy can be rated with a modest importance of 1 point for W3, since using medical devices in hospitals does not stipulate any special requirements in those terms. Usability is, however, very important since physicians and nurses must work efficiently and every day with their equipment. Also, environmental requirements are quite challenging in hospitals,

since there are many constraints as hectic surroundings and hygiene aspects. We weight both – W4 and W5 – with 3 points. Finally, the interoperability aspect W6 can be considered as rather low: Necessary functions, e. g., documentation, treatment research, and information gathering, are provided by commercial-off-the-shelf centralized services.

Noticeably, the evaluation for this situation is similar to the previous one: The most suitable authentication method is possession-based with 26 points in total, followed by a biometric-based approach with 15 points. The latter might consequently be fit as a second factor. A behavioral and knowledge-based approach perform slightly worse with 14 and 13 points respectively.

### 6.3 (Mass) Testing and Communication

With many potential users that need to be authenticated – possibly on very short notice – the usability and interoperability is extremely important. This assessment is backed by the need to support many people that might not be particularly tech-savvy. In the (mass) testing scenario usability therefore rank highest between the different requirement categories with 3 points. Reliability is also quite important and is assigned 2 points. A failure of either reliability or interoperability can lead to the need for increased support effort up to a point where the system becomes unusable. Last but not least security, privacy, and environmental is not extremely important but should obviously still be considered carefully.

With those parameters in mind, the most suitable approach (with 22 points) is a possession-based approach. This result is validated by real-world adaption, where COVID-19 test results are sent to tested people by mail in combination with a password sent via SMS. The other methods score significantly lower with 8 to 14 points. Deployment and user training for those authentication methods seems to difficult for mass use.

### 6.4 Patients' Physical and Mental Handicaps

For people affected by disabilities, the scenario described in Section 2 focuses on the reliability and interoperability of different solutions. Those requirements are needed to support the many facets of disabilities. As a result, W1 and W6 are the most important and are scored with 3 points. Moderately increased importance is determined for the usability requirement. Because disabilities usually reduce the ease of interaction, having a user-friendly design to begin with is important. This is depicted by scoring 2 points to W4. The requirements for security W2, privacy W3, and environmental








		Reliability *W1	Security *W2	Privacy *W3	Usability *W4	Environmental *W5	Interoperability *W6
Knowledge	*****	1	2	1	1	0	2
Possession		2	2	2	2	2	2
Behaviour	 	1	1	0	1	2	0
Biometric	 	2	1	0	1	1	1

Figure 3: Decision matrix for proper and scenario-based authentication mechanisms selection.






		Reliability 3x	Security 2x	Privacy 2x	Usability 3x	Environmental 3x	Interoperability 1x	
Knowledge	*****	1	2	1	1	0	2	14
Possession		2	2	2	2	2	2	28
Behaviour	 	1	1	0	1	2	0	14
Biometric	 	2	1	0	1	1	1	15

Figure 4: Application of the decision matrix on Scenario 1

factors W5 are usually not elevated above regular levels. Therefore, they do not receive any special score and are assigned 1 point.

After applying the scoring factors to the matrix, the resulting score favors possession-based authentication methods with 22 points. This clear first place is followed by a tie between knowledge-based and biometric authentication factors, both 14 points. The least suitable authentication method – according to the matrix – for this situation is behavior-based authentication with 8 points.

### 6.5 Authentication with Specific Disabilities

As our scenario generically considers disabilities, we want to give a specific example, where the results also differ. Let us assume that the person affected by disabilities has amyotrophic lateral sclerosis (ALS). ALS is a motor neuron disease causing the death of neurons controlling voluntary muscles. Stephen Hawking was a known example. Since the input, physical, and operational restrictions are limiting the affected person, the sub requirements are used for the evaluation. At the same time, the range for weights is increased to 10, in order to quantify the environment restrictions input, physical, and operational. The sub requirements in reliability as well as software interoperability gains 2 points, while usability receives 5 points. This results in 75 points for possession (average of 1.5), 67 points for behavior (average 1.34), 55 points for biometric (average 1.1), and 38 points for knowledge (average 0.76). If, for example, the wheelchair can be used for possession based authentication, this is an easy method for the person. If not, the next method is behavior, where, e. g., muscle movements are one option.

## 7 CONCLUSION AND FUTURE WORK

Identities are everywhere and with growing identity theft and credential stuffing attacks, secure identity management gets more

and more relevant. One important factor for the acceptance and inclusion of identity management is authentication. This is not only the case within cyber-physical systems in healthcare environment, which we focused on. Additionally, special conditions require special authentication mechanisms. In this paper, we show that authentication with special conditions has specific requirements that are not always regarded. Based on real world scenarios within the care cycle, we gathered specific requirements. We then generalized them to reliability, security, data protection just as privacy, usability, environmental requirements, and interoperability. These requirements were used to evaluate different existing approaches, resulting in a matrix which can be adapted according to a certain use-case in order to promote a systematic decision-making approach.

The matrix consists of authentication mechanisms and weighted fulfillment of requirements. With this matrix, a first as well as a second factor can be chosen. This is shown by applying the four real world situations in our scenario, which were used to extract requirements. In order to choose a specific authentication mechanism, more work needs to be done. The weighted requirements cannot only guide in scenarios with special conditions, but everywhere, where guidance is needed. As a result, all stakeholders can profit from this matrix, which includes different approaches and requirements and is flexible enough for future approaches.

A more thorough user study is planned in a future work with a special focus on the area of blue light organizations and especially hospital environments, where we maintain good relations from several projects. For our evaluation approach, we plan a two-stage user study where we want, on the one hand, the implementation perspective where we ask administrators in charge of implementing authentication approaches, and on the other hand, atop the prior study, we are going to evaluate the user comfort and suitability in

the area. Additionally, we plan to improve the matrix by detailed guidance for different authentication mechanisms. Last but not least, we plan to adapt the matrix for virtual reality based on [30].

## REFERENCES

- [1] Abdullah Alhayajneh, Alessandro N. Baccarini, Gary M. Weiss, Thair Hayajneh, and Aydin Farajidavar. 2018. Biometric Authentication and Verification for Medical Cyber Physical Systems. *Electronics* 7, 12 (Dec. 2018), 436. <https://doi.org/10.3390/electronics7120436>
- [2] Ali Abdullah S. AlQahtani, Hosam Alamleh, Jean Gourd, and Hend Alnuhait. 2020. TS2FA: Trilateral System Two Factor Authentication. In *2020 3rd International Conference on Computer Applications Information Security (ICCAIS)*. 1–4.
- [3] Namrata Bhartiya, Namrata Jangid, and Sheetal Jannu. 2018. Biometric Authentication Systems: Security Concerns and Solutions. In *2018 3rd International Conference for Convergence in Technology (I2CT)*. 1–6.
- [4] Seunghun Cha, Sungsu Kwag, Hyoungshick Kim, and Jun Ho Huh. 2017. Boosting the Guessing Attack Performance on Android Lock Patterns with Smudge Attacks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (Abu Dhabi, United Arab Emirates) (ASIA CCS 17)*. Association for Computing Machinery, New York, NY, USA, 313–326. <https://doi.org/10.1145/3052973.3052989>
- [5] Geumhwan Cho, Jun Ho Huh, Junsung Cho, Seongyeol Oh, Youngbae Song, and Hyoungshick Kim. 2017. SysPal: System-Guided Pattern Locks for Android. In *2017 IEEE Symposium on Security and Privacy (SP)*. 338–356.
- [6] Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, and YoungHo Park. 2018. Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment. *IEEE Journal of Biomedical and Health Informatics* 22, 4 (2018), 1310–1322.
- [7] Bryan Dosono, Jordan Hayes, and Yang Wang. 2018. Toward Accessible Authentication: Learning from People with Visual Impairments. *IEEE Internet Computing* 22, 2 (2018), 62–70.
- [8] Frédéric Ehrler, Katherine S Blondon, Dominique Baillon-Bigotte, and Christian Lovis. 2017. Smartphones to Access to Patient Data in Hospital Settings: Authentication Solutions for Shared Devices. In *pHealth*. 73–78.
- [9] Yangyang Sha et. al. 2016. The design of Access Control System based on dynamic audio token. In *2016 International Conference on Audio, Language and Image Processing (ICALIP)*. 106–110.
- [10] Keke Gai, Yulu Wu, Liehuang Zhu, Kim-Kwang Raymond Choo, and Bin Xiao. 2020. Blockchain-Enabled Trustworthy Group Communications in UAV Networks. *IEEE Transactions on Intelligent Transportation Systems* (2020), 1–13.
- [11] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. 2009. Wirelessly Pickpocketing a Mifare Classic Card. In *2009 30th IEEE Symposium on Security and Privacy*. 3–15.
- [12] Kanika Garg, Pavi Saraswat, Sachin Bisht, Sahil Kr Aggarwal, Sai Krishna Kothuri, and Sahil Gupta. 2019. A Comparative Analysis on E-Voting System Using Blockchain. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*. IEEE, 1–4.
- [13] Ryohei P. Hasegawa, Yukako T. Hasegawa, and Yoshiko Nakamura. 2017. Development of Neuroauthenticator: Feasibility of an EEG-based Authentication. In *2017 International Conference on Biometrics and Kansei Engineering (ICBAKE)*. 127–131.
- [14] Rosa R Heckle and Wayne G Lutters. 2007. Privacy Implications for Single Sign-on Authentication in a Hospital Environment. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*. 173–174.
- [15] Kirsi Helkala. 2012. Disabilities and Authentication Methods: Usability and Security. In *2012 Seventh International Conference on Availability, Reliability and Security*. 327–334.
- [16] Abderrahmane Herbadji, Noubel Guermat, Lahcene Ziet, and Mohamed Cheniti. 2019. Multimodal Biometric Verification using the Iris and Major Finger Knuckles. In *2019 International Conference on Advanced Electrical Engineering (ICAEE)*. 1–5.
- [17] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Evaluating Attack and Defense Strategies for Smartphone PIN Shoulder Surfing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) (CHI 18). Association for Computing Machinery, New York, NY, USA, 1–10. <https://doi.org/10.1145/3173574.3173738>
- [18] Joseph Migga Kizza. 2017. Authentication. In *Guide to Computer Network Security*. Joseph Migga Kizza (Ed.). Springer International Publishing, Cham, 207–225. [https://doi.org/10.1007/978-3-319-55606-2\\_10](https://doi.org/10.1007/978-3-319-55606-2_10)
- [19] Marc Alexander Kowtko. 2014. Biometric authentication for older adults. In *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*. 1–6.
- [20] Pramod Kumar and Manmohan Singh Rauthan. 2016. Remote User Authentication Scheme: A Comparative Analysis and Improved Behavioral Biometrics Based Authentication Scheme. In *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*. 311–313.
- [21] Andrew L. Kun, Travis Royer, and Adam Leone. 2013. Using Tap Sequences to Authenticate Drivers. In *Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (Eindhoven, Netherlands) (AutomotiveUI 13). Association for Computing Machinery, New York, NY, USA, 228–231. <https://doi.org/10.1145/2516540.2516567>
- [22] Efthymoulos Kyriacou, Riana Constantinou, Chris Kronis, George Hadjichristofi, and Constantinos Pattichis. 2020. eEmergency System to Support Emergency call Evaluation and Ambulance dispatch Procedures. In *2020 IEEE 20th Mediterranean Electrotechnical Conference (MELECON)*. 354–357.
- [23] Duo Li and Xiao-Ping Zhang et. al. 2018. Modeling Thermal Sequence Signal Decreasing for Dual Modal Password Breaking. In *2018 25th IEEE International Conference on Image Processing (ICIP)*. 1703–1707.
- [24] Daniel Lopes, Filipe Relvas, Soraia Paulo, Yosra Rekik, Laurent Grisoni, and Joaquim Jorge. 2019. FEETICHE: FEET Input for Contactless Hand gEsture Interaction. In *The 17th International Conference on Virtual-Reality Continuum and Its Applications in Industry* (Brisbane, QLD, Australia) (VRCAI 19). Association for Computing Machinery, New York, NY, USA, Article 29, 10 pages. <https://doi.org/10.1145/3359997.3365704>
- [25] Pradip Mainali, Carlton Shepherd, and Fabien A. P. Petitcolas. 2019. Privacy-Enhancing Context Authentication from Location-Sensitive Data. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (Canterbury, CA, United Kingdom) (ARES 19). Association for Computing Machinery, New York, NY, USA, Article 87, 10 pages. <https://doi.org/10.1145/3339252.3340334>
- [26] Felix Marattukulam and Waleed Abdulla Abdulla. 2019. On Palm Vein as a Contactless Identification Technology. In *2019 Australian New Zealand Control Conference (ANZCC)*. 270–275.
- [27] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2020. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *IEEE Symposium on Security and Privacy (SP '20)*. IEEE, San Francisco, California, USA, 1525–1542.
- [28] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou. 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys Tutorials* 17, 3 (2015), 1268–1293.
- [29] Yi Mu and Vijay Varadarajan. 1998. Anonymous secure e-voting over a network. In *Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217)*. IEEE, 293–299.
- [30] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland UK) (CHI 19). Association for Computing Machinery, New York, NY, USA, 1–12. <https://doi.org/10.1145/3290605.3300340>
- [31] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif, and Waqas Haider. 2012. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal* 19, 4 (2012), 439–444.
- [32] Scott Ruoti, Brent Roberts, and Kent Seamons. 2015. Authentication Melee: A Usability Analysis of Seven Web Authentication Systems. In *Proceedings of the 24th International Conference on World Wide Web* (Florence, Italy) (WWW 15). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 916–926. <https://doi.org/10.1145/2736277.2741683>
- [33] Kashif Saleem, Zhiyuan Tan, and William Buchanan. 2017. Security for Cyber-Physical Systems in Healthcare. In *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*, Christoph Thuemmler and Chunxue Bai (Eds.). Springer International Publishing, Cham, 233–251. [https://doi.org/10.1007/978-3-319-47617-9\\_12](https://doi.org/10.1007/978-3-319-47617-9_12)
- [34] Ruthy Sebastian. 2013. Literature Survey on Automated Person Identification Techniques. *International Journal of Computer Science and Mobile Computing - IJCSMC* 2, 5 (2013), 232–237.
- [35] Riccardo Spolaor, QianQian Li, Merylin Monaro, Mauro Conti, Luciano Gamberini, and Giuseppe Sartori. 2016. Biometric Authentication Methods on Smartphones: A Survey. *Psychology Journal* 14, 2 (Dec. 2016), 87–98.
- [36] Luigi Sportiello. 2019. "Internet of Smart Cards": A pocket attacks scenario. *International Journal of Critical Infrastructure Protection* 26 (2019), 100302. <https://doi.org/10.1016/j.ijcip.2019.05.005>
- [37] Xiaoyuan Suo, Ying Zhu, and G.S. Owen. 2005. Graphical Passwords: A Survey. In *21st Annual Computer Security Applications Conference (ACSAC 05)*. 10 pp.–472. <https://doi.org/10.1109/CSAC.2005.27>
- [38] Ruben Tolosana and Marta et. al. Gomez-Barrero. 2020. Biometric Presentation Attack Detection: Beyond the Visible Spectrum. *IEEE Transactions on Information Forensics and Security* 15 (2020), 1261–1275.
- [39] Thang Tran, Faqir Zarrar Yousaf, and Christian Wietfeld. 2010. RFID Based Secure Mobile Communication Framework for Emergency Response Management. In *2010 IEEE Wireless Communication and Networking Conference*. 1–6.
- [40] X. A. A. M. Verbeek and W. P. Lord. 2007. The Care Cycle: An Overview. *Medica-mundi* 51, 1 (2007), 06.
- [41] Axel Weissenfeld, Andreas Zoufal, Christoph Weiss, Bernhard Strobl, and Gustavo Fernández Domínguez. 2018. Towards Mobile Contactless 4-Fingerprint Authentication for Border Control. In *2018 European Intelligence and Security Informatics Conference (EISIC)*. 73–76.