Implementation of User Authentication System in Smart Hospitals Useful in the Age of the Covid-19 Pandemic

Nenad Badovinac

Faculty of Organizational Sciences - University of Belgrade, nenad.badovinac@gmail.com

Contribution to the State of the Art

https://doi.org/10.7251/JIT2101024B UDC: 004.72.057.4:[616.98:578.834

Abstract: The security system for authentication and user records in a smart hospital is part of an integrated security system consisting of various authentication devices. The security system should be adapted to different characteristics of users, their user processes, but also to periods when the possibility of infection is increased due to a virus pandemic and contamination during multiple touches of different persons on authentication devices. The use of gloves and a medical face mask during a pandemic limits biometric scanning of fingerprints and facial images. During a virus pandemic, some authentication devices have limitations that need to be considered when creating an integrated security system that will have the purpose of securing doctors, staff, patients, information, and things in a smart hospital. In this paper, the parameters on the basis of which it is possible to design an optimally integrated security system are recommended.

Keywords: smart hospital, access control, user authentication, virus pandemic.

Introduction

Part of the smart hospital's integrated security system is the access control system. Due to the different characteristics of smart hospital users in relation to users of other types of smart buildings, it is necessary to create a customized user interface that should enable the interaction of specific types of users with the security system of the smart hospital. Users of smart hospitals, unlike users of other smart buildings, differ in psycho-physical characteristics and user processes that they perform on a daily basis. The system should enable the recording of doctors, other hospital staff, patients and visitors. Due to the large number of patients, but also visitors who become part of the smart hospital system every day, it is necessary to design a specific user interface with which different types of users will be able to easily register in the access control system. Each type of user interface has its advantages and disadvantages. In a time of virus pandemic, authentication devices such as biometric fingerprint scanners are a potential source of disease transmission due to contamination from touch by different users. These devices pose a potential risk of transmitting the infection. The deposition of dirt from a finger that touches the surface of authentication devices or a biometric fingerprint scanner can contaminate the surface of the device [1]. It is potentially possible for a smart hospital user to become infected with viruses that can be found on the surface of authentication devices [2]. These authentication models increase the possibility of the user becoming infected with viruses [3]. The essence of this paper is a set of parameters on the basis of which different designs of authentication and identification devices are proposed, which should be adapted to all specific users of smart hospitals and their user processes. The design and implementation of several different authentication and identification devices enables the smart hospital: records of all present users of the smart hospital, reporting of incidents in the building with facilitated identification of the responsible person, control of user movement in smart hospital departments. This system is able to control the optimal number of doctors in individual departments. With adequate software, the system could control the maximum number of visitors per ward, then, it could activate an alarm, in case the optimal number of doctors in the wards is reduced. This paper is conceived as follows: Chapter 2 of this paper presents an overview of previous research and available literature. Chapter 3 describes the problem of authentication and identification in smart hospitals. Chapter 4 describes the proposed parameters for the implementation of the smart hospital user authentication system. Chapter 5 describes the implementation process. Chapter 6 contains the conclusion of the paper.

LITERATURE REVIEW

Initially, smart buildings referred only to buildings that had a system for optimizing energy consumption. In the early 1980s, a smart building could manage systems such as lighting, air conditioning, and electricity consumption. Today's smart buildings are multifunctional systems that use the available technology of various sensors and automation systems. The systems and technologies used in today's smart building are [14]:

- Sensors - a network of sensors installed inside the building provides various information about the user's location and accordingly allows automatic control of systems such as: system for switching electrical devices on and off, switching heating on and off. An important segment in smart buildings is security. Therefore, it is necessary to ensure the security of systems in a smart building and protect them from attacks, especially the user access control system (access control), which consists of security cameras, ID devices and motion detectors. Sensors and face recognition cameras are used to identify a person in smart buildings. Unauthorized access is considered the greatest danger in a smart building.
- The access control system assigns different access rights to different users. Some functions (e.g. lighting control or air conditioning) can be assigned to all users, but some users (children, visitors) can be restricted to certain functions. The process of registration and identification of users who log in to the system should be as simple as possible, but secure enough. A good solution to this problem is biometric fingerprint protection [14], but this solution is not optimal for different types of smart hospital users.

Accurate patient and visitor identification is of great importance for hospital safety [15]. It can be found in the literature that the health industry is increasingly accepting new technologies [16]. Organizations want to improve the treatment phase and make patient care easier. Hunderdon Healthcare has simplified the registration of patients, because they decided to apply iris biometrics. All users were well informed about the benefits of new technologies and there was no opposition when using this technology [3]. ImPrivata company proposes the identification of smart hospital users using PalmVein biometrics (palm blood biometrics). In this case, the patients bring their hand closer to the palm reader and the scanner recognizes the pattern of veins on the palm on the basis of which it identifies the user. This simple scanning procedure improves patient identification: It reduces errors in patient identification and reduces the possibility of infection, as there is no palm contact on the device. Palm recognition is one of the most accurate and appropriate methods of patient identification [17]. Different technologies are available for implementation in a smart hospital.

PROBLEM OF AUTHENTICATION AND IDENTIFICATION OF SMART HOSPITAL USERS

Due to the large number of users who enter smart hospitals on a daily basis, it is necessary to implement a system of records and access control. The record system should allow only authorized persons to move through the hospital. It is a great challenge to create special ID devices that will be financially optimized, and at the same time efficient enough for different types of smart hospital users. User records should be made in front of each hospital ward, hospital room or any other room. Upon entering the building, an unauthorized person must register in order to obtain an authorization to move. The identification and authentication system is performed on an ID device that needs to be optimally designed with regard to the type of

ID technology. When designing ID devices for the needs of user records in smart hospitals, it is necessary to focus on understanding the diversity of users. There are several types of users that need to be registered. Each type of user has its own work processes and its own psychophysical characteristics, for that reason the recording system must be harmonized with several parameters. The implementation of unnecessarily expensive or inefficient identification technology should be avoided. Therefore, it is necessary to design several variants of the ID device that will enable fast and efficient identification of all types of users.

For the purposes of implementing a record keeping system, it is necessary to design financially optimized devices. The paper proposes to take into account the parameters on the characteristics of user types shown in Table 1 and their user processes for the implementation of optimized devices. An integrated system for user identification and authentication (access control) should enable:

- Records of all present smart hospital users
- Reporting an incident with facilitated identification
- Control of user movement in smart hospital wards
- Control of the optimal number of doctors in certain departments
- Control of the maximum number of visitors per department
- Activation of the alarm if the number of doctors in the hospital wards is reduced,
- Parking control, etc.

PROPOSED PARAMETERS FOR IMPLEMENTATION OF AUTHENTICATION DEVICES

The parameters that affect the development of the optimal system for user authentication are presented in four groups:

- Characteristics and processes of hospital users
- Available technologies from which it is necessary to choose the optimal ones
- ID device layout by hospital premises
- User registration and identification process.

Characteristic processes of hospital users

It is necessary to implement ID devices for identification and authentication application that would be adapted to all users of the smart hospital and their user processes [5]. The design of the ID device should meet the psychophysical needs of the user and enable a simple process of user registration and identification. Table 1 lists the characteristics of the smart hospital user process that affect the authentication and identification process.

***Table 1** – Characteristic processes of hospital users*

User type	Characteristic processes of users
Medical staff	A fast system is needed to identify the entrance to operating rooms and hospital rooms. Work in gloves and a special medical suit.
Other staff	A fast identification system is needed in front of operating rooms and hospital rooms. Work with dirty hands, with which they cannot be registered with a PIN number.
Patients	Due to reduced psychophysical abilities, the range of proposed ID technologies, such as remembering a PIN number or carrying an ID token, has been reduced.
Visitors	The area of movement is the corridors from the entrance to the building to the hospital room where the patient the visitor wants to visit is accommodated. There are many visitors in the hospital and cheap ID technology is needed.

List of available ID technologies

A list of proposed ID technologies with advantages and disadvantages depending on the user processes in the hospital can be found in Table 2. [6] [7]. Various identification and authentication technologies are available: Biometrics, PIN number, RFID chips, barcodes. Each of these technologies has certain advantages and disadvantages. For example: RFID cards can be lost or forgotten, PIN numbers can be used without authorization, biometric systems must be adapted to the psychophysical characteristics of the user. Due to health disorders, patients cannot use any biometric system. It is impossible to expect elderly patients to remember PIN numbers. The voice-based biometric system cannot be used by patients who have a problem with sore throat.

Barcode technology requires optical visibility [6]. Unlike barcodes, the RFID system actively broadcasts data, eliminating the need for manual reading. This advantage significantly improves customer service [8]. RFID systems have a shorter scan time than

Table 2 *– Characteristics of ID technologies*

Characteristics of various ID technologies				
1D barcode	**2D barcode**	**RFID**	**PalmVein biometrics**	**PIN**
Requires optical visibility	Requires optical visibility	Readable even though it is not in sight	There is no transmission of the infection, because the user has no contact with the device.	4-digit number easy to remember.
Unauthorized copying is possible	Unauthorized copying is possible	RFID distance from the scanner - a few centimeters.	It is used where a higher level of hygiene is needed.	Adequate for older and younger population
Low production costs.	Easy to make, low production costs.	It can also be used in aggressive environments.	Identification is not affected by skin moisture	Cheap technology.

barcode systems. RFID is an automated solution that makes the process of identification and data collection more efficient [7].

Technology selection by user types:

a. Doctors - Emergency medical intervention in the surgical department requires rapid identification on all identification devices. An effective way of identification is for the doctor to have an RFID wristband, which will enable him to quickly identify himself by placing his hand near the scanner with a few tens of centimeters. It is possible for doctors to identify with surgical gloves, because even then, a thin RFID bracelet can be identified. The problem with RFID is the high cost of tags [14], however, the model assumption in this paper is that tags will be used exclusively by physicians and other hospital staff, which in a complete implementation will not represent a major investment. For these reasons, RFID technology was chosen for the needs of this model for the needs of doctors.

b. Other hospital staff - hospital staff need to have a fast and efficient identification system due to frequent visits to other wards, rooms or corridors. It would be inefficient if the user had to stay in front of the ID device for a long time to enter a PIN number or identify himself with Palm biometrics. The registration process would be difficult while the user is wearing hospital gloves or has dirty hands. For these reasons, RFID technology was chosen for the needs of this model for the needs of hospital staff.

c. Patients - It is impossible to expect the patient to carry an RFID device with him. For the needs of patient records, a biometric technology was chosen - PalmVein, whose advantages are: a high level of security, simplicity of the identification process and reduced transmission of infectious diseases [17].

d. Visitors - the most represented users of the smart hospital are visitors. Cheap identification PIN technology was chosen for the needs of visitor records. They need access to only one hospital ward in the hospital, and that is the ward where the patient they are visiting is lying. The visitor has the possibility to move only to one hospital room, so it is enough that the system assigns a certain PIN number to enter only one hospital room. Table 3 shows the optimal technologies by user types.

Table 3 *– optimal ID technologies by user types*

Users	Chosen technology
Medical staff	RFID bracelet
Other staff	RFID bracelet
Patients	PalmVein biometrics
Visitors	PIN number

Spatial units in the hospital

The data in Table 4 shows the technology IDs to be implemented on sites. The "+" symbol defines the user and the ID technology that is necessary to be installed in the ID device at a specific location in the hospital. The sign "-" defines that a certain ID technology is not required in a certain location. Each variant of the ID device will have optimal ID technology depending on the needs of a particular location. With such an approach, the implementation cost will be optimized.

Table 4 *– ID device variants for user identification*

Spatial unit	Doctors (RDIF)	Other staff (RFID)	Patients (PalmVein)	Visitors (PIN)	ID device variant
Registration	+	+	+	+	A
Hospital parking lot	+	+	+	-	B
Passageways	+	+	+	+	A
Waiting room	+	+	+	+	A
Registration unit	+	+	+	+	A
Spec. department	+	+	+	-	B
Cafeteria for employees	+	+	+	+	C
Warehouses	+	+	-	-	C
Apartments	+	+	+	+	A
Rooms	+	+	+	+	A
Technical rooms	+	+	+	-	B
Medical premises	+	+	-	-	C

The data in Table 4 show that it is necessary to design three variants of ID device for a specific smart hospital. Each of the devices will have selected identification technologies.

User identification and authentication process

The process of entering an unauthorized person in the hospital begins with the process of user registration. After registration, the system user accesses the ID of the device on which they need to authorize. In accordance with the successful authorization, they will receive a permit to enter the department. The system recognizes three operational processes and these are: User Registration, Successful Authorization and Failed Authorization. After registration, an unauthorized person becomes a user of the hospital and after that the security system will allow the user to move through the smart hospital after successful identification on ID devices. The list of locations in front of which the registration and identification system should be implemented can be found in Table 4. User registration - Figure 1 shows the process of registration of unknown persons. The user approaches the system administrator who inserts the smart card into the card reader. The administrator processes the data from the ID card and registers the user. The admission department in the hospital enters in the database a permit for categorization of an unauthorized person in the category (patient, visitor).

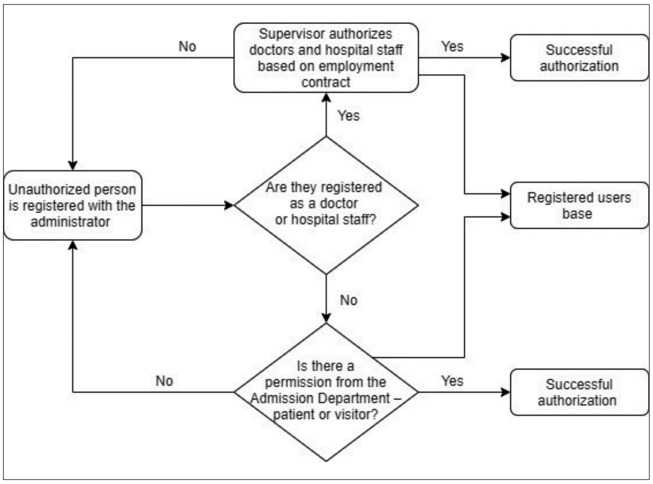
Supervisor authorizes doctors and hospital staff based on employment contract
No
Yes
Successful authorization
Yes
Unauthorized person is registered with the administrator
Are they registered as a doctor or hospital staff?
Registered users base
No
No
Is there a permission from the Admission Department – patient or visitor?
Yes
Successful authorization

Figure 1 *– User registration*

The movement of the authorized user through the wards of the smart hospital is enabled by identification on the ID device. Upon successful authorization, the system will allow access to the department. Successful user identification - Figure 2 shows the successful identification process. After successful identification, the system provides access and the user is authorized to enter. The user accesses the ID device, uses one of the offered ID technologies and, depending on the authorization rules, the ID device allows access to the department by opening the electronic lock.

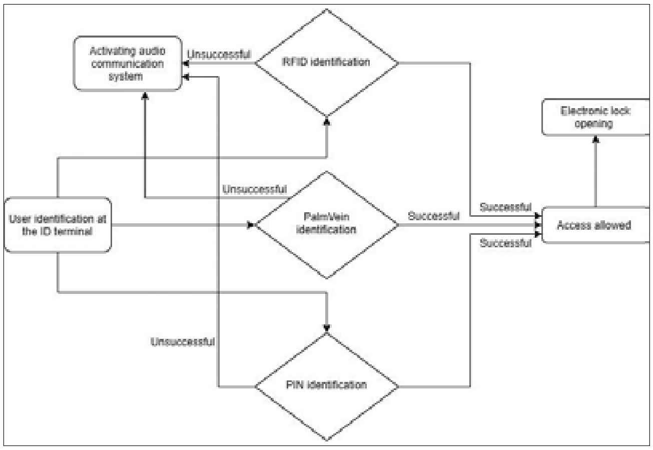

Figure 2 – *Successful identification process*

Failed user identification - Figure 3 shows the failed identification process. The user tries to identify himself, but the system does not recognize the user. In that case, an audio device is turned on, through which the system directs the user about the direction of movement through the hospital.

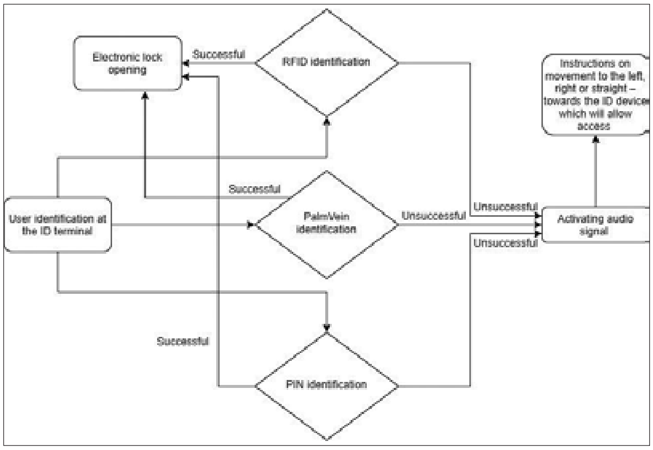

Figure 3 – *Failed identification process*

IMPLEMENTATION

The implementation of a user record system requires prior categorization of users and user processes that will determine the optimal ID technology. Implementation planning implies that security objectives are well defined [5]. The data analysis shown in Table 4 will determine the required ID device types. If a good estimate is not made in terms of the total number of ID devices, the system may not be able to provide the required level of security. Examples of parameters are defined on the basis of a general hospital. Analyzing the parameters from Chapter 4 of this paper, three variants of identification and authentication (ID) devices are proposed. Their implementation achieves optimized costs. Below are the processes that will run on each of the three designed interfaces.

ID device variant A - enables identification of all users:

Figure 4 shows a variant of the ID device that allows the identification of the Physician and Hospital staff to perform the process of visiting the patient, entering the operating rooms and other medical rooms. This variant of the ID device allows patients to identify themselves for the process of entering hallways, waiting rooms and rooms. Also, this variant of the device enables the identification of the visitor in the room where the patient is accommodated.

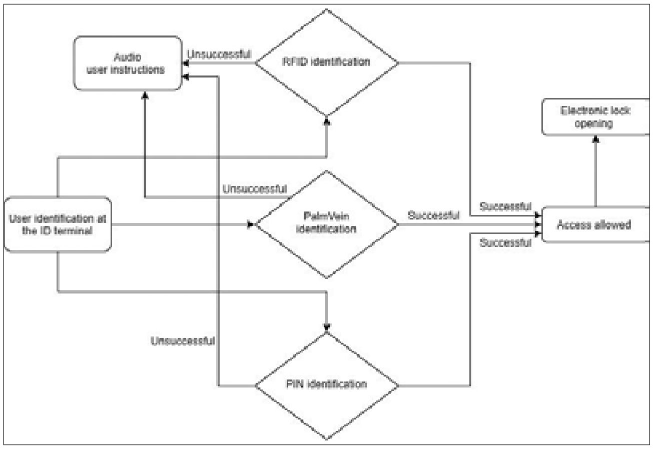

Figure 4. *Identification processes on an ID device – Variant A*

ID device variant B - enables identification of doctors, staff and patients:

Figure 5 shows a variant of the ID device that allows the identification of the Physician and Hospital staff for the processes of visiting the patient, entering the operating rooms and other medical rooms. This variant of the ID device allows patients to identify themselves for the process of entering hallways and rooms. This device will be implemented in front of a location that visitors do not enter.

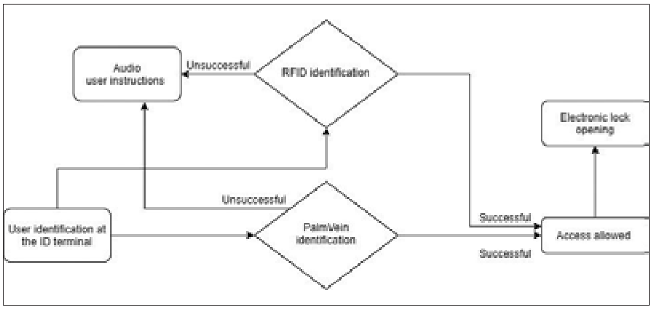

Figure 5. Identification processes on an ID device – Variant B

ID device variant C - enables identification of doctors and hospital staff:

This variant of the device is the cheapest to implement and enables the process of identification of doctors and hospital staff. It enables RFID identification and that is enough for their user processes: going to visit the patient, entering the operating rooms and other doctor's rooms.

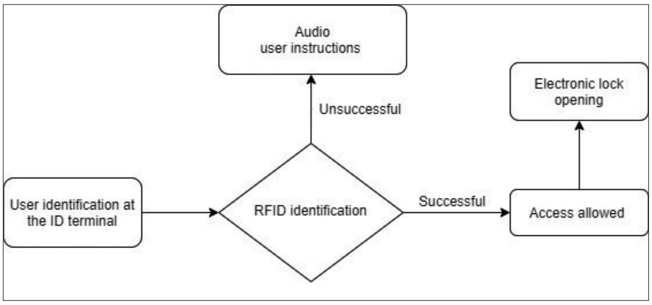

Figure 6. Idetification processes on an ID device – Variant C

All hospital users are registered on these three variants of the ID device. For the implementation of the user record system in hospitals, the design of the ID device is shown in Figure 7 with three interface variants arranged in the locations defined in Table 4. The selected interface must be in accordance with the user characteristics. It is necessary to test the security, effectiveness and functionality of the recording system and in that way it is possible to reach the optimal interface design. Figure 7 shows the proposed three interface models to be used in the user record system. Each of them needs to pass the use phase test. Redesign may be required during testing.

ID devices in Figures 8 - 10 are proposed. The ID devices meet the HCI interfaces defined in this paper. For the variant variant, the proposed model is from the manufacturer Dehicon [12], [13].

CONCLUSION

The presented system for user authentication in a smart hospital is adapted to different characteristics of users, their user processes, but also to periods when the possibility of infection is increased, such as the period due to a virus pandemic. The proposed set of parameters of this system enables the development of a specific system for user authentication in smart hospitals and helps in the development of different variants of the device with respect to different authentication interfaces. The innovative interface model for authentication and user access control presented in the paper is applicable in the era of a pandemic of a virus like Covid-19. The implementation process keeps track of the required HCI (human-computer interface) components depending on the users who are authorized to access a particular hospital room. Such an approach will enable the optimization of implementation costs. Us-

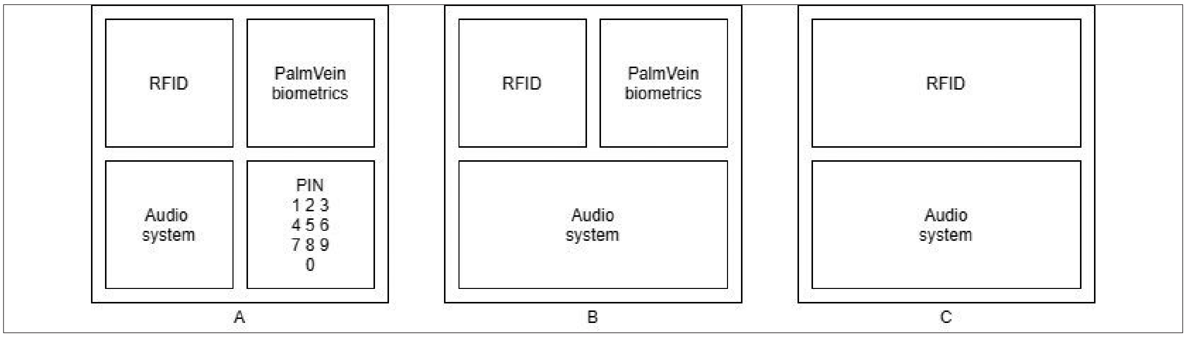

Figure 7. Three variants of ID device: a) variant A, b) variant B, and c) variant C

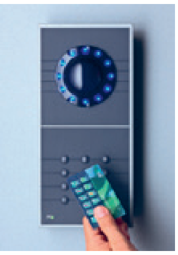

Figure 8.
ID device - variant A

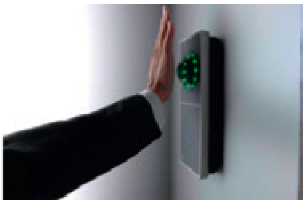

Figure 9.
ID device - variant B

Figure 10.
ID device - variant C

ing additional software support, the functions of the user record system can be expanded with a detailed record of smart hospital users present, such as controlling the optimal number of doctors in a particular hospital ward at a given time, but it is also possible to control the maximum number of visitors per ward. In short, by choosing an adequate software component, the possibilities of control in the field of smart hospital security are expanded.

REFERENCES

[1] Sano E, Maeda T, Nakamura M, Shikai K, Sakata M, Matsushita M, et al. “Fingerprint Authentication Device Based on Optical Characteristics Inside a Finger”, 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW’06); New York, DOI: 10.1109/CVPRW.2006.83

[2] Jonathan A. Otter, PhD Saber Yezli, PhD James A.G. Salkeld, BSc Gary L. French, MD, FRCPath: “Evidence that contaminated surfaces contribute to the transmission of hospital pathogens and an overview of strategies to address contaminated surfaces in hospital settings”, VOLUME 41, ISSUE 5, SUPPLEMENT , S6-S11, MAY 01, 2013. DOI:https://doi.org/10.1016/j.ajic.2012.12.004

[3] Nana Mensah Abrampah, Maggie Montgomery, April Baller, Francis Ndivo, Alex Gasasira, Catherine Cooper, Ruben Frescas, Bruce Gordonb & Shamsuzzoha Babar Syeda: Improving water, sanitation and hygiene in health-care facilities, Liberia” Bull World Health Organ 2017;95:526–530| doi: http://dx.doi.org/10.2471/BLT.16.175802

[4] Sankalp Bagaria (2014): „Authenticating Transactions using Bank–Verified Biometrics“. https://arxiv.org/ftp/arxiv/papers/1407/1407.3366.pdf

[5] Lukać, K., Šošević, U., Milovanović, M. (2014). Dizajniranje korisničkog interfejsa za multimodalnu akviziciju biometrijskih podataka. Infoteh.

[6] Sremčev, N., Lazarević, M., Tarjan, T., Baranovski, I., Medojević, M. (2017). Uporedna analiza savremenih identifikacionih tehnologija, Infoteh-Jahorina, vol. 16.

[7] Jones, P., Clarke-Hill, C., Hillier, D. (2005). The benefits, challengeres and impacts of radio frequency identification technology (RFID) for retailers in the UK. Mark. Intell.

[8] Pongpaibool, P. (2008). A study on performance of UHF RFID tags in a package for animal traceability application”, inf. Technol.

[9] Lin, Y.C.L, Cheung, W.F., Siao, F.C. (2014). Developing mobile 2D barcode/RFID-based maintenance management system, Autom. Constr., vol 37, pp. 110-121.

[10] Blagojević, D. (2011). Model korisničkog interfejsa interaktivnog obrazovnog softvera, “Tehnika i informatika”, Čačak.

[11] Vilendečić, B., Dejanović, R., Ćurić, P. (2016). Uticaj ljudskog faktora u implementaciji SIEM sistema, INFOTEH-JAHORINA Vol. 15.

[12] Text taken from web page: http://www.albatech.rs/resenja/dexicon/

[13] Text taken from web page: https://www.pcs.com/en/solutions-products/access-control/rfid-readers/intus-600-reader/

[14] An example of the use of biometric systems in smart hospitals. Internet link created (2012). http://www.cis.hr/files/dokumenti/CIS-DOC-2012-04-045.pdf

[15] An example of use of PalmVein in a hospital: http://www.rightpatient.com/

[16] Text “Using biometric identification to improve patient safety” from the web page taken in July 2016. https://www.imprivata.com/blog/using-biometric-identification-improve-patient-safety

[17] Text “Biometric patient identification” taken from the web page in July 2016. https://www.imprivata.com/imprivata-patientsecure

Submitted: April 21, 2021
Accepted: May 31, 2021

About the authors

Nenad Badovinac received his Master degree at the Faculty of Organizational Sciences, University of Belgrade, Serbia in 2015. He is the author of several scientific papers in the field of e-business and electronic payment system that have been published in local and international conferences and publications. He is PhD student at Faculty of Organizational Sciences, University of Belgrade.

For citation

Nenad Badovinac, Implementation of User Authentication System in Smart Hospitals Useful in the Age of the Covid-19 Pandemic, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 11(2021) 1:24-32, (UDC: 004.72.057.4:[616.98:578.834), (DOI: 10.7251/JIT2101024B), Volume 11, Number 1, Banja Luka, June 2021 (1-68), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004