CZECH TECHNICAL UNIVERSITY IN PRAGUE

FACULTY OF BIOMEDICAL ENGINEERING

Department of Health Care and Population Protection

Improving Computer Security in Healthcare Facilities through Biometric Authentication

Bachelor Thesis

Study programme:	Population Protection
Branch of study:	Planning and Management of Crisis Situations

Bachelor Thesis Author:	Tereza Špačková
Bachelor Thesis Supervisor:	Ing. Anna Horňáková, Ph.D.

Kladno 2023

BACHELOR‘S THESIS ASSIGNMENT

I. PERSONAL AND STUDY DETAILS

Student's name:	**Špačková Tereza**	Personal ID number:	**500117**
Faculty:	**Faculty of Biomedical Engineering**		
Department:	**Department of Health Care and Population Protection**		
Study program:	**Ochrana obyvatelstva**		
Branch of study:	**Planning and Management of Crisis Situation**		

II. BACHELOR’S THESIS DETAILS

Bachelor’s thesis title in English:

Improving Computer Security in Healthcare Facilities through Biometric Authentication

Bachelor’s thesis title in Czech:

Zlepšení zabezpečení počítačů ve zdravotnických zařízeních za pomoci biometrického ověřování

Guidelines:

The bachelor thesis addresses an analysis of the possibilities of using computer security through biometric authentication with a focus on healthcare. The result of the thesis will serve as a proposal for a solution for user identification or authentication using a selected biometric method. The theoretical part will focus on basic concepts and history of biometric authentication and description of selected methods of biometric identification and authentication. The practical part will include an analysis of different types of biometric authentication in comparison with other biometric methods with respect to the possibilities of improving computer security. The practical part is also focused on the current state of computer security in healthcare facilities. At the same time, it analyses the applicability of individual methods or specific applications in the field of healthcare. According to the results, a solution for user identification using the selected biometric method will be proposed as well as proposal for integrating the solution into the operation of the selected facility. The proposed methods are intended to be as much userfriendly and as least financially and technically demanding as possible.

Bibliography / sources:

[1] MEMON, Nasir, How Biometric Authentication Poses New Challenges to Our Security and Privacy , 2017, IEEE Signal Processing Magazine. Boston, MA: Springer US, 2015-7-3, 34(4), 196-194, 1053-5888

[2] SANCHEZ-REILLO, Raul, Hand Geometry, Encyclopedia of Biometrics. Boston, MA: Springer US, 2015, 2015-7-3, 849-854, ISBN 978-1-4899-7487-7

[3] ANTAL, Margit a Elöd EGYED-ZSIGMOND, Intrusion detection using mouse dynamics, 2019, IET Biometrics , 8(5), 285-294 , 2047-4938

Name of bachelor’s thesis supervisor:

Ing. Anna Horňáková, Ph.D.

Name of bachelor’s thesis consultant:

Mgr. Jitka Mariňáková, Ing. David Jirsa

Date of bachelor’s thesis assignment: **14.02.2023**
Assignment valid until: **20.09.2024**

doc. Mgr. Zdeněk Hon, Ph.D. Head of department	prof. MUDr. Jozef Rosina, Ph.D., MBA Dean

DECLARATION

I declare that I have prepared my bachelor thesis entitled Improving Computer Security in Healthcare Facilities through Biometric Authentication independently using only the sources listed in the bibliographic references.

I have no objection to usage of this work in compliance with the act § 60 no. 121/2000 Coll., (copyright law), and with the rights connected with the copyright act including the changes in the act.

In Kladno on May 12th 2023

....
Tereza Špačková

ACKNOWLEDGEMENTS

I would like to thank my supervisor Ing. Anna Horňáková PhD. for her time, patience, support and valuable advice that she provided me throughout the entire process of my bachelor thesis. I would also like to thank Ing. Jitka Mariňáková, who helped me a lot with the correctness of the English terminology. Gratitude goes to all the respondents and experts who provided me with information and suggestions for the thesis. Last but not least, I would like to thank my family for their support.

ABSTRACT

The bachelor thesis addresses applicability of biometric user authentication to improve computer security in healthcare facilities and focuses on both the biometric methods themselves as well as their implementation in healthcare facilities.

The theoretical part is devoted to technical information on biometric authentication, its history, classification of 10 different biometric methods and their introduction and description. It also describes what the abbreviations FAR, FRR and EER mean and their importance in assessing the reliability of biometric methods.

The practical part of the bachelor's thesis contains first an overview of the current state of computer security in hospitals performed by a questionnaire survey in which 80 healthcare facilities participated. The findings obtained from the questionnaire are further used to propose security improvements. The bachelor thesis also contains an analysis of selected biometric methods regarding their accuracy, user-friendliness and difficulties in their implementation. This section subsequently analyses selection of appropriate biometric methods based on the needs of healthcare facilities. Finally, the paper concludes with a proposed solution to improve current security state and its implementation in a healthcare facility.

Keywords

Biometrics; biometric authentication; healthcare; healthcare facilities; security; computer; cybersecurity

Contents

1 INTRODUCTION 8

2 OBJECTIVES OF THE THESIS 9

3 CURRENT STATUS overview 10

3.1 Biometric Authentication 11

3.1.1 History 11

3.1.2 Anatomical-physiological and behavioural biometrics 12

3.1.3 False Acceptance and False Rejection Rate 13

3.2 Selected methods of biometric authentication 15

3.2.1 Fingerprint Technology 15

3.2.2 Face Recognition Technology 16

3.2.3 IRIS Technology 16

3.2.4 Hand Geometry Technology 17

3.2.5 Palmprint Technology 17

3.2.6 Hand vein Technology 18

3.2.7 Voice recognition technique 18

3.2.8 Signature verification technique 19

3.2.9 Keystroke Dynamics 20

3.2.10 Computer Mouse Dynamics 20

4 METHODOLOGY 22

4.1 Structured interview 22

4.2 Multiple-criteria analysis 23

5 RESULTS 25

5.1 The questionnaire - Current state of HCF security 25

5.2 The analysis of biometric methods 29

5.3 The applicability of biometric methods in HCF.................................... 34

6 DISCUSSION 36

6.1 Evaluation of the current situation 36

6.2 Use of biometric methods... 39

6.3 Solution proposal and future outlook 44

7 CONCLUSION 49

8 LIST OF ABBREVIATIONS USED.. 50

9 LIST OF LITERATURE USED 51

10 LIST OF FIGURES USED 58

11 LIST OF TABLES USED 59

12 LIST OF ATTACHEMENTS.. 60

1 INTRODUCTION

A computer security in healthcare facilities is a topic which is becoming increasingly important, especially with the upcoming digitalisation of the Czech healthcare system. Data including a patient's health status, but also, for example, their birth number or insurance number, are among the most sensitive. Leaking or deleting them would pose a huge security risk that could directly endanger people's lives. Therefore, it is necessary to guard this data carefully and to avoid any leaks possibly caused by, for example, a lax approach of the staff. However, lower funding of the health sector which may result in a deteriorating security of sensitive data might potentially be also a problem.

Biometric authentication is one of the security techniques that is on the rise and its benefits cannot be denied. In particular, it is by far the most accurate as well as the most difficult to falsify method of determining whether a person is really who they say they are. Interlinking of these two sectors, i.e. healthcare security and biometric authentication, seems like a possible solution to improve sensitive data security while making authentication more accurate and user-friendly. This could then contribute to safer storage and use of patient data.

The bachelor's thesis focuses on this issue and in addition to addressing the current situation, it also aims to find possible improvements to the current system and to determine the applicability of biometric authentication in healthcare.

2 OBJECTIVES OF THE THESIS

The objective of the bachelor thesis is to determine current state of computer security in healthcare facilities, and, in particular, to determine whether the current state of security is sufficient and what changes, if any, would benefit it. Another goal is to analyse selected biometric methods and then evaluate their usability in healthcare facilities. The final aim of the bachelor thesis is to propose a suitable solution regarding computer security in these facilities using the selected biometric method and to propose its integration into the healthcare facility operation.

The theoretical part focuses mainly on the basic concepts of biometric authentication and the description of biometric methods. The practical part includes an analysis of different types of biometric authentication, current state of computer security in healthcare facilities overview and the evaluation of individual methods' applicability in the healthcare field. In conclusion, it also contains a proposal for a computer security solution and a proposal for the implementation of this solution.

3 CURRENT STATUS OVERVIEW

Computer security and how to ensure it is becoming an important topic currently. The amount of information and data we put into computers every day is enormous and it is crucial to ensure its protection against misuse. And therefore, computer security is becoming more and more critical. There are various ways to secure computers against misuse. This thesis will focus on the physical security of devices which means security against external intrusion into the system and, more specifically, the use of biometric authentication.

There are many techniques and tools which can be used to ensure the security of devices. Authentication is a basic term that refers to the security of access to a computer. It is the process by which someone or something is marked as authentic, which means true. User authentication is employed to confirm that the electronic form of a user's identity corresponds to the user's actual individuality. It verifies the legitimate login of the owner and checks unauthorised login attempts. This form of security is always based on at least one specific factor. There are three types of factors: knowledge, ownership and biometrics.

The knowledge factor is based on the user's knowledge, for example, a password. If the knowledge given matches the information previously stored in the system, the user is authorised. This method of authentication is preferred for its simplicity and user-friendliness. At the same time, however, it is breakable.

Ownership is based on a thing we own, for example, a card or a chip. These methods, however, have flaws that limit their use in certain types of facilities in terms of ability to share them with others (whether intentionally or unintentionally).

Biometric user authentication verifies a person's identity based on their characteristics. That includes both measurable physical and behavioural characteristics. Each person has a certain set of unique characteristics that no one else in the world has. Thus, advantage of biometric authentication is that an unbreakable one-to-one match can be made between an individual and a piece of information. [1], [2], [3]

3.1 Biometric Authentication

3.1.1 History

As early as BC, in empires such as ancient Egypt and Mesopotamia, our ancestors used primitive biometric methods to determine a person's identity. The Babylonians, for example, used the outline of a finger as a confirmation of trade contracts. People were often identified by scars, wounds, body shapes or even eye colour. Nevertheless, it was nothing compared to today's biometrics.

The origins of the system we know and use today began to take shape in the 19th century with a fingerprint being the first developed biometric method. However, evidence of the use of fingerprints as a means of identifying people dates back to 14th century China, where ceramic vessels with fingerprints as the signature of the author or cave paintings containing fingerprint-like structures have been found.

In 1882, Alphonse Bertillo began researching a method that was later named after him, the Bertillonage method, which became widely employed in criminalistics. It involved identifying a person by anthropometry while eleven body measurements were taken to identify the perpetrator. However, this method was soon discarded due to several false convictions. It was fully replaced by the fingerprint method, which proved to be more effective and reliable. This method is called dactyloscopy and has been implemented to identify and verify persons in criminalistics. This was also thanks to Francis Galton, who demonstrated the uniqueness and immutability of the papillary lines on the fingers.

In 1964, the first version of AFIS (Automated Fingerprint Identification System) was created in the USA, which at that time contained 810,000 different fingerprints. This system is still used in criminalistics today. In the European Union, for example, the EURODAC database, containing the fingerprint records of all applicants for asylum, subsidiary protection, or illegal migrants, is widely used.

However, the use of biometrics has also been transferred to the commercial sector, for example, in the 1970s, when hand geometry began to be used as an authentication tool for access to buildings or for checking attendance. The development of different types of biometric methods was then very rapid, and today it is the most reliable way of authenticating people. [1], [4]

3.1.2 Anatomical-physiological and behavioural biometrics

There are two types of characteristics that can be used for biometric authentication.

The first type is authentication using an anatomical-physiological biometric characteristic. These characteristics can be determined by using our senses and therefore clear, quantifiable differences can be defined between them. This is, for example, a person´s looks - eye colour or facial features. Then there is a person's voice, fingerprints or palm prints. Nonetheless, the most reliable of these factors is a person's DNA. The majority of anatomical-physiological biometric characteristics are innate, and it is very difficult or even impossible to falsify them. Although biometrics based on physiological elements is more accurate to determine and verify a person's identity than behavioural biometrics, it often requires an installation of expensive hardware and is more user-invasive. It also poses a greater risk to privacy in case of leakage of data such as facial images or fingerprints.

The second type is authentication, using behavioural biometric characteristics which involves recognising one´s style of writing and speed, behaviour, walking style and rhythm, or, for example, the dynamics with which a computer keyboard and mouse are used. In fact, all of the above characteristics are unique to each person. But since these are acquired, they may vary and alter over time. This means that an adult is unlikely to have the same gait as they did ten years ago. These characteristics depend on experiences and acquired patterns, but also, for example, on injuries or illnesses that have long-lasting effects.

On the one hand, behavioural methods can often use existing software and are, therefore, less costly. At the same time, the biometric data collected is less sensitive and less damaging in the event of a leak. On the other hand, this authentication is less deterministic than physiological biometric methods due to the variability over time as mentioned above. [5], [6]

3.1.3 False Acceptance and False Rejection Rate

Biometric authentication also has its limitations which must be considered when implementing in facility security. These limitations are called False Acceptance Rate (FAR) and False Rejection Rate (FRR). Both pose a security threat, although one higher than the other, and both can negatively affect the convenience of using that biometric method. However, neither of these vulnerabilities can be avoided entirely. The percentage of these errors subsequently evaluates the reliability of a biometric system compared to correct identifications. These two values are, therefore, suitable parameters to measure reliability and user acceptability of the biometric method. [7]

FAR is a situation in which a biometric system incorrectly evaluates and authenticates a user who is not the required person, which means, it allows someone who is not authorised to enter the system. FAR is stated as a percentage and is calculated as the number of false acceptances divided by the number of login attempts by unauthorised persons. From a facility security perspective, this highly undesirable phenomenon threatens protected assets. [7], [8]

On the contrary, FRR is when a biometric system evaluates an authorised user as a non-authorised one. More specifically, it denies access to a person who has all rights to enter the system based on an erroneous evaluation. Like the FAR, this value is determined as a percentage. It can be calculated as the number of false rejections divided by the number of login attempts by authorised persons. This is not so much a security issue as a phenomenon that negatively affects the user-friendliness of the biometric method due to the fact that the user has to repeat the authentication process. [7], [8]

Equal Error Rate (EER), sometimes referred to as Crossover Error Rate (CER), is a function of a biometric security system. It describes the value at which the false acceptance and false rejection rates are equal. An inverse proportionality applies here; the lower the equal error rate, the greater the accuracy of the

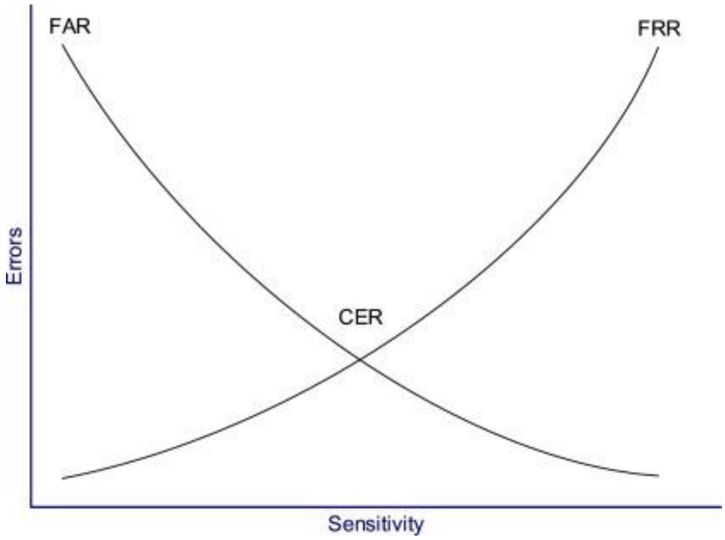


Figure 1: Dependency of FAR and FRR [10]

biometric method. However, EER is used sparingly as it is challenging to achieve the same error rate for both FAR and FRR. [9]

3.2 Selected methods of biometric authentication

A biometric system can perform two functions. One is authentication, and the other is verification. The techniques used for biometric authentication must be rigorous and efficient enough to use both functions simultaneously. There are multiple methods which may be used for biometric authentication. However, regardless of which method we choose, the main limitation will be its effectiveness in real life. The selected biometric methods are as follows:

3.2.1 Fingerprint Technology

The surface of each person's finger consists of a unique cluster of dermal ridges observed on a fingerprint which places this method among the anatomical-physiological ones. Fingerprint authentication is performed by an automated method in which a match between different fingerprints in the database is verified. Fingerprints are one of the most advanced biometric technologies and are taken as a legitimate evidence in courts worldwide. Fingerprints are, therefore, commonly used in forensic departments around the world for investigations, as aforementioned in the text.

It is a method that has been researched and used for the longest time and its recognition accuracy is therefore very high. However, it may be affected by the quality of the specimen recognised, especially if the finger is, for example, dirty, greasy, wet or injured. [11], [12]

3.2.2 Face Recognition Technology

Like fingerprints, each person has unique facial features which is what facial recognition technology is based on. It is an application capable of identifying and authenticating a person by their facial features. Currently, this type of authentication is widely used in smartphones. However, it may also be employed to recognise a person in a photo or video. This is demonstrated by the Chinese credit system operating on the principle that ubiquitous cameras with facial recognition are able to identify a person who committed an offense, track him down in a database, subsequently deduct credits from him, and thus reduce his citizen's index. [13]

It is also an anatomical-physiological method since facial features are innate and, as a rule, unchangeable. The rule's exceptions may include serious head injuries or extensive plastic surgery which may alter facial features. This may be one of the minor disadvantages of this method.

3.2.3 IRIS Technology

This technique is one of the most secure authentication and recognition techniques. The number of false rejections or acceptances is very low. The technology recognises the iris which is the coloured part of the eye surrounding the pupil. Each iris has a very complex pattern that is unique in each person, and simultaneously, it remains unchanged throughout life. This specific pattern is made up of pits, freckles, streaks and other formations found in the iris in addition to the colours. This method is usually performed in four steps: image capture, matching and image enhancement, image compression, and creation of a biometric template for comparison. The way it works is that the camera/sensor takes a photo of a person's eyes and maps the unique iris pattern to verify their identity. Nowadays, it is often used in multimodal biometrics; a biometric authentication combining two or more biometric methods. Iris is most commonly used with face recognition technology. [14]

3.2.4 Hand Geometry Technology

This method is based on the fact that each person's hand has a slightly different shape. At the same time, it does not change from a certain age. The measured characteristics are a hand's length, width, thickness and surface. The main principle of the technology is scanning the hand and then looking for individual points on the scan between which the distance is measured and on the basis of which a match with a user is then made. This method has several steps. In the first step, the system obtains stored data of each registered user. In the next step of authentication, the system captures an image of a hand and extracts a set of information needed to identify a user as genuine. This set of information is then compared to the one in the database and determines whether it matches or not.

In the commercial sphere, it was used as one of the first biometric methods at the beginning of the 20th century to check attendance and access to building. [15], [16]

3.2.5 Palmprint Technology

Palm print biometrics is gradually finding a vast use due to its non-invasiveness, easy data acquisition, and stable texture pattern on a palm. Palmprint recognition is related to fingerprint technology, as fingerprint recognition programs have many features in common. At the same time, the progress in the field of palmprint analysis research has also been made due to the experience and knowledge gained in fingerprint recognition research. This verification system focuses on the area of the hand from the wrist to the base of the fingers in which the skin covering the inner surface of the hand is subsequently analysed. Palm prints, like fingerprints, have many distinctive features used for accurate biometric authentication. In addition, they are more user-friendly than fingerprints, and the equipment used is less costly. [17], [18]

3.2.6 Hand vein Technology

As it is depicted in the paragraphs above, many physiological features used for biometric purposes can be obtained from the front and back view of the hand, i.e., fingerprint, hand geometry, palm print, palm vein or finger vein, for example. The dorsal hand vein (DHV) is another feature that this view can use and may be defined as a subcutaneous vascular pattern appearing on the back of the hand. Among other biometric techniques, this is a promising method due to the difficulty of a sample falsification, its uniqueness, immutability over time and versatility. At the same time, it is also rarely damaged. DHV can be detected in two ways, either by the shape of the vein or by its texture.

This method of biometrics has only become very popular in recent years. In any case, DVH has been researched for more than 42 years, within which various problems of using this technology have been solved. [19], [20]

3.2.7 Voice recognition technique

In addition to the methods above, voice recognition biometrics is growing in popularity. This is the first behavioural-based method mentioned in this paper.

The matching of samples works the same way as with a fingerprint or, for example, palm geometry, i.e. the original sample is uploaded to the system, and then a match is sought to it as part of the verification. There are two types of voice authentication: text-dependent recognition and text-independent recognition.

In text-dependent recognition, a predefined phrase that is recorded in the system is repeated, and a match is sought within the utterance of that phrase. On the contrary, in text-independent recognition, the system does not recognise any pre-recorded phrase but only the voice itself based on a predetermined sample. [21]

3.2.8 Signature verification technique

Biometrics signature verification is popular due to the fact that the data set can be easily obtained from the user. There are two forms of signature verification: offline and online.

The offline form involves manual pattern matching and it is not entirely provable, as it can be easily bypassed by learning how to do the signature. In the online form, verification is done by a device using artificial intelligence. It consists of a training and a test data set. The training one is used to train the device for a given signature, and the test file is already used to test whether the signature matches the sample or not. During testing, a comparison is made, based on which a match score, indicating whether the signature is genuine or fake, is determined. In addition to the signature itself, other patterns, such as speed of execution or pressure, are analysed during online verification. This makes it almost impossible to forge a signature. It is therefore obvious why online authentication is preferred over offline authentication. [22]

3.2.9 Keystroke Dynamics

Keystroke dynamics is a biometric method based on a style of typing. Although it may not be obvious at first sight, each person has a distinctive way of using and typing on the keyboard. This is used in user authentication. However, biometric authentication using keystroke dynamics is usually not used by itself but as the second phase of authentication, preceded by, for example, knowing the password. Thus, if an imposter were to obtain an access password, the system would still be able to reject it due to its mismatched keystroke dynamics. It is most often used in situations where a person's identity needs to be determined and verified with the greatest possible portability and certainty. The great advantage of this method is its low software requirements. At the same time, it allows continuous control of a user during the entire process of using the device. This method measures the individual keystrokes, i.e., the time each key is pressed and the intervals between keystrokes.

There are two ways in which the user is authenticated. Either it is authentication using predefined text or using free dynamic text. As the name suggests, with predefined text, a user has to copy the defined text, and then the match of his keystrokes is compared with the stored data. With free text, it does not matter what the user types. Matching is done on reference templates matching the claimed patterns.

3.2.10 Computer Mouse Dynamics

In comparison to other biometric methods, biometrics of computer mouse dynamics is still a field under study. It is often compared to the dynamics of keyboard strokes. However, unlike this method, its use does not require sensitive data input, for example, when entering a password or specific text. At the same time, it is more often used when browsing web pages, where a user usually does not type anything but clicks the mouse.

As with the keystroke dynamics, the computer mouse dynamics is, due to its higher error rate, used solely as one of the authentication phases. It is also commonly used together with keystroke dynamics in a single authentication system, which increases the accuracy of authentication. This authentication method is also gaining popularity due to its low cost, as the use of existing hardware is sufficient. Data collection requires only a keyboard and a computer mouse or touchpad, which is standard hardware for most users. At the same time, it is a very user-friendly method that does not inconvenience the user in any way. [23], [2]

4 METHODOLOGY

4.1 Structured interview

One of the data collection techniques should be used to find out the current status in health facilities and a structured interview in the form of a questionnaire was selected for the purposes of this paper.

The questionnaire consists of a set of questions that can be either open or closed. Its aim is to provide a structured set of data that can be easily extracted, analysed, evaluated and, if necessary, compared. In order to ensure that the data obtained in this way are reflecting reality, the survey needs to be carried out on a sufficiently representative sample.

A closed-answer questionnaire was used to obtain data on the current status. This type of questions was chosen because of the clarity of the answers and the possibility of exact determination of current situation. It was anonymous, and the only identifier of a given health facility was the number of its employees in order to determine the number of people involved. The questionnaire was given mainly to the management of the health facility. At the same time, only one employee per facility could fill it out to avoid data bias. The aim was to get at least 50 respondents, i.e. data from 50 facilities, to better understand the current situation. The questionnaire was sent to healthcare facilities in all parts of the Czech Republic, to small and large hospitals and to private and public ones. The outcome of the data collection should therefore be truly relevant. [24]

4.2 Multiple-criteria analysis

Multicriteria analysis is one of the ways in which the assessed values can be evaluated, considering multiple criteria. Both qualitative and quantitative criteria can be considered in this analysis. However, in order for the analysis to have a clear and measurable output, everything in the result needs to be converted to the same scale.

The procedure for creating a multicriteria analysis is as follows:

- Creating a set of evaluation criteria
- Weighing of the evaluation criteria
- Establishing sample values for the criteria weights
- Partial evaluation of individual criteria
- Ranking of variants or selecting the most suitable variant [25]

In this paper, multicriteria analysis was used to evaluate selected biometric methods. Ten methods were selected and assessed according to certain criteria to determine which one was generally the most suitable to use. The results of this analysis were then compared with the conditions in healthcare facilities to further evaluate which biometric methods are most suitable to use in healthcare facilities where specific needs may be encountered.

The analysis identified three main criteria for assessing usability. These were Accuracy, User-friendliness and Implementation. To determine these factors, each of them had its own sub-criteria where accurate data were entered and evaluated. A numerical scale of one to five was used to rate the data entered, with one being the best and five the worst. Therefore, all input values were converted to this scale according to the specified thresholds or specified characteristics. Each of the sub-criteria was given a number from this scale according to the value. These numbers were then averaged, producing a final number for one of the three criteria. After determination of numerical values of each of the three main criteria, an overall average was taken and the resulting value for every biometric method was determined.

To further evaluate the applicability of the biometric methods, another analysis was created, taking into account factors crucial for the hospital use. These factors were, in particular, the possibility of performing biometric verification even with protective equipment commonly worn in hospitals. Therefore, 4 criteria were established: the possibility to perform the verification with gloves, face mask, goggles and full body protective suit on. The last criterion identified was the possibility of implementing a biometric system without needing external hardware, which is often a key factor for hospital implementation.

It was possible to indicate only YES or NO. YES was evaluated as a positive answer (required answer). In order to be considered suitable for use in healthcare facilities, the method was supposed to score YES in all 5 criteria.

5 RESULTS

5.1 The questionnaire - Current state of HCF security

The questionnaire was used to determine the current state of computer security in hospitals. It was distributed in healthcare facilities across the Czech Republic. In total, responses were obtained from 80 respondents from various health facilities (Each HCF could only complete the questionnaire once). This structured way of collecting data from hospitals included 12 closed multiple-choice questions where only one could be ticked at a time. The questionnaire was divided into three main parts. The first one was to find out how large the hospital was in terms of the number of employees. The second part was to find out information regarding the general security of computers in HCF, so it consisted of stating objective facts. The last part addressed reflecting on the current situation, i.e. a subjective assessment of the current situation in the HCF.

More than 50% of all respondents were HCFs of smaller size with a maximum of 500 employees. 33% were hospitals with up to a maximum of 1,500 employees, and the remaining 11% were with more than 1,500 employees. Thus, data was collected from all possible HCFs, from small regional clinics to large university hospitals.

The second part of the questionnaire first asked about the type of security used by HCF to access the computer. Here, the majority response was clear. 71 of the respondents answered that they only use passwords. 8 facilities use ID cards to log in. One of the 80 facilities even uses biometric fingerprint authentication to access the computer. A very positive result is that none of the facilities leaves their computers unsecured. Number of employees with access to one computer - evaluation

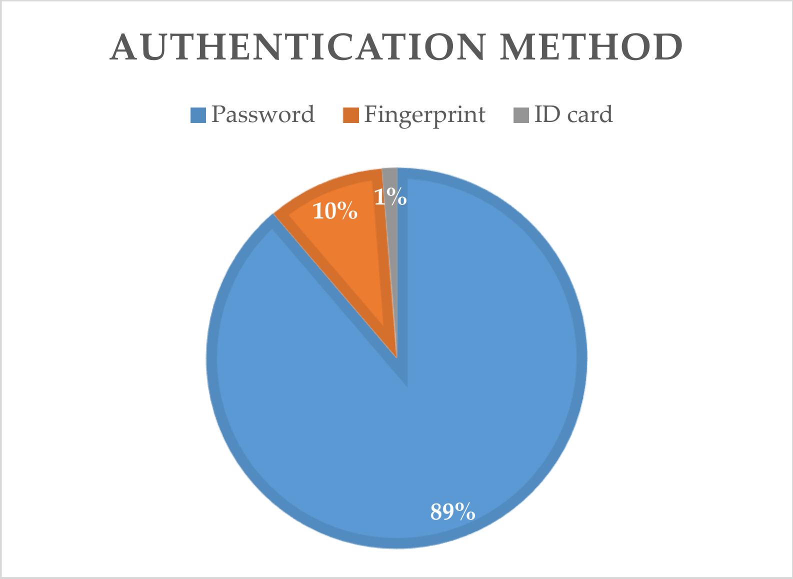


Figure 2: Authentication method - evaluation

This was followed by two interlinked questions. At first, everybody had to answer a question about whether each staff member had an individual computer to work with patient data on. The second question was directed only to the respondents, who answered NO. They had to determine how many employees have access to one computer on average. The results can be seen in the chart below.

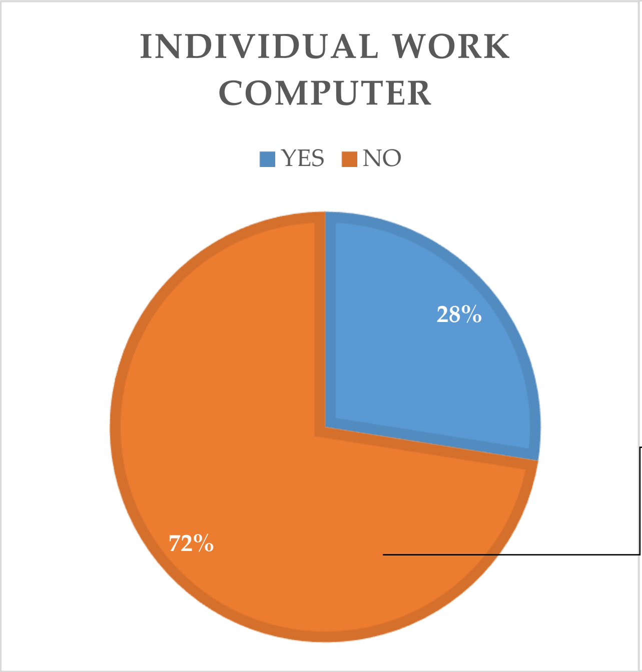


Figure 3: Individual work computer - evaluation

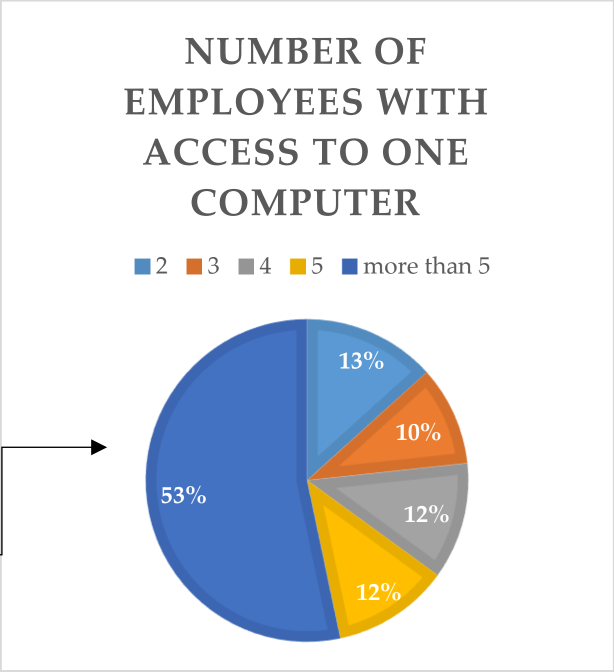


Figure 4: Number of employees with access to one computer - evaluation

The remaining four questions in this section clearly indicated high security level considering that in 69 from 80 facilities, a user has to re-verify their identity when working with sensitive patient data. Furthermore, the computers in the majority of healthcare facilities (over 97%) are located so that only staff and not the general public have access to them. At the same time, in 76 facilities, members of staff are trained, at least through written instructions, on how to secure the computer against outside intrusion. Even 77 facilities responded that they have a staff member who explicitly handles cybersecurity and computer security at their HCF.

The final part of the questionnaire was to assess the current state of security in HCF from the respondent's perspective. The section is called Reflecting on the current situation and included only four questions. The first two questions asked whether HCF had ever encountered a problem related to computer security.

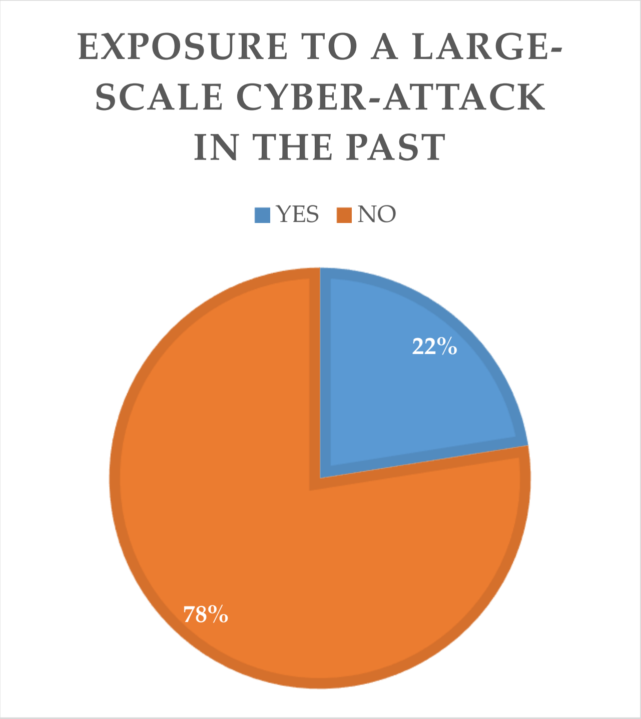


Figure 5: Exposure to cyber-attack - evaluation

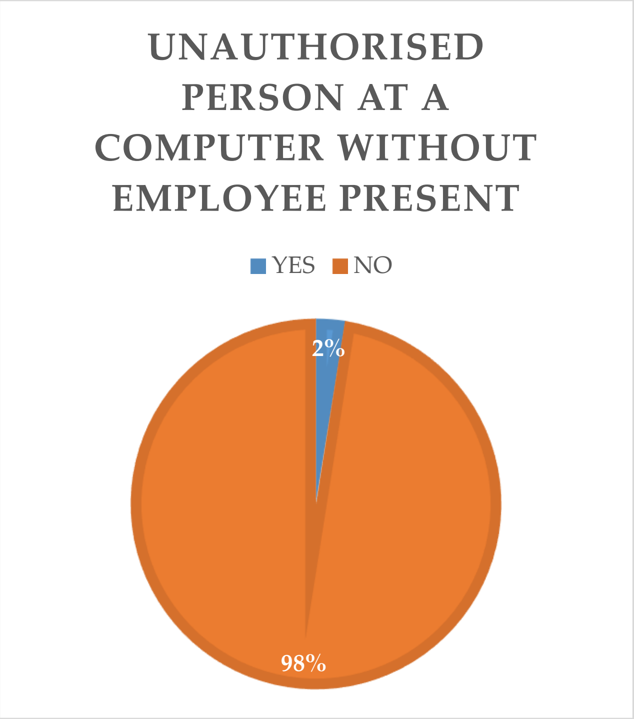


Figure 6: Unauthorised person at a computer - evaluation

As the results show, when it comes to internal computer security, as many as 22 in 80 devices have been targeted in the past. That is almost one-quarter of all participating HCFs. Concerning external security, the situation is much better because only 2 facilities encountered a situation where an unauthorised person was present or even used a working HCF computer without the presence of a staff member.

The remaining two questions focused on subjective attitudes towards computer security at the respondent's facility. The first question asked if the respondent rated the security of the computers in their HCF as sufficient. The second question then asked if the facility would consider improving computer security in the future if the solution was minimally costly and user-friendly. The results of the evaluation of the responses can be seen below.

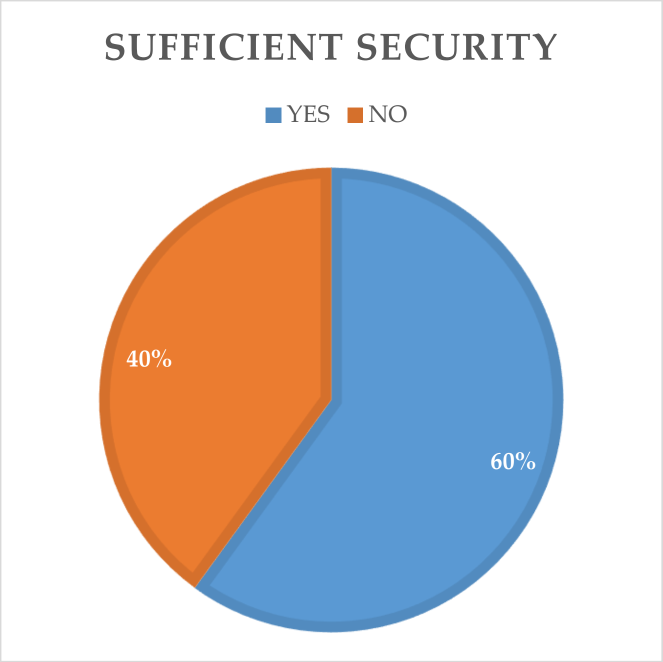


Figure 7: Sufficient security - evaluation

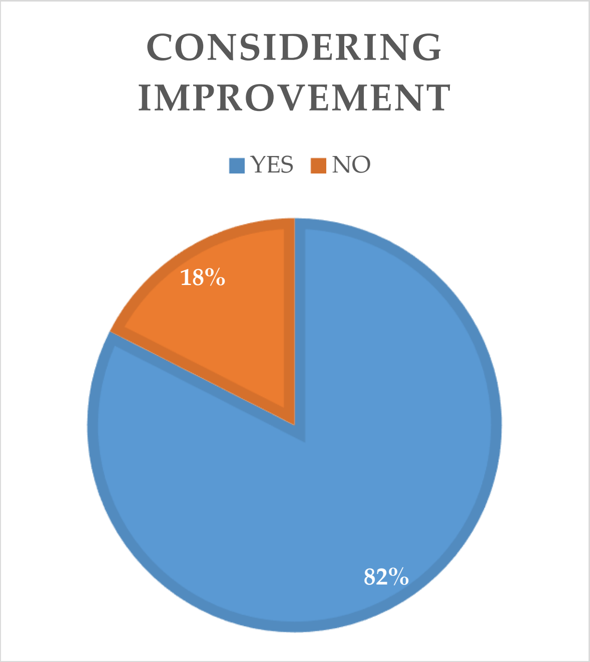


Figure 8: Considering improvement - evaluation

As the results show, respondents were not unanimous, especially with the first question. As many as 44 facilities responded that they rated the security of their

HCF as adequate. In contrast, 48 respondents considered current computer security to be sufficient. For the second question, 66 respondents answered in the affirmative, i.e., that they would be in favour of improvement. Only 14 were against it. This shows that although 44 facilities consider their security to be sufficient, 18 of them would still be in favour of its improving.

5.2 The analysis of biometric methods

The theoretical part presented ten different biometric methods based on anatomical-physical and behavioural characteristics. This first analysis was performed only to generally determine which of the presented biometric methods are the most effective, user-friendly and easiest to implement. It was not intended to compare how suitable the methods are regarding their use in a healthcare facility. For this purpose, a further analysis was compiled later in the thesis. In order to determine which method was best suitable for a healthcare setting, general data on reliability, user-friendliness, and implementation were first needed. The multicriteria analysis below contains all of this information. This type of analysis was chosen in order to compare and evaluate large number of criteria that are emphasised. The analysis was carried out using data and information obtained from expert open sources.

Three main criteria were identified in the analysis; Accuracy, User-Friendliness and Implementation. These were then evaluated according to their sub-criteria. For Accuracy, there were three sub-criteria: FAR, FRR and Permanence in time since all these three items contribute to the degree of reliability of a given biometric method. For example, if both FAR and FRR were in the thousands of per cent range, but Permanence in time was insufficient (i.e., it changes weekly), the biometric method could not be used to authenticate a person. In this category, the IRIS verification method won easily, showing extremely low FAR and FRR and almost absolute invariance over time.

The second main criterion was User-friendliness which means that the method should bother a user as little as possible and should not make their work more difficult. It was also assessed against three sub-criteria. One of them was the already mentioned FRR due to the fact that if a user is really the person who they claim to be but the system denies access due to a wrongful denial, it is annoying for the user as they have to repeat the whole process, in the worst-case scenario they may not get into the system at all. In addition, this category evaluated the difficulty of using a biometric method given with respect to the user, assessing how difficult it is to correctly attach or enter a sample, which is then used as the basis for authentication. At last, the amount of time from when a person walks up to the biometric system and starts the authentication process to when the authentication is evaluated was assessed. As in the first category, IRIS was identified as the best method, however, the only thing that brought it down a bit was the verification time, which was longer than, for example, in a fingerprint method.

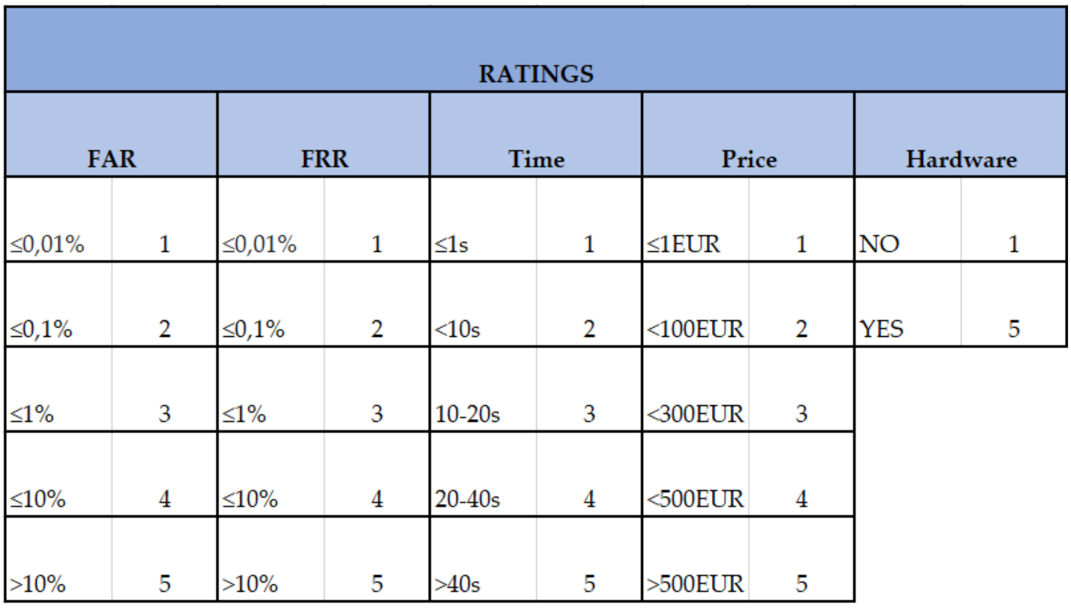
In the last main criterion, the analysis focused on the difficulty of system implementation. This was evaluated using two sub-criteria: price and the need for external hardware, i.e. equipment that must be purchased in addition to the system for biometric authentication. In this category, three methods were evaluated as the best, all three being behavioural biometric methods. These are Voice Recognition, Keystroke and Computer Mouse Dynamics. No external hardware is required for these three methods as an application can be used or programmed into the device where authentication takes place directly. This also makes them very inexpensive.

If we individually average the scores of each of the main criteria based on the sub-criteria and then take the resulting overall average, we get the analysis result, i.e. which biometric method is generally the most convenient. The results of the analysis can be found below: [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37]

METHODS	ACCURACY							USER-FRIENDLINESS							IMPLEMENTATION					TOTAL Average
	FAR		FRR		Permanence in time		Av	FRR		Difficulty		Time		Av	Price		External Hardware		Av	
Fingerprint	≤0,01%	1	≤1%	3	**Very Good** Some deseases (f.e. leprosy) can change papillaries	2	2	≤1%	3	**Good** Need to expose the finger (problem with gloves), dirt or injuries can influence the acceptance	3	≤1s	1	2,3	<100EUR	2	YES	5	3,5	**2,61**
Face Recognition	≤0,1%	2	≤10%	4	**Good** Can be infuenced by injury or covered face (f.e. mask)	3	3	≤10%	4	**Good** Need to expose whole face, sometimes hairs or injuries on the face can influence the acceptance	3	≤1s	1	2,7	>500EUR	5	NO	1	3	**2,89**
IRIS	≤0,01%	1	≤0,01%	1	**Excellent**	1	1	≤0,01%	1	**Excellent**	2	<10s	2	1,7	<500EUR	4	YES	5	4,5	**2,39**
Hand Geometry	≤1%	3	≤1%	3	**Good** Changes with age and injuries	3	3	≤1%	3	**Good** Need to expose part of the hand, frequent misapplication	3	<10s	2	2,7	<300EUR	3	YES	5	4	**3,22**
Palmprint	≤0,01%	1	≤1%	3	**Good** Changes with age and injuries	3	2,3	≤1%	3	**Very Good** Need to expose tha palm (f.e. problem when using gloves)	2	<10s	2	2,3	<500EUR	4	YES	5	4,5	**3,06**
Hand Vein	≤0,1%	2	≤0,1%	2	**Excellent**	1	1,7	≤0,1%	2	**Good** Need to expose part of the hand, frequent misapplication	3	<10s	2	2,3	>500EUR	5	YES	5	5	**3,00**
Voice Recognition	≤0,01%	1	≤10%	4	**Good** Can be influenced by sickness or ambient noise	3	2,7	≤10%	4	**Good** Speaking out loud, possible barriers (f.e. face mask)	3	10-20s	3	3,3	≤1EUR	1	NO	1	1	**2,33**
Signature	>10%	5	≤10%	4	**Sufficient** Influencable by the injury and the condition of the person (f.e. drunk)	4	4,3	≤10%	4	**Sufficient** Need to write something, possible multiple repetition	4	10-20s	3	3,7	<100EUR	2	NO	1	1,5	**3,17**
Keystroke	≤10%	4	≤10%	4	**Sufficient** Influencable by the injury and the condition of the person (f.e. drunk)	4	4	≤10%	4	**Very Good** Possible rejection - repetiton	2	20-40s	4	3,3	≤1EUR	1	NO	1	1	**2,78**
Computer Mouse	≤10%	4	≤10%	4	**Sufficient** Influencable by the injury and the condition of the person (f.e. drunk)	4	4	≤10%	4	**Very Good** Possible rejection - repetition	2	20-40s	4	3,3	≤1EUR	1	NO	1	1	**2,78**

Table 1: Analysis of biometric methods

Two sub-criteria are assessed verbally. These are Permanence in time and Difficulty as measurable values cannot compare these two categories. For those, no further explanation is required, the one given in the analysis is sufficient. To better understand the other criteria, a rating table has been created where the values and indicators of each biometric method are assigned numerical values from 1 to 5, with 1 being the best and 5 being the worst (as described in the Methodology chapter). The table can be found below:



RATINGS									
FAR		FRR		Time		Price		Hardware	
≤0,01%	1	≤0,01%	1	≤1s	1	≤1EUR	1	NO	1
≤0,1%	2	≤0,1%	2	<10s	2	<100EUR	2	YES	5
≤1%	3	≤1%	3	10-20s	3	<300EUR	3		
≤10%	4	≤10%	4	20-40s	4	<500EUR	4		
>10%	5	>10%	5	>40s	5	>500EUR	5		

Table 2: Ratings of sub-criteria

To evaluate the analysis, the Voice recognition method came out as the most reliable method in general, mainly due to its financial and hardware accessibility. IRIS biometrics was ranked as the second-best method, which, although it scored excellent in both the Accuracy and User-Friendliness categories, lost some points in the Implementation category, as it is both financially and technically challenging to implement. Next in the ranking was the Fingerprint method, followed by Keystroke and Computer Mouse Dynamics. Even though the latter two methods are relatively volatile over time and have higher FAR percentages than other methods, their User-friendliness and Implementation perform so well that they rank substantially high in this analysis.

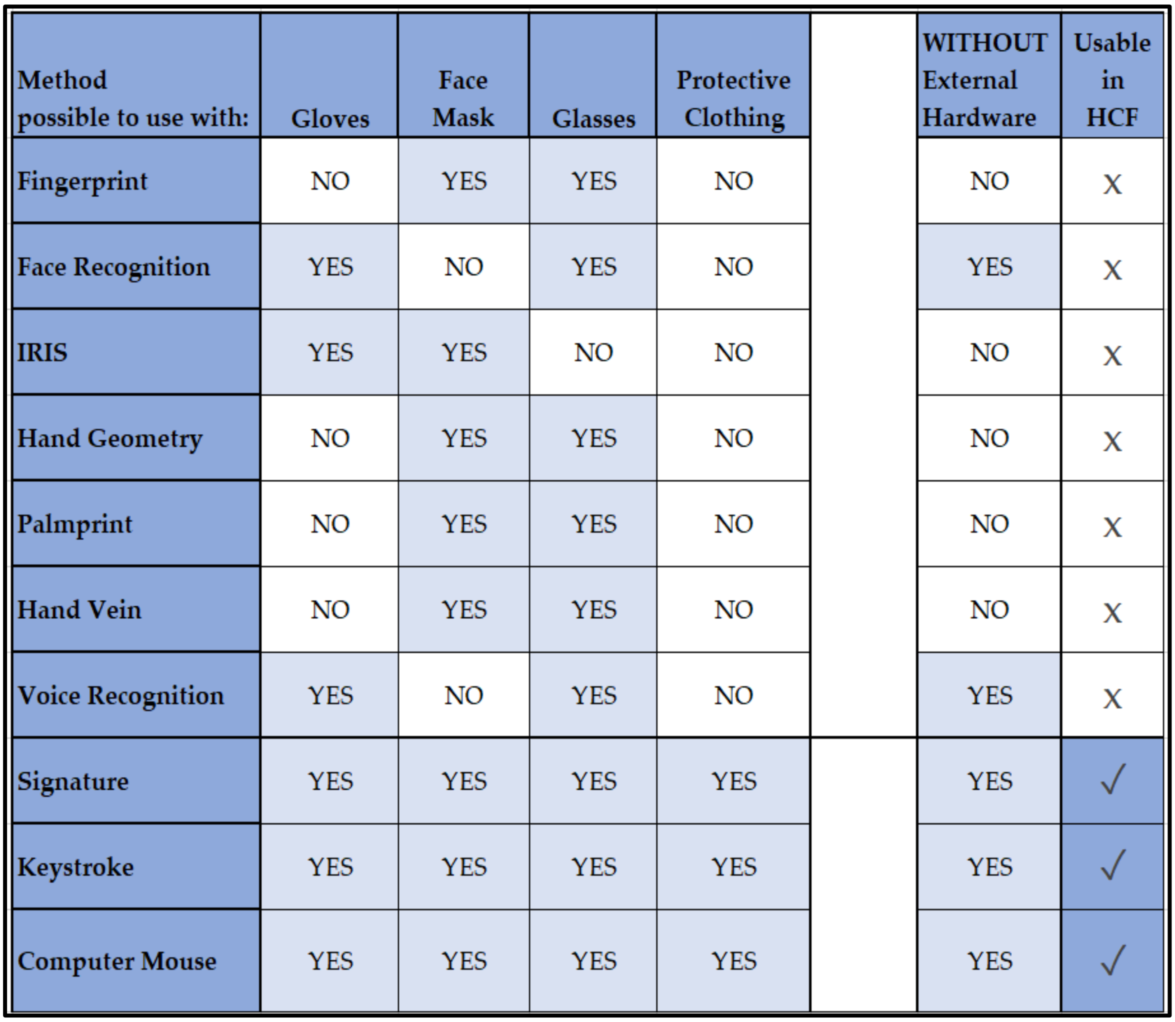
The biometric method using Palmprint was the worst evaluated in the analysis. This was mainly due to a combination of factors such as its acquisition cost, hardware requirements, or relative volatility over time due to potential injuries and illnesses. Even so, its rating is not trivial, and it certainly cannot be dismissed as one of the suitable biometric methods.

5.3 The applicability of biometric methods in HCF

Although a conducted analysis clearly defined which biometric methods are more appropriate than others, specific characteristics of individual biometric methods may prevent them from using in HCF. It is common to wear protective equipment that can make it difficult or even impossible to use the abovementioned methods. Another factor that makes the biometric method unsuitable for use in HCF is the need for external hardware due to its cost and technical complexity.

Therefore, the evaluation below contains a table indicating whether each of the biometric methods meets the basic specified requirements; i.e., whether the method could be used when an employee is wearing goggles, face mask, glasses or a full-body protective gown (used, for example, during a covid pandemic). The last box asked whether the method could be used without installing external hardware. The method was rated as suitable for HCF only if the answer to all five questions above was YES.

The data for this analysis was again obtained from open sources and using information already used in the first analysis. The evaluation can be seen below:



Method possible to use with:	Gloves	Face Mask	Glasses	Protective Clothing	WITHOUT External Hardware	Usable in HCF
Fingerprint	NO	YES	YES	NO	NO	X
Face Recognition	YES	NO	YES	NO	YES	X
IRIS	YES	YES	NO	NO	NO	X
Hand Geometry	NO	YES	YES	NO	NO	X
Palmprint	NO	YES	YES	NO	NO	X
Hand Vein	NO	YES	YES	NO	NO	X
Voice Recognition	YES	NO	YES	NO	YES	X
Signature	YES	YES	YES	YES	YES	✓
Keystroke	YES	YES	YES	YES	YES	✓
Computer Mouse	YES	YES	YES	YES	YES	✓

Table 3: The analysis of applicability of biometric methods in HCF

As the results show, although methods such as voice recognition, IRIS or Fingerprint prevailed in the overall analysis of biometric methods, their applicability in healthcare settings is not suitable. On the other hand, behavioural biometric methods such as Keystroke Dynamics, Computer Mouse Dynamics or Signature Verification, which ranked in the middle in the overall analysis, meet all the basic requirements to be used in HCFs. This is mainly due to their low hardware requirements and the possibility of using them without exposing any part of the body.

6 DISCUSSION

6.1 Evaluation of the current situation

A questionnaire survey conducted as part of this bachelor's thesis and participated by 80 medical institutions from all over the Czech Republic and of various sizes shows that the password is the most commonly used method for securing computers in hospitals and other medical institutions. This can bring along a number of complications, namely that in almost three-quarters of the surveyed healthcare facilities, each employee does not have his or her own individual work computer but shares it with several other employees. The most common answer to this question was that more than 5 employees have access to one computer (53% of respondents). People often do not have the habit of logging out of their profiles after using the computer, or even their passwords are hanging on the edge of the monitor, as stated in the interview by Petr Samek, an expert in cybersecurity and data protection in healthcare. [38]

On a more positive note, many HCFs already have a system where the user must re-authenticate to gain access to sensitive patient data. However, this loses its significance if the login process is the same as for the computer access itself, i.e., the password remains the same. When the password is compromised, there is nothing easier than to use it twice, both to access the computer and to gain access to patient data. This risk should be addressed by ensuring that members of staff are adequately trained on how to secure their account properly and, for example, create and use passwords. This assertion is supported by the survey data, where 95% of HCFs have staff trained on this topic. However, it is one thing to train employees, where the gist of the problem is communicated to them either through written instructions or through training, and it is another thing for employees to actually follow these instructions. This assertion is again confirmed in the interview by Mr Samek, who points to people's carelessness in creating and using passwords. [38]

In terms of security, we can also positively evaluate the result of the questionnaire, where almost all facilities not only have computers in places accessible only to staff, so that no one unauthorised should get to them, but also have an IT employee in charge of cybersecurity. Here, the answers in the questionnaire could be slightly questioned, given that many ordinary people do not distinguish between an ordinary IT worker, who is mainly responsible for the functioning of servers and medical IT, and a person who deals directly with cybersecurity, which was the subject of the question in the questionnaire. However, this is where the problem arises, especially for smaller HCFs that can barely afford to fund one IT person to be in charge of all the computers in the facility. This person must have particular knowledge of medical IT. Often, however, he or she does not have sufficient cybersecurity knowledge. Then having a dedicated staff member just for cybersecurity is usually budget prohibitive. This conclusion can also be supported by an article from Zdravotnický deník, which focuses on the problem of the shortage of IT workers in healthcare. [39]

Looking at the overview of the current situation resulting from the survey results, it is possible to notice that less than one-quarter of hospitals have been exposed to a significant cyberattack in the past. However, hospitals struggle on a daily basis with attempted cyberattacks which are usually fortunately stopped by a capable firewall, antivirus or the intervention of an IT staff member. This is confirmed not only by the aforementioned article from Zdravotnický deník [39], but also by the cyber security manager of one of the Brno hospitals, Mr. Třešňák. He says that these are mostly phishing attack attempts targeted mainly at employees, and in the vast majority of cases, the threat is successfully extinguished. [40]

According to the questionnaires, the intrusion of an unauthorized person into a work computer could be rated as negligible, as only 1 out of 80 facilities surveyed experienced this. However, as Mr. Samek suggests in the interview [38], it is relatively easy today to get access to a hospital computer and cause significant damage. According to him, one can "*Take a white coat, an endoscope, and walk into any large hospital where the doctors do not know each other personally. I guarantee that within half an hour, you will get a computer with a willing nurse who will log on to it so you can look at the system because you desperately need data on such and such a patient. Unless the password is written directly on the monitor, as is the good practice. Then you can put a program directly on the internal network that will collect the data and allow access to the system.*" [38] This claim would be supported by the above-mentioned careless computer security and password sharing by medical staff.

Looking at the last two questions in the questionnaire which focused on subjective perceptions of security, it can be deduced that over half of HCFs perceive their level of security as adequate. Despite this, the vast majority (over 82 per cent) of respondents would be in favour of further improving computer security unless the solution was expensive and user intensive which is consistent with the current financial situation in the healthcare sector as well as the frequent reluctance of staff to perform any extra time-consuming tasks.

To summarise the current state of computer security in HCFs, underfunding of HCFs is a major problem. As a result, there is not enough money to pay for special technologies to improve security or to hire additional IT staff to specifically focus on IT security. Although the situation is slowly improving, even with the coming digitisation of healthcare and the need to protect the data, the healthcare sector still needs to catch up. Mr. Třešňák provided an example of the banking sector in which 9 % of all employees are employed in IT. Unfortunately, it is only 1% in the healthcare sector, even though the data to be protected is just as important, if not more important. [40]

At the same time, it is possible to observe a phenomenon where computers are well-secured and ready to resist cyber-attacks. However, the weakness is the user who is able to cause unwanted intrusions into the system by their careless behaviour. This may be not only an internal intrusion, through certain viruses or phishing emails, where a user enters a password where it is not supposed to be, but also the possibility of infiltration by an unauthorised person who, thanks to the trust of employees who do not log out of their profiles or leave passwords publicly accessible, infiltrates in the computer and gains access to sensitive data, as confirmed by Mr Samek in his statement.[38] In this issue, I see the use of passwords for security as a significant problem, with users mostly unable or unwilling to create them properly and to use and store them securely. Despite these problems, the Czech healthcare system is not doing badly regarding computer security, as attacks of a larger scale are usually prevented, and it is rare for an unauthorised person to access work computers and unauthorised places. At the same time, there is an effort and interest in improving security in the future, which can only be appreciated. However, it is necessary to be constantly prepared for possible attacks, and the fact that their success rate is not frequent does not mean that efforts should not be made to prevent them.

6.2 Use of biometric methods

As the summary of the current situation has shown, it is necessary to come up with a new user authentication system because the use of passwords alone becomes easily exploitable due to the poor use of their owners. IDs or smart cards, where authentication is based on an item we own, are offered as another authentication option. This method certainly has its pros and cons. However, it was not proposed as a new solution because of the need to carry it around and the possibility of it being easily stolen or forgotten and used to access data by an unauthorised person. The solution preferred to focus on the use of biometric authentication methods and their applicability.

The result of the multicriteria analysis of biometric methods showed that when combining the three criteria (Accuracy, User-friendliness and Implementation), the best method is generally Voice recognition, which is relatively accurate and relatively stable over time, yet very easy to implement due to its meagre cost (often just an application or program to use it). However, regarding user-friendliness, it loses some points in this category, especially in the healthcare environment. In order to make the best use of it, one has to speak up, which not only may be uncomfortable for some people but also may be distorted by ambient sounds, illness or, for example the face mask, which is very often used, especially in hospitals. This method was therefore rejected. The same problems arose with the IRIS, one of the most reliable biometric methods. For example, the American biometric company Aware describes it as the most accurate modality of biometric identification. [41] However, we again encounter the problem of protective equipment and, this time, also glasses which can distort the result and, therefore, must be removed for verification, which is no longer considered user-friendly. Nevertheless, a bigger problem of this method is its financial complexity and the necessity of acquiring external hardware for accurate iris scanning. Since there are sometimes hundreds of computers in larger hospitals that would need this device, it can be excluded from a possible proposal. Slowly, systems that would not need external hardware for iris scanning in the future are being developed. However, they still currently need to be developed to the point where they can be relied on and they can also be affected by factors such as distance or direct sunlight. [42]

The rejection also came from the fingerprint method, the reason of which was simple; it was necessary to expose hands. Yet, in healthcare institutions, gloves are worn more often than anywhere else, and the need to remove them is undoubtedly not considered as user-friendly. This is why this method was not taken into account, even though it is generally considered to be the most well-known biometric method and probably also the most widely used, according to NEC, a biometric systems company. [42] For the same reason, all other methods working with a human hand, i.e., Palmprint, Hand Vein and Hand Geometry methods, were rejected.

This leaves us with 3 of the analysed methods that could be considered for use. All 3 methods are behavioural biometrics. First it is Signature verifications. Although it met all the criteria defined in the usability analysis in HCFs, this method was not recommended as the need to perform the signation every time to log in to the system or to verify the identity may be considered very user-unfriendly. Simultaneously, the high error rate of the system compared to other biometric methods should also be taken into account, which could force a user to repeat the login procedure several times or, even worse, could allow an unauthorised person to enter the system.

Thus, the exclusion method led us to the two biometric methods proposed in this paper as the most suitable for their use in HCFs. These are Keystroke Dynamics and Computer Mouse Dynamics. The two methods are evaluated identically in the two analyses performed. Although their accuracy is not as good as that of anatomical-physiological biometrics, they have several undeniable advantages. One of them is the simplicity of their implementation in the device system. No external hardware is required, and a simple computer application recording keystrokes and the use of a computer mouse are sufficient. Another advantage is that this authentication can be done with all possible medical protective equipment on. At the same time, authentication can be done directly while the computer is being used, so there is no need to enter a password, attach a chip or say something out loud, for example. It is also possible to set the program to authenticate the user continuously. Thus, it should be possible to identify from the log who, for example, wrote a note or an email or who performed a particular action on the computer just by the recorded dynamics of typing on the keyboard and using the computer mouse. This system could also be used, for example, by running the application in the background. When it detects a deviation from the stored sample, it could request the user to perform a primary identification. [43] Although both keystroke dynamics and computer mouse dynamics can be used separately, in this case it would be recommended to use them simultaneously. That is, the software will capture and compare not only the keyboard typing pattern but also the dynamics of a mouse use. This is mainly because of their higher potential for error compared to anatomical-physiological methods. This would increase their accuracy even further. However, one of the possible problems was pointed out by Ms Talandová in her bachelor thesis from 2010. She states that there is a possibility of a problem when a not so experienced user registers and, over time, learns to type with all ten fingers. Then the registration needs to be repeated.[43] The same applies, for example, after sustaining injuries to the upper limbs.

Another thing that needs to be taken into account, but which could be perceived as an advantage of this method, is the fact that the user will never have 100% the same sample as the one stored in the database for a simple reason: one cannot repeat the dynamics of keyboard strokes and computer mouse movements identically. Thus, if the authentication matches the stored pattern

100%, it is easy to deduce that it is an artificial intelligence or robot performing the task and not a human. Therefore, the system should not accept the user if their sample matches 100%. This could prevent attempts to circumvent this security method using algorithms or AI.

The results of the general analysis of biometric methods carried out in Chapter 5.2 showed that the order of behavioural and anatomical-physiological biometric methods is intertwined. One type of biometrics is not better than the other in the final evaluation. Each has its own strengths and weaknesses and their use in individual institutions depends strictly on the requirements of its users.

This brings us to the great advantage of behavioural biometrics over anatomical-physiological biometrics in a sector with an extensive collection of biometric data, such as healthcare. When talking about hospital security, Mr Třešňák very well pointed out that the use of biometrics, in general, carries one considerable risk; the possibility of leaking or breaking the database storing biometric samples. This could be described as irreparable if data with anatomical-physiological biometric samples leaked. As noted in the paper above, these patterns are often very little or absolutely invariant over time. Therefore, a data leak would render the data useless and discredit them in the future. This is probably the biggest risk of using biometric methods in general. [40] However, this irreversible situation does not apply to behavioural biometrics. Indeed, behavioural samples change with age, illness and injury. These are not usually rapid changes, but in any case, if the data leaked, the sample would only become unusable for a certain period of time but could be recovered in the future. As can be seen, none of the biometric methods is 100% ideal. However, their use has its undeniable advantages and could help to raise the level of security in HCFs. This issue will be discussed more in the proposed solution.

6.3 Solution proposal and future outlook

Nowadays, there is a tendency digitalise the Czech healthcare system which means to convert all patient data from paper to online environment. This issue was widely discussed with Mr Třešňák, the cyber security manager of a large hospital in Brno who managed to describe current challenges that need to be considered when designing a solution.

One of the biggest problems that small healthcare facilities in particular would struggle with in case of full digitisation of healthcare is the fact that the management, backup and archiving this data is to be taken care of by the facility itself. However, this can be a big problem for HCFs that have, for example, only one IT staff member and no longer have the capacity to manage this agenda properly and securely. Therefore, the most sensitive data about a person, such as their health status or birth number, for example, would be collected in places that cannot be perceived as secure for such important data. [40]

Therefore, it would be advisable for the state to take over the agenda of collecting and archiving the data with dedicated, professionally qualified staff and secure storage facilities. It is also necessary to address the fact that if the data is only stored in the online form, there is a severe problem if it is deleted or stolen. In case the data cannot be recovered in any way, HCFs will lose access to patients' medical histories, lists of medications they take or complications they have experienced, which could trigger another wave of complications directly affecting and threatening patients' health. Mr Třešňák was also in agreement with this point identifying it as one of the most significant potential threats. [40] However, this is a problem the state must address in the future. It will not be solved by healthcare facilities alone. They can, however, concentrate on making the data they handle as secure as possible so that irresponsible behaviour and attitude do not create an unwanted situation that could have easily been prevented.

At this point, the thesis results in the proposal on how to make computer security and user authentication as efficient as possible but at the same time as cost-effective as possible, given the long-term underfunding of hospitals, and also as user-friendly as possible, since the facilities are already understaffed and have to manage many tasks, so there is no point in adding more.

As mentioned in the work, there are different authentication methods based either on things we know - passwords, things we have - tokens or things we are - biometrics. Each of these methods has its limitations but also its strengths. The most reliable of these methods seems to be the use of biometrics, as it is almost impossible to steal or forge it and at the same time, the person is always "wearing" it. In this respect, the opinion of this paper and that of Mr Třešňák diverge. He is more sceptical about the use of biometrics, especially for the reasons already mentioned above; i.e., the possibility of theft of biometric samples. However, this problem could be addressed by designing a solution using a combination of keystroke biometrics and computer mouse dynamics since their combination would increase their accuracy. At the same time, if biometric samples are leaked, they are not compromising their owner and are recoverable within a certain period of time. Simultaneously, this method is able to authenticate the user during any activity on the computer; that is, they constantly check if the person using the computer is who they say they are.

Even so, this method also has some limitations, such as the inability to deviate more from the pattern caused, for example, by a hand injury, where the keystroke pattern is likely to be different than when the hand is healthy. The method is still not perfect enough to take these possible deviations from the original state into account and incorporate them. However, this limitation could be covered by incorporating another authentication method, for example, using a password. Thus, two authentication methods would be linked, which themselves have certain limitations, but in synergy can rapidly increase efficiency and security while covering each other's weaknesses.

The system would then look like this: a user would have to enter a password to enter the computer. When entering the password, it would be verified whether the keystroke dynamics and mouse dynamics match the given sample in the database. This would prevent the computer from being misused by anyone who could enter the device and know the password or see it written on the edge of the monitor, for example. Then, as the user is working on the computer, it would run in the background to check whether the pattern matched the given keyboard and a mouse usage. At this stage, the sensitivity would be set lower, as the sample may vary more when typing longer texts. This would allow the employee to leave the computer for a while and not have to log off as the system would recognise if someone unauthorised started using the computer. In this case, the password window would reappear. If, for example, nurses and doctors take turns at the computer, keystroke and mouse dynamics biometric samples of all of them would be recorded in the system. This would then work in a way that although the logged-in user, i.e. a doctor, would leave and a nurse would come in to look up something in the database, the computer would not immediately deny her access but would instead compare her sample with those stored in the database. If it traced her as an authorised person, she would not have to enter any password, the system would switch to the new user in the background and adjust the permissions accordingly. If, by any chance, a match was not found, the system would just pop up a login window where the nurse would enter her password (again, biometric verification would be running in the background) and would get the access to the computer with no problem.

This designated solution meets two main requirements. Firstly, it is user-friendly. It does not require any excessive tasks from its users. However, it does require a bit more user participation than password-only security. Anyway, if we look at the ratio of user-friendliness vs reliability and security, this proposal seems very favourable. Another criterion was affordability. The method does not require external hardware, making it easier to implement. At the same time, the application can be left running in the background and does not require any specific requirements. Fleksy, a virtual keyboard app company itself, states that a big advantage of keystroke biometrics over other biometric methods is its affordability. [44] Speaking of the Fleksy app, it would be one of the possible adepts to use to create a suitable app tailored to healthcare facilities. This company is particularly interested in virtual keyboards and offers options such as biometric authentication explicitly produced for the organisation. [44]

As an example of what the integration of this new security method could look like, I chose a small hospital with about 500 employees which so far only uses password authentication. Ideally, the hospital's IT staff would have the knowledge and experience to design and develop the application themselves or with the help of an external company. However, it may also happen that the IT employee does not have sufficient experience and the entire implementation will therefore have to be outsourced. However, the result would be an application of the principles described in the paragraph above. How would its introduction into the hospital system work? First, there would be a period when the application would be installed in all computers. Then a gradual collection of employee samples would begin to be stored in the database. This phase would require the patience and understanding of the staff as it can be slightly user-intrusive. Once the samples were uploaded, a test run of this application could be initiated to identify and correct various vulnerabilities. Once the final version is reliable and sufficient, it will be officially implemented as a security and verification method.

The implementation may not meet with the approval of all employees as not all people welcome new changes and innovations. For this reason, staff would need to be informed of the reasons to move to better security and to become familiar with the importance of the security of sensitive data.

As for the future outlook and possible extension of this method, one could consider its possible use for blocking malware and other viruses. As mentioned several times in the thesis, the weakest link in the whole security chain is the end user. There will always be someone who will not follow the rules or open attachments from unreliable sources, either knowingly or unknowingly. It would therefore be great if this application could not only detect the presence of a virus in a computer but also, based on the fact that the virus was performing certain activities that did not match the user's biometric pattern, the system would be able to deny access and thus protect the system. In this subject, it is worth mentioning the observation of Mr. Třešňák, who said that in his opinion, the future of computer security belongs to artificial intelligence. Today, many malicious programmes already operate on the basis of artificial intelligence. The best way to defend against this is to use the same weapon since the capabilities of human thinking today no longer reach AI's scale and reaction speed. [40] However, this is still rather a long-term outlook for the future, especially in the healthcare sector, where trends always find application with a certain delay.

7 CONCLUSION

The bachelor thesis determined the current state of HCF security through a questionnaire survey in order to find out whether the state is sufficient or not. Furthermore, a conducted multicriteria analysis evaluated which biometric method is generally the most suitable. Subsequently, the use of each biometric method in the healthcare sector was assessed in order to determine which method is the most suitable concerning its financial requirements but also the level of difficulty of its use for the staff and the possibility to use it, for example, while wearing protective equipment. Eventually, a solution for the use of a biometric system to secure computers in HCFs and its possible implementation was proposed and thus all the set objectives of the thesis have been met. The first part of the thesis focused mainly on general information on biometric methods and a brief description of 10 selected methods. The second, practical part, was devoted to achieving the predetermined objectives of the work through questionnaire survey, multi-criteria analysis and search of open sources to propose appropriate security solutions.

Given the current state of computer security in HCFs and the planned digitalization of healthcare, the topic of securing sensitive data must be taken seriously and certain measures should be taken to improve the current situation. Therefore, a solution using a combination of biometric authentication method along with the use of password authentication has been proposed in order to provide greater data protection and to prevent unauthorised persons from accessing the data. In the future, we can count on even greater involvement of biometrics and artificial intelligence in the security process, not only in healthcare. HCFs therefore need to be able to keep up and withstand new threats.

8 LIST OF ABBREVIATIONS USED

HCF	Healthcare Facilities
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate
CER	Crossover Error Rate
AI	Artificial Intelligence

9 LIST OF LITERATURE USED

[1] RANJAN, Rahul, Debnath BHATTACHARYYA, Farkhod ALISHEROV a Choi MINKYU, 2009. Biometric Authentication: A Review. In: International Journal of u- and e- Service Science and Technology. ISSN 2005-4246.

[2] ROY, Soumen, Jitesh PRADHAN, Abhinav KUMAR, Dibya Ranjan Das ADHIKARY, Utpal ROY, Devadatta SINHA a Rajat Kumar PAL, 2022. A Systematic Literature Review on Latest Keystroke Dynamics Based Models. IEEE Access. 10, 92192-92236. ISSN 2169-3536. Available from: doi:10.1109/ACCESS.2022.4397756.

[3] MEMON, Nasir, Jitesh PRADHAN, Abhinav KUMAR, Dibya Ranjan Das ADHIKARY, Utpal ROY, Devadatta SINHA a Rajat Kumar PAL, 2017. How Biometric Authentication Poses New Challenges to Our Security and Privacy [In the Spotlight]. IEEE Signal Processing Magazine. 34(4), 196-194. ISSN 1053-5888. Available from: doi:10.1109/MSP.2017.3897179.

[4] LÁZNIČEK, Matěj, 2019. Biometrické identifikační systémy. Brno. Bachelor's thesis. Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS. Thesis supervisor Doc. RNDr. Jaroslav Tureček, Ph.D.

[5] NELSON, CPP, Joseph, 2013. Biometrics Characteristics. Effective Physical Security. Elsevier, 2013, 255-256. ISBN 9780124158924. Available from: doi:10.1016/B978-0-12-415892-4.00012-2

[6] CHONG, Penny, Yuval ELOVICI a Alexander BINDER, 2020. User Authentication Based on Mouse Dynamics Using Deep Neural Networks: A Comprehensive Study. IEEE Transactions on Information Forensics and Security. Elsevier, 2013, 15, 1086-1101. ISBN 9780124158924. ISSN 1556-6013. Available from: doi:10.1109/TIFS.2019.4142441

[7] AWAD, Ali Ismail a Aboul Ella HASSANIEN, 2014. Impact of Some Biometric Modalities on Forensic Science. Computational Intelligence in

Digital Forensics: Forensic Investigation and Applications. Cham: Springer International Publishing, 2014, 47-62. Studies in Computational Intelligence. ISBN 978-3-439-05884-9. Available from: doi:10.1007/978-3-439-05885-6_3

[8] Autentizační metody založené na biometrických informacích [online], 2010. [cit. 2023-03-21]. ISSN 1214-9675. Available from: http://access.fel.cvut.cz/view.php?cisloclanku=2010110002

[9] EER – Equal Error Rate. Webopedia [online]. [cit. 2023-03-21]. Available from: https://www.webopedia.com/definitions/equal-error-rate/

[10] CONRAD, Eric, Seth MISENAR a Joshua FELDMAN. Domain 5. 2017, 117-134. Available from: doi:10.1016/B978-0-12-811248-9.00005-X

[11] JAIN, Anil, Sharath PANKANTI a Alexander BINDER, 2009. Fingerprint Recognition: A Comprehensive Study. The Essential Guide to Image Processing. Elsevier, 2009, 15, 649-676. ISBN 9780123744579. ISSN 1556-6013. Available from: doi:10.1016/B978-0-12-374457-9.00023-8

[12] YANG, Wencheng, Song WANG, Jiankun HU, Guanglou ZHENG a Craig VALLI, 2019. Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry. Elsevier, 2009, 11(2), 649-676. ISBN 9780123744579. ISSN 2073-8994. Available from: doi:10.3390/sym11020141

[13] VALENTOVÁ, Anna. Sociální kreditní systém v Číně. Security Outlines [online]. 39.11.2021 [cit. 2023-03-14]. Available from: https://www.securityoutlines.cz/socialni-kreditni-system-v-cine/

[14] H. HAMD, Muthana a Marwa Y. MOHAMMED, 2019. Multimodal Biometric System based Face-Iris Feature Level Fusion. International Journal of Modern Education and Computer Science. 11(5), 1-9. ISSN 20750161. Available from: doi:10.5815/ijmecs.2019.05.01

[15] SANCHEZ-REILLO, Raul a Marwa Y. MOHAMMED, 2015. Hand Geometry. Encyclopedia of Biometrics. Boston, MA: Springer US, 2015-7-3, 11(5), 849-854. ISBN 978-1-4899-7487-7. ISSN 20750161. Available from: doi:10.1007/978-1-4899-7488-4_251

[16] PRIHODOVA, Katerina a Miloslav HUB, 2019. Biometric Privacy through Hand Geometry- A Survey. 2019 International Conference on Information and Digital Technologies (IDT). Boston, MA: IEEE, 2019, 11(5), 395-401. ISBN 978-1-7401-1401-9. ISSN 20750161. Available from: doi:10.1109/DT.2019.8813660

[17] GENOVESE, Angelo, Vincenzo PIURI a Fabio SCOTTI, 2014. Palmprint Biometrics. Touchless Palmprint Recognition Systems. Cham: Springer International Publishing, 2014-8-22, 11(5), 49-109. Advances in Information Security. ISBN 978-3-439-10364-8. ISSN 20750161. Available from: doi:10.1007/978-3-439-10365-5_4

[18] CHAI, Tingting, Shitala PRASAD, Jianen YAN a Zhaoxin ZHANG, 2014. Contactless palmprint biometrics using DeepNet with dedicated assistant layers. The Visual Computer. Cham: Springer International Publishing, 2014-8-22, 11(5), 49-109. Advances in Information Security. ISBN 978-3-439-10364-8. ISSN 0178-3989. Available from: doi:10.1007/s00371-022-02571-6

[19] RAGHAVENDRA, R., Shitala PRASAD, Jianen YAN a Zhaoxin ZHANG, 2012. Sparse Representation for Accurate Person Recognition Using Hand Vein Biometrics. 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Cham: IEEE, 2012, 11(5), 41-44. Advances in Information Security. ISBN 978-1-4673-1741-2. ISSN 0178-3989. Available from: doi:10.1109/IIH-MSP.2012.16

[20] JIA, Wei, Wei XIA, Bob ZHANG, Yang ZHAO, Lunke FEI, Wenxiong KANG, Di HUANG a Guodong GUO, 2021. A survey on dorsal hand vein

biometrics. Pattern Recognition. Cham: IEEE, 2012, 120(5), 41-44. Advances in Information Security. ISBN 978-1-4673-1741-2. ISSN 00434403. Available from: doi:10.1016/j.patcog.2021.108122

[21] Biometric Voice Recognition – Everything You Should Know. Imageware [online]. [cit. 2023-03-14]. Available from: https://imageware.io/biometric-voice-recognition/

[22] Biometric Authentication and Identification using Behavioral Biometrics Technique of Signature Verification, 2019. International Journal of Innovative Technology and Exploring Engineering. 8(9S4), 33-38. ISSN 2398-4275. Available from: doi:10.35940/ijitee.I1106.0789S419

[23] RAUL, Nataasha, Radha SHANKARMANI a Padmaja JOSHI, 2020. A Comprehensive Review of Keystroke Dynamics-Based Authentication Mechanism. International Conference on Innovative Computing and Communications. Singapore: Springer Singapore, 2020-11-17, 8(9S4), 149-162. Advances in Intelligent Systems and Computing. ISBN 978-981-15-0443-8. ISSN 2398-4275. Available from: doi:10.1007/978-981-15-0444-5_13

[24] Kvalitativní rozhovory – polostrukturované a nestrukturované. WikiKnihovna [online]. [cit. 2023-03-23]. Available from: https://wiki.knihovna.cz/index.php?title=Kvalitativn%C3%AD_rozhovory_%E2%80%93_polostrukturovan%C3%A9_a_nestrukturovan%C3%A9

[25] Využití multikriteriální analýzy (MCA) pro hodnocení inteligentních elektroinstalací. TZB-info [online]. [cit. 2023-03-23]. Available from: https://elektro.tzb-info.cz/inteligentni-budovy/7651-vyuziti-multikriterialni-analyzy-mca-pro-hodnoceni-inteligentnich-elektroinstalaci

[26] ZATLOUKAL, Filip, 2012. Analýza a porovnání biometrických metod. Vysoká škola ekonomická v Praze.

[27] Autentizační metody založené na biometrických informacích, 2010. ISSN 1214-9675.

[28] RAJASEKAR, Vani, Bratislav PREDIĆ, Muzafer SARACEVIC, Mohamed ELHOSENY, Darjan KARABASEVIC, Dragisa STANUJKIC a Premalatha JAYAPAUL, 2022. Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm. Scientific Reports. 12(1). ISSN 2045-2442. Available from: doi:10.1038/s41598-021-04652-3

[29] KONTSEVICH, Lenny. The future of biometrics is in the palm of your hand. Biometric Update [online]. [cit. 2023-05-12]. Available from: https://www.biometricupdate.com/202007/the-future-of-biometrics-is-in-the-palm-of-your-hand

[30] PODDAR, Jivesh, Vinanti PARIKH a Santosh Kumar BHARTI, 2020. Offline Signature Recognition and Forgery Detection using Deep Learning. Procedia Computer Science. 170, 610-617. ISSN 18770509. Available from: doi:10.1016/j.procs.2020.03.133

[31] JORGENSEN, Zach a Ting YU, 2011. On mouse dynamics as a behavioral biometric for authentication. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM, 2011-03-22, 476-482. ISBN 9781450425648. Available from: doi:10.1145/1966913.1966983

[32] Verieye sdk IRIS identification for stand-alone and client-server solutions. NEUROtechnology [online]. [cit. 2023-05-12]. Available from: https://neurotechnology.com/prices-verieye.html?gclid=EAIaIQobChMIw-Kk0v_e_QIVGs13Ch2voQtMEAAYASABEgI9YfD_BwE

[33] Hand Geometry System. Indiamart [online]. [cit. 2023-05-12]. Available from: https://www.indiamart.com/proddetail/hand-geometry-system-13408641842.html

[34] How Much Do Access Control Systems Cost?. Vizpin [online]. [cit. 2023-05-12]. Available from: https://vizpin.com/blog/access-control-pricing/

[35] WU, Wei, Stephen John ELLIOTT, Sen LIN, Shenshen SUN a Yandong TANG, 2020. Review of palm vein recognition. IET Biometrics. 9(1), 1-10. ISSN 2047-4938. Available from: doi:10.1049/iet-bmt.2019.0034

[36] Signature Verification System. Aws marketplace [online]. [cit. 2023-05-12]. Available from: https://aws.amazon.com/marketplace/pp/prodview-w7czyu3coxbke?stl=prodview-w7czyu3coxbke

[37] Palm print readers. Biometric Supply [online]. [cit. 2023-05-12]. Available from: https://www.biometricsupply.com/product-category/fingerprint-readers/palm-capture/

[38] MARTINEK, Jan. Hacknout nemocnici? Stačí bílý plášť a počítač. Právo [online]. 13. 2. 2019 [cit. 2023-04-41]. Available from: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hacknout-nemocnici-staci-bily-plast-a-pocitac-40391055

[39] KOUBOVÁ, Michaela. Nemocnicím nechybí jen zdravotníci, ale i experti na informační technologie. Přitom čelí palbě kyberútoků. Zdravotnický deník [online]. 7.12.2021 [cit. 2023-04-41]. Available from: https://www.zdravotnickydenik.cz/2021/12/nemocnicim-nechybi-jen-zdravotnici-ale-i-experti-na-informacni-technologie-pritom-celi-palbe-kyberutoku/

[40] TŘEŠŇÁK, Jaroslav, Cybersecurity Manager at St. Anne's University Hospital in Brno [oral communication]. Brno, 13.4.2023.

[41] Which biometric authentication method is the best?. AwareID [online]. 18.11.2021 [cit. 2023-04-42]. Available from: https://www.aware.com/blog-which-biometric-authentication-method-is-the-best/

[42] Which biometric authentication method is most secure?. NEC [online]. 16.4.2020 [cit. 2023-04-42]. Available from: https://www.nec.co.nz/market-leadership/publications-media/which-biometric-authentication-method-is-most-secure/

[43] TALANDOVÁ, Hana, 2010. Studie využití biometrických systémů v průmyslu komerční bezpečnosti. Zlín. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

[44] GRIFFIN, John. Why Keystroke Dynamics is key to preventing Identity Theft. Fleksy [online]. 12/2022 [cit. 2023-04-42]. Available from: https://www.fleksy.com/blog/why-keystroke-dynamics-is-key-to-preventing-identity-theft/

10 LIST OF FIGURES USED

Figure 1: Dependency of FAR and FRR [10]..14

Figure 2: Authentication method - evaluation 26

Figure 3: Individual work computer - evaluation 26

Figure 4: Number of employees with access to one computer - evaluation... 26

Figure 5: Exposure to cyber-attack - evaluation... 27

Figure 6: Unauthorised person at a computer - evaluation 27

Figure 7: Sufficient security - evaluation... 28

Figure 8: Considering improvement - evaluation 28

11 LIST OF TABLES USED

Table 1: Analysis of biometric methods 32

Table 2: Ratings of sub-criteria 33

Table 3: The analysis of applicability of biometric methods in HCF 35

12 LIST OF ATTACHEMENTS

Attachement A: The Questionnaire 61

The Questionnaire

1. Number of employees in your healthcare facility (hereafter referred to as HCFs)
    1. Up to 100 employees
    2. 100 - 500 employees
    3. 500 - 1500 employees
    4. More than 1500 employees

Securing access to a work computer/tablet/laptop/... (hereinafter referred to as computer)

2. What authentication method do you use to access computers in your HCFs?
    1. None
    2. Password
    3. Fingerprint
    4. Facial recognition
    5. Chip/ID card
    6. Other...

3. Do most employees (more than 60%) have an individual work computer with access to patient and hospital data?
    1. No
    2. Yes

4. If you selected No in previous question, how many employees on average have access to one computer within a department?
    1. 2
    2. 3
    3. 4
    4. 5
    5. More than 5

5. When working with sensitive patient data on a computer, does an employee have to re-verify their identity (e.g. by entering a password, using a chip or fingerprint)?
    1. No
    2. Yes

6. Are computers used by the staff located in places accessible only to medical staff or also in publicly accessible places (e.g. corridors, waiting rooms, reception areas,...)?
   1. Only in areas accessible to staff
   2. Also in places accessible to the public

7. Are employees instructed on proper security of a computer from external intrusion (how to create a password, secure their login account, etc.), e.g. through training or written instructions?
   1. No
   2. Yes

8. Does your HCF have an IT staff member to take care of computer and network security?
   1. No
   2. Yes

Reflecting on current situation

9. Do you register that your HCF has been exposed to a large-scale cyber-attack in the past?
   1. No
   2. Yes

10. Have you encountered an unauthorised person (e.g. a patient) in your HCF at a computer without an HCF employee present?
    1. No
    2. Yes

11. Do you find security of the computers in your HCF sufficient?
    1. No
    2. Yes

12. Would you consider improving computer access security in your HCF if the solution would be user- and financially friendly?
    1. No
    2. Yes