Received: May 23, 2023. Revised: July 5, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Access Control to Robotic Systems Based on Biometric: The Generalized Model and its Practical Implementation

Amer Tahseen Abu-Jassar[1] **Hani Attar**[2]* **Vyacheslav Lyashenko**[3] **Ayman Amer**[2]
Svitlana Sotnik[4] **Ahmed Solyman**[5]

[1]*Faculty of Computer Science and Information Technology, Ajloun National University, Ajloun, Jordan*
[2]*Faculty of Engineering, Department of Energy Engineering, Zarqa University, Zarqa, Jordan*
[3]*Department of Media Systems and Technology,*
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[4]*Department of Computer-Integrated Technologies, Automation, and Mechatronics,*
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[5]*Department of Electrical and Electronics Engineering, Faculty of Engineering and Architecture,*
Nişantaşı University, 34398 ˙Istanbul, Turkey
*Correspondence author’s Email: Hattar@zu.edu.jo

Abstract: The paper presents a generalized system's structural scheme and components for monitoring and controlling access to robotic systems based on biometric data for decision-making. Mathematical decision-making models for choosing the best alternative based on fuzzy sets are proposed. The fuzzy analytical hierarchy process determined weights of 6 criteria (for k_1 criterion weighting factor is equal to 2.2; for k_2 criterion – 1.8; for k_3 criterion – 0.6; for k_4 criterion – 0.6; for k_5 criterion – 0.6; for k_6 criterion – 0.2, that is, most weighty would be k_1 – recognition accuracy) against which the best option was evaluated. Thus, during evaluation of alternative on six criteria it was obtained that t alternative X_1 (face recognition in full-face), will have the key value of membership function of resulting fuzzy set alternatives with ideal value of integral criterion, equal to 0.53, and as result, implemented rational choice, taking into account given criteria. The difference is that we have introduced such criteria as anti-spoofing. The access control system for robotic systems works in real-time. It is implemented based on an algorithmic decision-making complex, which includes two-factor authentication to increase security: registration involves entering employee data from the keyboard (password, login, surname, first name, position) and physiological authentication (identification by face). Face detection is proposed to be implemented on several images: face, profile, face, and profile in the mask. A distinctive feature of our development is that often, a main requirement for "access control systems with facial identification" is the frontal location of the face relative to the camera; in our case, the image of the face at an angle was added.

Keywords: Access, Control, Robotic systems, Biometric data, g\Generalized model.

1. Introduction

Currently, robotics is very actively developing [1-6]. Aviation, household, military, space, medical, underwater, industrial, and construction robotics exist.

There is a constant increase in interest in industrial robotics and robotic systems (RS).

The access control system (ACS) is the best security and control of any organization, and enterprises with robotic systems are no exception since it allows you to automatically determine access rights to important data. However, simultaneously, it is necessary to identify the subject automatically – the person (employee) who accesses ACS object (enterprise with RS).

Access control affects various areas. At the same time, disadvantages of traditional methods can be highlighted:

- Discretionary access control (DAC) [7-9] –

DOI: 10.22266/ijies2023.1031.27

flexible method based on identification of resource owners, however, if it is necessary to ensure anonymity of user, this type of access control is not suitable, as it requires identification of all subjects and objects in system and is not provided.

- Mandatory access control (MAC) [7, 8] – access to objects is defined and controlled based on classification of information and levels of secrecy, but there are limits to flexibility and difficulty of making changes to access rights.

- Role-based access control (RBAC) [7, 10] – method in which access rights are assigned at level of roles rather than individual users, but this method is not always flexible enough to manage access at more granular level.

- Attribute-based access control (ABAC) [8, 11] – method that allows you to define access rights based on wide range of attributes, including, for example, user IDs, groups, access time, location, data type and other properties, however, ABAC alone does not provide anti-spoofing protection, and additional security mechanisms and solutions may be required to achieve this goal.

Therefore, taking into account listed disadvantages, this paper will implement verification of key attributes to prevent unauthorized access or use of forged identifiers, and this will expand applicability of system in real world.

The security of robotic systems and their associated middleware infrastructures is a critical issue for industrial and consumer IoT and needs to be continuously evaluated throughout the development lifecycle [12].

The authors consider issues related to the safety of deploying robots in the real world [12]. This paper proposes a control markup language applicable to robotic systems, ComArmor, as syntax access and computational graphs; however, the degree of model validation for semantic resolution profiles is not described, and a comparison with existing analogs is not given.

The safety of robotic operating systems (ROS) is discussed in [13]. The authors propose an access control mechanism for ROS based on advanced policy-based access control model (PBAC), but it is still being determined why PBAC was chosen. You should be aware of PBAC compatibility issues because PBAC policy may not be compatible with all organizations. This is because not all of them can set policies that will affect access to sensitive resources without compromising security.

In [14], authors proposed general architecture for distributed cloud-enabled robotic information fusion systems. The paper presents a typical scenario of a robotic cloud system; the abstract architecture of a cloud robotics system; workflow when a user request service from a Web portal; frame with tagged targets of video tracking algorithm, but no attention is paid to specifics of decision-making to provide access to cloud-enabled robotic information fusion system. Although there is information that authentication and access control are implemented, some web interface functionality is implemented in the framework.

The administrator uses a Web interface to monitor all robot camera images. All users, including administrators, are authenticated using a username and password scheme and can access any resource.

The solution to the problem of remote control of rehabilitation robots is presented in [15]. As a wrist robot, it is a sophisticated robot that provides two wrist movements (flexion /extension and abduction/adduction). Integrating a fuzzy controller into the system management architecture achieves patient safety during therapy. The Wi-Fi screen provides the media access control address (MAC address), so the robot has its physical address as a unique identifier for the network interface controller. Connecting the Arduino board to the Internet was designed using a Wi-Fi library. In this paper, we are talking about connecting to the Internet, so data privacy is also important since incorrect management of robotic systems or leakage of important information can harm human health.

Access control of the robotic operating system is described in [16]. Access control for robotic middleware systems has been investigated in both ROS1 and ROS2. The authors explored RBAC (Role-Based Access Control) mechanism. However, RBAC sometimes needs more flexibility, as roles defined at the beginning of the RBAC project may no longer align with the company's goals. In addition, administrators face pressure to quickly attract new employees, even those who still need undefined roles.

The problem of access control covers not only the issue of access to individual specialized objects but also to a set of RSS, for example, robotic lines interconnected by vehicles and control systems or several blocks of technological equipment serviced by one or more industrial robots to perform operations in accepted technological sequence.

By analyzing current research, for example, authors of [17] considered security issues to control access to sensitive data for Internet of Things. Here we present approach to security management in authentication, which is distinguished by use of two coupled convolutional neural networks (CNNs) for biometric user identification. Despite achievements and advantages of presented approach to security management in Internet of Things authentication, this method is difficult to implement, that is, implementation and deployment of such complex security system, especially when using neural networks and machine learning technologies, may require significant effort and resources. Therefore, our proposed method is simpler in this regard.

In [18] authors solved problems of electrocardiogram recognition in field of biometrics. A method of biometric recognition based on electrocardiogram (ECG) feature vector, which uses a pooling layer to accept beats of variable length, is proposed. The method accepts new classes without the need to retrain the model, achieving excellent recognition performance. Although our work is not in the field of ECG, it allows to increase level of security and protect system from unauthorized access through two-factor authentication.

Two-factor authentication is important tool for enhancing security and protecting access control. That is, it requires provision of two independent factors to verify identity. It supplements traditional authentication method based on password knowledge with additional factor such as physical device, biometric data (e.g. fingerprints, facial recognition, etc.) or time code.

In [19], authors presented system-level real-time face analysis system design. The emphasis of paper is on age, gender and facial expression, but given current pandemic and widespread use of medical masks, it is important to note that paper [19] does not include facial recognition analysis of medical masks. This limitation may reduce applicability of system in real-world settings, where face masking has become common safety measure. Paper [19] does not address problem of anti-spoofing, which is important aspect in development of face recognition systems.

In [20] focus is on facial recognition, with real-time emotion recognition as distinguishing feature, but there is no discussion of problems and challenges associated with anti-spoofing and face recognition in medical masks, which are now relevant and important in context of COVID-19 pandemic.

The main objective of this study is to determine access to robotic systems based on biometrics.

The strengths of proposed method include the fact that work takes into account current trends in two-factor authentication (registration involves entering employee data from keyboard (password, login, name, title) and physiological authentication (identification by face). In second part of two-factor authentication distinctive feature is that we take into account: image of face in mask; image of face in mask in profile; image of face in tilt and anti-spoofing. These allow developed access control and management system to have more functionality, improve security and efficiency and be adapted to real-world usage scenarios.

The structure of article is structured in such way that introduction justifies relevance of research, brief review of previous research in field of access control and management systems based on biometric data. Then there is review of existing Basic decision-making models; generalized access control and management system is described; mathematical model of decision-making based on fuzzy sets is presented; process of accounting data on employees admitted to automated facility and implementation of access control system is described; explanation of fuzzy analytical hierarchy process for determining criterion weights is given; research on comparison of developed real-time identification system with analog recognition systems is conducted.

Table 1. Comparison of basic MDS models

MDS	Advantages	Disadvantages
Analytical model [21]	- easier to implement; - does not require special development tools.	- does not take into account time, dynamics, and random factors; - does not take into account complex limitations; - cannot "play" script in time.
Mathematical model [22].	- allow you to take into account all influencing factors simultaneously; - the possibility of studying each factor separately, while in reality, they act simultaneously; - the possibility of studying unrealizable processes in practice.	- in the course of disclosing all prerequisites, they are more vulnerable to criticism in comparison with analog models, in which initial points of reasoning are formulated by their creators; - the problem of determining parameters and sometimes flawed evaluation theory as a basis for constructing such models.
Physical model [23]	- physical model simplifies visual perception; - the study of phenomena that defy mathematical description; - is a more exact copy, but it costs much less than the present.	- for the new process, you need to create a new model; - The original model must frequently be physically changed or replaced to change the specifications.

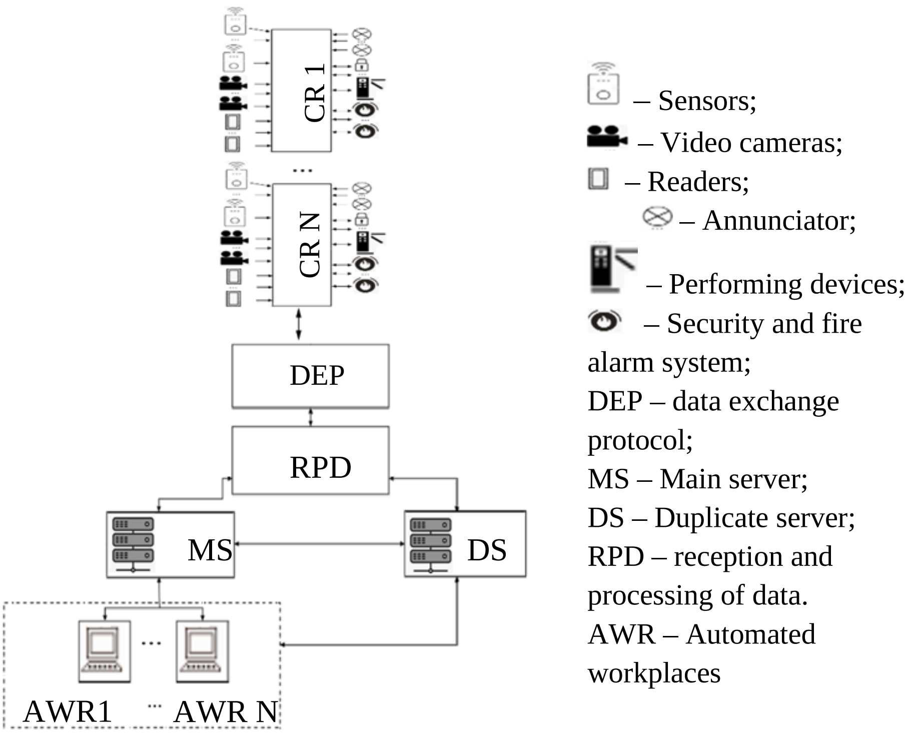


Figure. 1 Generalized ACS

2. Basic decision-making models

ACS is faced with the problem of decision-making. In the decision-making process analysis (see the first part of this study), it is determined that there are many classifications of decision-making models. The most generalized are physical, analog, and mathematical models, a comparison of which is presented in Table 1.

Structural scheme and elements of generalized control and management system of access to RS based on biometric data to decision-making

Based on the analysis above, the generalized structural scheme of ACS, which is considered in this work, can be presented in Fig. 1. Such generalized structural scheme of ACS includes:

- sensors (opening sensors – door closures, motion sensors, partitions, door status sensor, etc.);
- video cameras and video recorders;
- key readers;
- detectors (light, sound, or combined);
- actuators (turnstiles, locks, latches, reed switches, etc.);
- security and fire alarm system;
- ACS controllers;
- servers (primary (MS) and duplicate (RS));
- autonomous workplaces (AWP) (security position, ACS administrator, etc.).

Fig. 1 shows a generalized scheme. Therefore, it must be borne in mind that not all proposed elements may have ACS, and their choice depends on the task.

An important principle of ACS is to provide the possibility of comprehensive identification of users by several signs. Such signs include electronic passes and biometric indicators (fingerprint, face, iris, following hand geometry, facial thermogram, etc.).

The basic principle of the access control system is primarily access control. The system allows access only through actuators (turnstiles, locks, etc.) equipped with special equipment: sensors, video cameras, readers, controllers, terminals, and other devices that allow monitoring and recording of visitors and employees.

ACS usually consists of well-defined technical means regardless of the system and software complexity.

One of the key factors in the operation of such a comprehensive access control system is to ensure the accuracy and performance of the system.

The time of passage through actuators and the passage itself consists of scanning data, processing and transmitting data to the server, obtaining template, comparing template with received data, opening turnstile, doors, and passage.

ACS components include:

- controller (in fact, this is the system's brain), making decisions on access based on information received from a reader. Data about users with access rights are stored in a database that the controller uses to make decisions. If the request is approved, the signal from the controller opens the gate, door, or turnstile.

It is a controller with interconnection with all sensors, video cameras, readers, alarm devices, locks or turnstiles, etc.

- readers are needed in the system as intermediaries between the identifier and controller.

- actuators: gates, turnstiles, barriers, locks, and latches which, when interacting with other technical elements of the access control system, open automatically or manually if access has been permitted.

- automated workplaces – for the functioning of ACS software (Fig. 1). Sometimes workstations can consist of several computers. Within the framework of ACS, each workstation has its purpose and sometimes a specialized interface.

- master and duplicate servers. The master server (MS) monitors the status of duplicate (DS) servers and notifies you when there is no communication. For each camera, both main and backup servers can be installed. The backup server will receive data from the camera, recording and analyzing them without access to the main server.

3. Generalized model of decision-making in RS access control system

For convenience of generalized model perception, here is list of symbols: ACS – access control system; DM – decision-makers; FS – fuzzy sets; MCI – matrix matching index; RMI – random matrix index; SMI – sequential mapping index.

We formalize the choice of the best alternative when making a decision using a mathematical model in conditions of fuzzy information (fuzzy sets (FS)).

FSs are chosen because the description in the form of fuzzy sets is much less demanding on experts' qualifications and often reflects much more accurately the essence of the case and information available to decision-makers (DM).

It is proposed to express the model in the form of many alternatives:

$$X_s = \{X_1, X_2, \dots, X_n \}, \tag{1}$$

where X_n – many alternatives, n = 1,….,5 (1 – full face image (Image 1), 2 – face image in profile (Image 2), 3 – masked face image (Image 3), 4 – masked face image in profile (Image 4); 5 – the image of the face at an angle (Image 5)).

In this study, five types of alternatives were selected because:

1. Always in face recognition systems, the image is selected in full face. We've also added a profile because people sometimes stand facing the camera.
2. everyone should wear protective medical masks because it's a pandemic. For the same reasons as in paragraph 1, Image 4 has been added.
3. Image 5 has been added to ACS to improve reliability (since many facial recognition systems do not consider slopes of objects).

Let's consider what was described earlier in the structural diagram (Fig. 1) – the main factors are ensuring system accuracy and performance (speed).

Decision criteria – factors and requirements on which decision will be based, and choice of the solution – on the degree to which alternative meets a certain set of requirements, which are described by many different criteria $k_1, k_2, \dots, k_m, m = 1, \dots ,6$.

Each criterion is proposed to be met by a fuzzy set:

$$X_{S_i} = \{\mu_{k_i}(X_1), \mu_{k_i}(X_2), \dots, \mu_{k_i}(X_n)\}, \tag{2}$$

where $\mu_{k_i}(X_1)$ – evaluation of alternatives X_1 by criterion k_1 , then, $\mu_{k_i}(X_n)$ – evaluation of alternatives X_n by criterion k_i herewith $\mu_{k_i}(X_n) \in [0,1]$, that is, $\mu_{k_i}(X_n)$ – characteristic of the degree of compliance with the requirement, which is determined by criterion k_i, $i = 1, \dots, m$.

It is proposed to compare criteria according to the hierarchy analysis method since it is widely used to select a single compromise solution, considering different criteria in different areas. Calculations using this method for tasks of small dimensions can be performed even manually.

Let's describe a method of hierarchy analysis. Briefly, the essence of the technique is pairwise comparisons (k_i / k_j), DM is carried out, then an approximation of each criterion is performed.

1. Preliminary ranking of criteria, as a result of which they are arranged in descending order of importance (significance).
2. Pairwise comparison of criteria for importance on a nine-point scale with a compilation of corresponding matrix (table) of size (n x n) (table 2).

In Table 2 k_1-k_6 – criteria on basis of which decision will be made.

$a_{ij=\frac{k_i}{k_j}}$ – the intensity of hierarchy element manifestation i relative to hierarchy element j, rated on an intensity scale from 1 to 9.

Table 2. Pairwise comparison of criteria by importance

Criteria	k1	k2	k3	k4	k5	k6	Geometric mean	The value of weighting coefficients, μ_i
k1	$\frac{k_1}{k_1} = a_{11}$	$\frac{k_1}{k_2} = a_{12}$	$\frac{k_1}{k_3} = a_{13}$	$\frac{k_1}{k_4} = a_{14}$	$\frac{k_1}{k_5} = a_{15}$	$\frac{k_1}{k_6} = a_{16}$	$\frac{S_1}{6} = a_1$	$\frac{a_1}{S^*} \cdot 6 = \mu_1$
k2	$\frac{k_2}{k_1} = a_{21}$	$\frac{k_2}{k_2} = a_{22}$	$\frac{k_2}{k_3} = a_{23}$	$\frac{k_2}{k_4} = a_{24}$	$\frac{k_2}{k_5} = a_{25}$	$\frac{k_2}{k_6} = a_{26}$	$\frac{S_2}{6} = a_2$	$\frac{a_2}{S^*} \cdot 6 = \mu_2$
k3	$\frac{k_3}{k_1} = a_{31}$	$\frac{k_3}{k_2} = a_{32}$	$\frac{k_3}{k_3} = a_{33}$	$\frac{k_3}{k_4} = a_{34}$	$\frac{k_3}{k_5} = a_{35}$	$\frac{k_3}{k_6} = a_{36}$	$\frac{S_3}{6} = a_3$	$\frac{a_3}{S^*} \cdot 6 = \mu_3$
k4	$\frac{k_4}{k_1} = a_{41}$	$\frac{k_4}{k_2} = a_{42}$	$\frac{k_4}{k_3} = a_{43}$	$\frac{k_4}{k_4} = a_{44}$	$\frac{k_4}{k_5} = a_{45}$	$\frac{k_4}{k_6} = a_{46}$	$\frac{S_4}{6} = a_4$	$\frac{a_4}{S^*} \cdot 6 = \mu_4$
k5	$\frac{k_5}{k_1} = a_{51}$	$\frac{k_5}{k_2} = a_{52}$	$\frac{k_5}{k_3} = a_{53}$	$\frac{k_5}{k_4} = a_{54}$	$\frac{k_5}{k_5} = a_{55}$	$\frac{k_5}{k_6} = a_{56}$	$\frac{S_5}{6} = a_5$	$\frac{a_5}{S^*} \cdot 6 = \mu_5$
k6	$\frac{k_6}{k_1} = a_{61}$	$\frac{k_6}{k_2} = a_{62}$	$\frac{k_6}{k_3} = a_{63}$	$\frac{k_6}{k_4} = a_{64}$	$\frac{k_6}{k_5} = a_{65}$	$\frac{k_6}{k_6} = a_{66}$	$\frac{S_6}{6} = a_6$	$\frac{a_6}{S^*} \cdot 6 = \mu_6$

3. Geometric mean definition in each row of the matrix [24]:

$$a_i = \frac{S_i}{n} = \sqrt[n]{\frac{k_i}{k_1} \cdot \ldots \cdot \frac{k_i}{k_j}}, \qquad (3)$$

where n – number of criteria;

S_i – the sum $a_{ij}$of each line.

4. Determination of normalized vector of priorities.

The value of weighting coefficients is determined $\mu_i = (\frac{a_i}{S^*}) \cdot 6$, where $S^* = S_1 + \cdots + n$ – sum S_i of all rows in the matrix (Table 2).

Next, we determine a normalized approximate estimate of the local priority of a particular criterion (k_i^*) to the criterion of the highest level of hierarchy according to the formula [25]:

$$k_i^* = \frac{a_i}{\sum_{j=1,n} a_j}, \qquad (4)$$

where a_i – is intensity of hierarchy element i manifestation (according to Table 2);

a_j – is intensity of hierarchy element j manifestation (according to Table 2).

5. Check the consistency of local priorities by calculating three characteristics:

- eigenvalue of matrix (5):
- harmonization index (6);
- consistency ratio (7).

To verify the adequacy of the results obtained, you must determine the matrix matching index (MCI), maximum eigenvalue ($\mu_{max} > 0$), and sequential mapping index (SMI) according to the formula [25]:

$$\mu_{max} = \sum_{i=1,n} k_i \cdot S_i, \qquad (5)$$

where S_i – the sum of column elements with number *i* of a matrix of pairwise comparisons;

n – number of alternatives [25].

$$MCI = \frac{\mu_{max} - n}{n-1}, \qquad (6)$$

$$SMI = \frac{MCI}{RMI}, \qquad (7)$$

where RMI – random matrix index.

Based on obtained index value of sequential comparisons, it is possible to conclude the adequacy of expert assessments – the resulting indicator should not exceed 10 % for systems that do not require exceptional accuracy – 20 % [25].

The global priority of alternative is defined as sums of local priorities products of components in the path of hierarchy from the last level component to the first.

To determine the priorities of all elements in the hierarchy analysis method, a scale of expert comparisons is used with values 1, 3, 5, 7, and 9 – quantitative values, each assigned a level of importance [25].

Thus, the solution to the original problem can be represented as an alternative X_j that maximally satisfies the conditions of the entire set of criteria k_j.

Suppose A is the decisive rule for choosing the best alternative, which can be described as the definition of the corresponding FS intersection:

$$A = C_{k_1} \cap C_{k_2} \cap \ldots \cap C_{k_m}, \qquad (8)$$

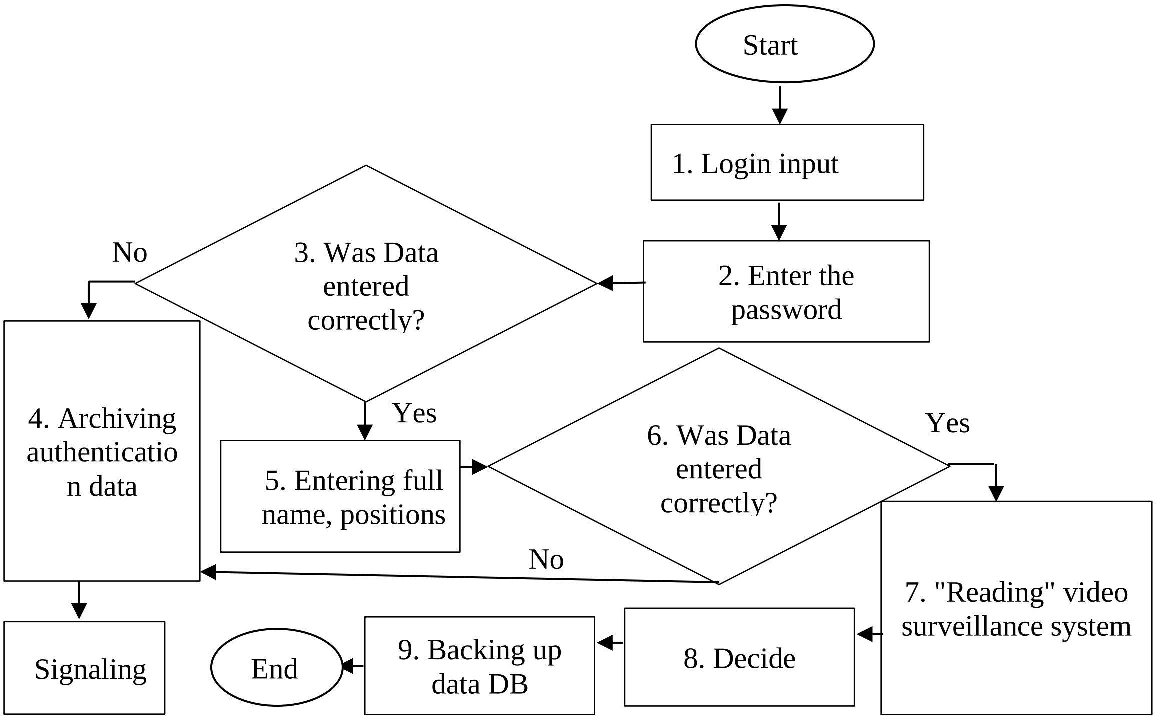

Start
1. Login input
2. Enter the password
3. Was Data entered correctly?
No
Yes
4. Archiving authenticatio n data
5. Entering full name, positions
6. Was Data entered correctly?
Yes
No
7. "Reading" video surveillance system
8. Decide
9. Backing up data DB
End
Signaling

Figure. 2 Algorithm for accounting for data about employees who are admitted to automated object

where C_{k_m} – many evaluations of alternatives.

According to the definition of the fuzzy set intersection operation, the membership function of the required solution is as follows [26, 27]:

$$\mu X_{S_A}(X_j) = \min_{i=1,n}\left(\mu X_{S_{k_i}}(X_j)\right), j = \overline{1,n}. \quad (9)$$

Hence, as the best alternative, it is necessary to choose one of the alternatives X_j^* for which the value of the membership function $\mu_\alpha(X_j)$ will be maximum.

Then, the membership function will have the form [26, 27]:

$$X_j^* = arg \max_{i=1.n}(min\{\mu X_{S_A}(X_j)\}). \quad (10)$$

This alternative is the solution to the original problem since it satisfies the requirements of the entire set of criteria under consideration as much as possible. This is if all default criteria were equal, that is, they have equal value; otherwise, to achieve a maximum objective function, a decisive rule will be formalized in the form of:

$$A = X_{S_{k_1}}^{\mu_1} \cap X_{S_{k_2}}^{\mu_2} \dots \cap X_{S_{km}}^{\mu_m}. \quad (11)$$

The sum of all coefficients must be equal to some integer, and suppose that to obtain scaled values of weightings $\sum_{i=1}^{m} \mu_i = 1$. The greater importance of the criterion, the greater value assigned to the weighting factor.

Implementation of a system for managing access to RSs based on a set of decision-making

As we described earlier, two-factor authentication is often used to increase security.

Therefore, it is proposed first to conduct registration – entering a password and login from the keyboard, and then, employee's data (surname, first name, position) and biometric approach to identification (identification by face). The algorithm of the initial step, when an employee registers to receive service that requires biometric authentication in Fig. 2.

Registration is also needed to account for data about employees admitted to the automated facility.

Let's briefly describe the registration process presented in Figure 2.

At stages 1 and 2, the employee must enter his login and password from the keyboard. Here we will be guided by ABAC restriction – allowing or denying user requests based on user attributes and object attributes, as this will allow us to implement a dynamic model for granting access, which is more flexible than the classic RBAC approach.

Stage 3. To verify that the data entry is correct. If data is incorrect, such data is unavailable on the enterprise security service's server in the database (DB), then an alarm occurs in a text message about incorrect input, and authentication data is registered

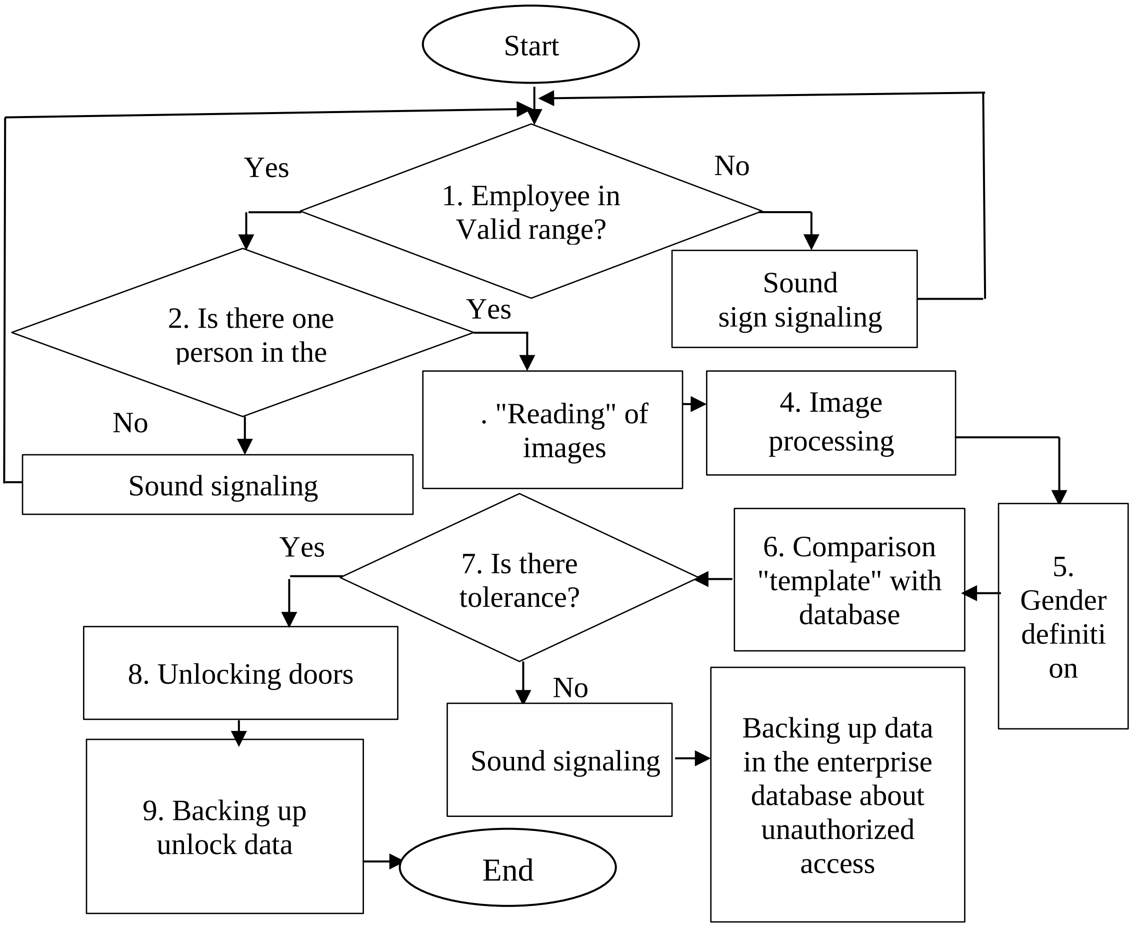

Start
Yes
No
1. Employee in Valid range?
Sound sign signaling
2. Is there one person in the
Yes
No
. "Reading" of images
4. Image processing
Sound signaling
Yes
7. Is there tolerance?
6. Comparison "template" with database
5. Gender definiti on
8. Unlocking doors
No
Sound signaling
Backing up data in the enterprise database about unauthorized access
9. Backing up unlock data
End

Figure. 3 Algorithm for implementing ACS

and archived about unauthorized login attempts.

Stage 4. If all data is entered correctly, you must enter your full name and position.

Stage 5. Verify that the data entry is correct. If data is incorrect, such data is unavailable on the server. An alarm occurs in a text message about incorrect input, registration, and archiving of authentication data about an unauthorized login attempt.

Stage 6. "Reading" of images by video surveillance system in real-time.

The camera's technical requirements govern the number of frames used and the speed at which data is sent from the camera to the computer. Each camera in a security system is typically given its channel, preventing network congestion from slowing the camera down. Since a video stream produces less data than a single image, a video camera was used to take the pictures. For instance, 200 frames make up a 10-second video clip, although 200 separate photos would provide substantially more data.

Since systems with video cameras require a minimum delay in making decisions, the system must be able to process 20 or more frames per second. However, video surveillance systems often use dozens, hundreds, and sometimes thousands of cameras.

Stages 8 and 9. Making decisions and archiving data in the company database about who was admitted and when. Since the first stage of two-factor authentication – registration has already been carried out, let's move on to the biometric approach to identification. For this study, the 2D face recognition method was chosen as a biometric approach; the corresponding algorithm for the operation of ACS is presented in Fig. 3.

The system works in real-time, as this mode is most convenient in our case; when recognized, do not need to stay long for identification, and this plays an important role in places with a large flow of people.

This system is designed for the fact that distance to door (turnstile) and distance (valid range 1,5 to 3 meters), while the employee is checking in, the camera has already "counted" (detected) face and recognized whether a person has access or not.

Taking into account the fact that the employee went to the door (turnstile) and was in the permissible zone, and passed preliminary identification for security service to confirm that registration was entered by the employee himself and not by the person to whom all data (password, login, full name and position of employee) was reported, it is necessary to conduct biometric approach to identification (BAI).

The door is connected to the controller. The door opens without checking credentials only when the button is pressed when exiting, and the "Exit by button" event is recorded in a protocol.

Step 1. Check: "Employee in valid range?"; if not, a voice message sounds: "Come closer to entrance" or "Move further away from the entrance," but often employee registers an invalid range.

Step 2. Check in the frame of one person. If not, the voice message is heard again: "Access is allowed one by one."

Step 3. "Reading" or, in simple words, detecting a person's face in 5 "positions."

Step 4. Image processing – conversion of resulting images into a form of "template" suitable for providing quick authentication of persons entitled to access RS.

Step 5. Determining characteristics of an employee is the sex of the person.

Step 6. Identification of employees occurs by comparing "template" with database data.

Step 7. Checking whether such an employee in the database is admitted to the facility. If such a person (Images) is not in the database, then sound alarm sounds, registration, and archiving of data in the database about unauthorized access occur.

Step 8. The data is transmitted to the controller, which sends a signal to the actuator (doors/turnstiles) to unlock doors.

Step 9. Archiving of data about unlocking doors (date, to whom access is granted, password, login, position).

There are three main types of algorithms: mathematical, neural network, and hybrid, based on a combination of the first two algorithms. Most modern recognition systems use algorithms built on neural networks. Neural network algorithms for face recognition are trained on large sets of photographs of people with specially marked elements in the image. The accuracy of recognition depends on the quality of the photos on which the neural network is trained. In our case, a hybrid type of face recognition was chosen, which, I more productive.

So, many alternatives for ACS are presented in Table 2, from which you must choose the best. In this instance, a "solution" is an alternative that will be "key" to the turnstile operating properly and allowing employees access to RS.

Let's rank criteria in order of their importance, where the last will be the less significant criterion: k_1, k_5, k_4, k_3, k_6, k_2, where k_1 – recognition accuracy, k_2 – identification of person gender, k_3 – anti-spoofing (ability to distinguish between a real face and graphic image of a person), k_4 – resistance to the environment (lighting), k_5 – speed, k_6 – identification of a person by facial expression (emotions)).

Table 3. Relative importance scale

Importance level	Quantitative value
Equal importance	1
Moderate superiority	3
Significant or strong superiority	5
Significant superiority	7
Significant super-priority	9

We have considered anti-spoofing for cases when an attacker uses a photo to hide his face or tries to penetrate an object using a photo of one of this object's employees.

Let's make the scale of relative importance, Table 3, based on the hierarchy analysis method [25].

Let ownership functions of ACS for each criterion be presented in Table 4 (as an example).

Earlier, we explained the significance of Image 1 to Image 5 in the study. As a part of the evaluation process, the fifth type of image was chosen as the test image to demonstrate the recognition system's stability to minor deformations, such as object rotation in the frame. Therefore, a unique aspect of our system is that while most "access control systems based on facial recognition" require a frontal view of the face relative to the camera, we included Image 5, which shows a face captured at an angle. In this study, values of weighting coefficients will be determined based on the standard procedure for pairwise comparison of criteria, as in Table 2.

Since selected criteria have different degrees of importance, the comparison is proposed to be carried out according to the hierarchy analysis method, according to which criteria are compared in pairs with each (each with each) and the relative degree of each criterion's importance in pair is determined by a 9-point system, the result will be presented in the form of comparison matrix from which we will determine relative value of each criteria importance degree for achieving the goal as whole.

The results are shown in Table 5.

Then geometric mean in each row of the matrix is determined by expression (3), and the sum of geometric means is determined by expression (5) and is equal to 12,6. In sum, let all values of weighting coefficients be equal to 1; that is, $\sum_{i=1}^{m} \mu_i = 1$.

Multiplying values of weighting factors by several criteria, which is six, because some are

Received: May 23, 2023. Revised: July 5, 2023.

Table 4. Set alternatives to ACS

Alternatives	k1	k2	k3	k4	k5	k6
	$\mu(X_1)$	$\mu(X_2)$	$\mu(X_3)$	$\mu(X_4)$	$\mu(X_5)$	$\mu(X_6)$
Image 1	0,9	0,7	0,8	0,7	0,8	0,9
Image 2	0,7	0,7	0,9	0,8	0,9	0,8
Image 3	0,7	0,6	0,9	0,5	0,7	0,4
Image 4	0,9	0,6	0,8	0,9	0,7	0,7
Image 5	0,8	0,4	0,6	0,8	0,6	0,6

Table 5. Determination of weighting coefficients by criteria

Criteria	k1	k2	k3	k4	k5	k6	Geometric mean	Value of weighting factors, μ_i
k1	1	9	5	3	3	7	4,7	0,37
k2	0,11	1	3	5	7	3	3,2	0,3
k3	0,2	0,33	1	3	3	3	1,8	0,1
k4	0,33	0,2	0,33	1	3	3	1,3	0,1
k5	0,5	0,14	0,33	0,33	1	5	1,2	0,1
k6	0,14	0,33	0,33	0,33	0,2	1	0,4	0,03

Table 6. Results of set $X_{k_i}^{\mu_i}$ formalization

Evaluation of alternative X_j, according to some criterion j=1,6	X1	X2	X3	X4	X5
$X_{S_{k_1}}^{2,2}$	0,79	0,46	0,46	0,79	0,61
$X_{S_{k_2}}^{1,8}$	0,53	0,53	0,4	0,4	0,19
$X_{S_{k_3}}^{0,6}$	0,87	0,94	0,94	0,87	0,74
$X_{S_{k_4}}^{0,6}$	0,81	0,87	0,66	0,94	0,87
$X_{S_{k_5}}^{0,6}$	0,87	0,94	0,81	0,81	0,72
$X_{S_{k_6}}^{0,2}$	0,98	0,96	0,83	0,93	0,9

evaluated as equivalent, we get weighting coefficient values that can characterize each criterion's importance. They will be equal to: $\mu_1 = 2{,}2$; $\mu_2 = 1{,}8$; $\mu_3 = 0{,}6$; $\mu_4 = 0{,}6$; $\mu_5 = 0{,}6$; $\mu_6 = 0{,}2$.

Taking into account weighting coefficients, we formalize sets, which can be represented as:

$$X_{S_{k_1}}^{2,2} = \{\langle X_1; 0{,}9^{2,2}\rangle, \langle X_2; 0{,}7^{2,2}\rangle, \langle X_3; 0{,}7^{2,2}\rangle, \langle X_4; 0{,}9^{2,2}\rangle, \langle X_5; 0{,}8^{2,2}\rangle\} = \\ =\{\langle X_1; 0{,}79\rangle, \langle X_2; 0{,}46\rangle, \langle X_3; 0{,}46\rangle, \langle X_4; 0{,}79\rangle, \langle X_5; 0{,}61\rangle\}. \quad (12)$$

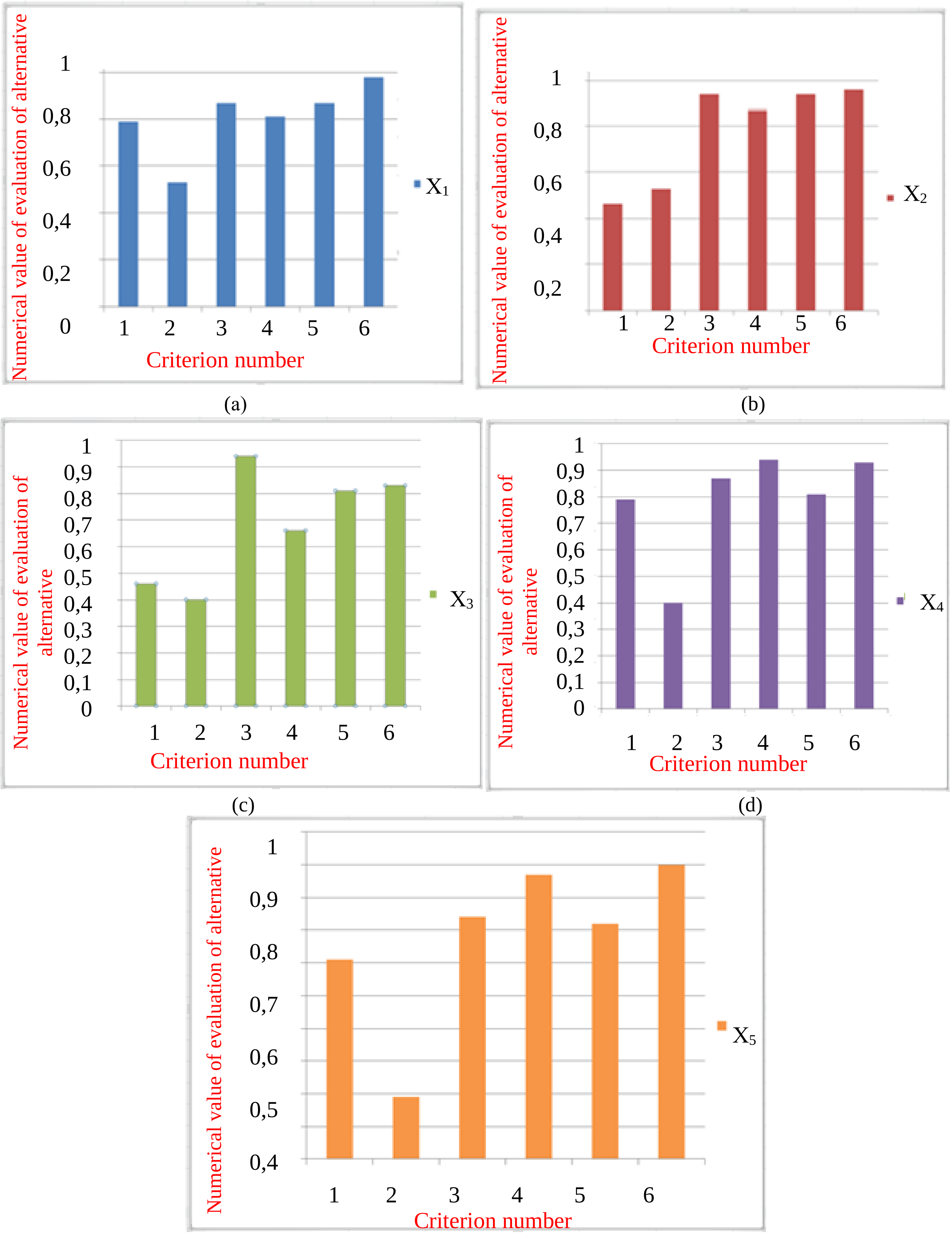
$$X_{S_{k_2}}^{1,8} = \{\langle X_1; 0{,}7^{1,8}\rangle, \langle X_2; 0{,}7^{1,8}\rangle, \langle X_3; 0{,}6^{1,8}\rangle, \langle X_4; 0{,}6^{1,8}\rangle, \langle X_5; 0{,}4^{1,8}\rangle\} = \\ =\{\langle X_1; 0{,}53\rangle, \langle X_2; 0{,}53\rangle, \langle X_3; 0{,}4\rangle, \langle X_4; 0{,}4\rangle, \langle X_5; 0{,}19\rangle\}. \quad (13)$$

$$X_{S_{k_3}}^{0,6} = \{\langle X_1; 0{,}8^{0,6}\rangle, \langle X_2; 0{,}9^{0,6}\rangle, \langle X_3; 0{,}9^{0,6}\rangle, \langle X_4; 0{,}8^{0,6}\rangle, \langle X_5; 0{,}6^{0,6}\rangle\} = \\ =\{\langle X_1; 0{,}87\rangle, \langle X_2; 0{,}94\rangle, \langle X_3; 0{,}94\rangle, \langle X_4; 0{,}87\rangle, \langle X_5; 0{,}74\rangle\}. \quad (14)$$

$$X_{S_{k_4}}^{0,6} = \{\langle X_1; 0{,}7^{0,6}\rangle, \langle X_2; 0{,}8^{0,6}\rangle, \langle X_3; 0{,}5^{0,6}\rangle, \langle X_4; 0{,}9^{0,6}\rangle, \langle X_5; 0{,}8^{0,6}\rangle\} = \\ =\{\langle X_1; 0{,}81\rangle, \langle X_2; 0{,}87\rangle, \langle X_3; 0{,}66\rangle, \langle X_4; 0{,}94\rangle, \langle X_5; 0{,}87\rangle\}. \quad (15)$$

$$X_{S_{k_5}}^{0,6} = \{\langle X_1; 0{,}8^{0,6}\rangle, \langle X_2; 0{,}9^{0,6}\rangle, \langle X_3; 0{,}7^{0,6}\rangle, \langle X_4; 0{,}7^{0,6}\rangle, \langle X_5; 0{,}6^{0,6}\rangle\} = \\ =\{\langle X_1; 0{,}87\rangle, \langle X_2; 0{,}94\rangle, \langle X_3; 0{,}81\rangle, \langle X_4; 0{,}81\rangle, \langle X_5; 0{,}72\rangle\}. \quad (16)$$

$$X^{0,2}_{S_{k_6}} = \{\langle X_1; 0{,}9^{0,2}\rangle, \langle X_2; 0{,}8^{0,2}\rangle, \langle X_3; 0{,}4^{0,2}\rangle, \langle X_4; 0{,}7^{0,2}\rangle, \langle X_5; 0{,}6^{0,2}\rangle\} =$$
$$=\{\langle X_1; 0{,}98\rangle, \langle X_2; 0{,}96\rangle, \langle X_3; 0{,}83\rangle, \langle X_4; 0{,}93\rangle, \langle X_5; 0{,}9\rangle\}. \quad (17)$$



(a)

(b)

(c)

(d)

(f)

Figure. 4 Evaluation of alternative: (a) evaluating alternative X_1, by some criteria k_1- k_6, (b) evaluating alternative X_2, by some criteria k_1- k_6, (c) Evaluation of alternative X_3, by some criteria k_1- k_6, (d) Evaluation of alternative X_4, by some criteria k_1- k_6, and (f) Evaluation of alternative X_5, by some criteria k_1- k_6

Table 7. Comparison of developed system with analog

System name	Sp Recognition speed	Ac Recognition accuracy	RL Resistance to the environment (lighting)	Advantages	Disadvantages
Proposed system	87,6 %	From 90 % before 96 %	Accuracy decreases in poor light.	Recognition in the medical mask. Rotations of the head/object are taken into account.	Errors in determining facial expressions.
Cascade Classifier and Fisherface algorithm [19]	85 %	From 81,0 % before 96,3 %	Incorrect recognition in cases of uneven lighting or low-light conditions.	Facial expression recognition.	Recognition in the medical mask was not considered, which is now very relevant in the pandemic. Rotations of the head/object were not considered. Nothing is said about anti-spoofing.
A system using convolutional neural network classifiers (CNN) [20]	87,25%	From 87,25 % before, 99,81%	Accuracy decreases in poor light.	An algorithm that works effectively with uneven rotation of lightning and the head of the subject (up to 25 °), different backgrounds, and skin tones. Six facial emotions (happiness, sadness, anger, fear, disgust, and surprise) are collected using ten virtual markers.	Recognition of medical masks was not considered. Nothing is said about anti-spoofing.

$$X_j^* = arg \underset{i=1,5}{\underline{\max}}\left(min\{\mu X_{S_A}(X_i)\}\right) =$$
$$= \{\langle X_1; 0{,}53\rangle, \langle X_2; 0{,}46\rangle, \langle X_3; 0{,}46\rangle, \langle X_4; 0{,}4\rangle, \langle X_5; 0{,}19\rangle\}.$$

The results will be presented as a matrix (Table 6).

Let's choose the minimum for each alternative (Figures 4, a, b, c, d, f).

If criteria k_j have different importance, when specifying functions belonging to alternatives to fuzzy sets $\mu_\alpha(X_j)$ on which selection is made, exponentiation operations (12-17) of belonging functions to original fuzzy sets X_S are performed. Figure 4 shows that solution to the choice problem is reduced to the definition by expression (9):

Thus, in this particular case (for our task), the best alternative to the biometric approach would be the alternative to X_1 (face 2D), having the greatest significance of membership function of resulting fuzzy set X_S of alternatives with an outstanding value of integral criterion j: $\mu X_{S_A}(X_1) = 0{,}53$.

Let's move on to comparing development with existing analog.

Comparisons will be made according to three main criteria: k_1 – recognition accuracy (Ac), k_5 – speed (Sp), and k_4 – resistance to the environment (lighting) (Rl).

As described above, the time of passage through the turnstile consists of scanning data, processing and transmitting data to the server, obtaining the template, comparing the template with received data, and opening the turnstile.

Let's compare the developed real-time identification system with a recognition system based on an artificial immune system algorithm [19] and a system using convolutional neural network (CNN) and long short-term memory (LSTM) classifiers by developing an algorithm for recognizing emotions in real-time using virtual markers through optical stream [20] (Table 7).

A set of face images containing 500 images to be used for testing recognition systems was selected as input data: face images taken under different lighting conditions, with different viewing angles. Face image recognition in medical mask was performed for our design and system number 2 in Table 7.

Indicators Sp, As and RL – are key in providing effective and secure operation of access control system based on biometric data [19, 20]. They were chosen because: recognition rate, for example, if it is high, it will allow system to make quick decisions and provides comfort and convenience for users; recognition accuracy – higher it is, less probability of false authentication or unauthorized access, and this is especially important in systems where high level of security and data protection is required; high resistance to environment ensures reliable operation of system regardless of external conditions and increases its applicability in various scenes

In general, choice of these parameters as key due to their critical role in efficiency and reliability of system.

Note: in the table, Sp refers to recognition rate, since the time of passage through ACS consists of registration time, time for scanning data, processing and transferring data to server, obtaining template, comparing template with received data, opening turnstile, doors, passage.

The main focus of this work is to consider ACS at the algorithmic level; the hardware level is planned to be disclosed in our further research.

It also shows analysis, provided that ACS is understood as simple user identification and is presented in Fig. 5. Table 8 data for the construction of Fig. 5.

As a result, Fig. 5, a is comparison of recognition rate, that is, to determine time it took to process same amount of data (set of face images containing 500 images). From Fig. 5, a shows that our system has higher rate than analogues presented in sources [19] and [20].

Since recognition rate percentage by itself does not give complete information about quality of system, let us consider Fig. 5, b and c, which presents obtained accuracy of recognition (its min and max possible values), as it is critical factor.

As a result, we aim to create system with high stability and minimization of errors in recognition process. The study was conducted with same amount of data. The minimum value of accuracy is metric of reliability and stability of recognition system (Fig. 5, b). Based on Fig. 5, b we can say that proposed system has higher minimum accuracy value than in analogues presented in sources [19, 20] and can predictably provide higher recognition reliability in wide range of scenarios and conditions.

It is proposed to conduct study with same amount of data also for maximum value of accuracy, as it is metric reflecting ability of system to achieve high level of recognition in ideal conditions. Here our system is slightly inferior to its counterparts, as it has lowest maximum accuracy value than counterparts presented in sources [19, 20], but in real conditions, such as changes in light, face pose, results may be different.

As for work [12], authors present syntactic language for access control markup, applicable to robotic systems, computational graphs, but issues related to accuracy or speed of system are not considered.

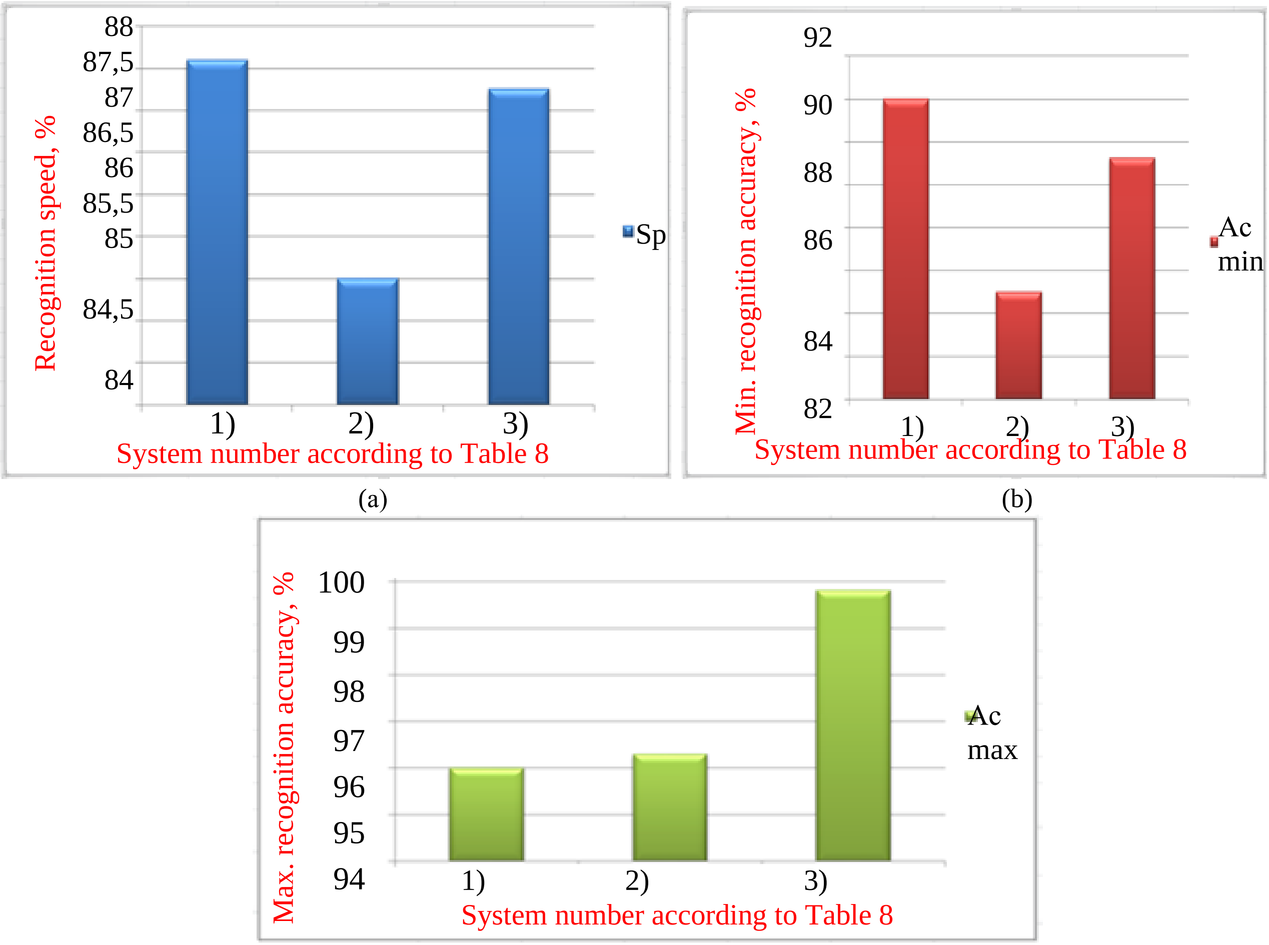
In [13] authors also consider security of access to RS, describe process of granting access; there is small description of technical means, comparison of average time spent on access control, but it is considered in terms of dependence on number of policies. The emphasis here is on extended policy-based access control (PBAC), but there is no data on accuracy of proposed method.

Based on Table 7 and Fig. 5, our development is not significant but still surpasses maximum speed; as for accuracy, it is no worse than analog, and as for environmental resistance (lighting), the system is on par with analogs.

If we compare proposed system with innovative works [17] and [18], although they achieve high accuracy and low false acceptance rate, but in these works there is no such detailed study of accuracy as in this paper, which allows us to conduct research in different conditions.

Table 8. Background data for Fig. 5

№, systems	Sp, Recognition speed, %	Ac, Min. recognition accuracy, %	Ac, Max. recognition accuracy, %
1.Proposed system	87,6	90	96
2. System [19]	85	81	96,3
3. System [20]	87,25	87,25	99,81



(a) (b)

(c)

Figure. 5 Accuracy and speed comparison charts: (a) System speed comparison chart, (b) The comparison chart on minimum accuracy of systems, and (c) Comparison chart for maximum accuracy of systems

4. Conclusion

This paper focuses on developing an access control and management system. A concise review of access control in robotic systems was conducted to provide context. The paper then presents the structural scheme and components of a comprehensive system for controlling and managing access to the robotic system based on biometric decision-making methods. In particular, the paper proposes mathematical decision-making models that rely on fuzzy sets to identify the best alternative. A fuzzy analytical hierarchy process was employed to determine the weights of the six criteria against which the options were evaluated. Notably, this study introduced an additional criterion, anti-spoofing, which measures the system's ability to distinguish between real faces and computer-generated images. The access control system to RS works in real time. The suggested solution is based on a framework for algorithmic decision-making that uses two-factor authentication to increase security. Employees must register by typing in their personal information (password, login, last name, first name, and position) on a keyboard and through physiological authentication using facial recognition. The system is made to find faces in five separate photos, including frontal and profile views with and without a mask. Despite the usual requirement for "access control systems with facial recognition" to have a frontal image of the face relative to the camera, our system's unique feature includes Image 5, which records a face at an angle. During research it was decided to choose following parameters for comparison: speed of recognition, as it affects ability to make quick decision, which is important in real time; minimum value of accuracy, as this parameter is metric of reliability and stability of recognition system and will provide greater recognition reliability in wide range of scenarios and conditions; maximum value of accuracy, as this parameter shows ability of system to achieve high recognition rate in ideal. Research was conducted on same dataset. Total, in paper gives a decision-making scenario within the access control system to show that our suggested system is better than its alternatives.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

Conceptualization, Amer Tahseen Abu-Jassar and Svitlana Sotnik; methodology, Hani Attar; software, Svitlana Sotnik; validation, Vyacheslav Lyashenko; formal analysis, Vyacheslav Lyashenko; resources, Ayman Amer; data curation, Ahmed Solyman; writing—original draft preparation, Amer Tahseen Abu-Jassar and Vyacheslav Lyashenko; writing—review and editing, Ahmed Solyman and Hani Attar.

References

[1] R. Matarneh, S. Maksymova, Z. Deineko, and V. Lyashenko, "Building robot voice control training methodology using an artificial neural net", *International Journal of Civil Engineering and Technology*, Vol. 8, No. 10, pp. 523-532, 2017.

[2] I. Nevliudov, V. Yevsieiev, J. H. Baker, M. A. Ahmad, and V. Lyashenko, "Development of a cyber design modeling declarative Language for cyber-physical production systems", *J. Math. Comput. Sci.*, Vol. 11, No. 1, pp. 520-542, 2020.

[3] J. H. Baker, F. Laariedh, M. A. Ahmad, V. Lyashenko, S. Sotnik, and S. K. Mustafa, "Some interesting features of the semantic model in Robotic Science", *SSRG International Journal of Engineering Trends and Technology*, Vol. 69(7), pp. 38-44, 2021.

[4] H. Attar, A. T. A. Jassar, V. Yevsieiev, V., V. Lyashenko, I. Nevliudov, I., and A. K. Luhach, "Zoomorphic Mobile Robot Development for Vertical Movement Based on the Geometrical Family Caterpillar", *Computational Intelligence and Neuroscience*, 2022.

[5] Y. M. A. Sharo, A. T. A. Jassar, S. Sotnik, and V. Lyashenko, "Neural Networks As A Tool For Pattern Recognition of Fasteners", *International Journal of Engineering Trends and Technology*, Vol. 69, No. 10, pp. 151-160, 2021.

[6] V. Lyashenko, F. Laariedh, A. M. Ayaz, and S. Sotnik, "Recognition of Voice Commands Based on Neural Network", *TEM Journal: Technology, Education, Management, Informatics*, Vol. 10, No. 2, pp. 583-591, 2021.

[7] E. Bertin, D. Hussein, C. Sengul, and V. Frey, "Access control in the Internet of Things: a survey of existing approaches and open research questions", *Annals of Telecommunications*, Vol. 74, pp. 375-388, 2019.

[8] V. M. Vilches, U. A. Carbajo, and E. G. Uriarte, "Industrial robot ransomware: Akerbeltz", In: *Proc. of 2020 Fourth IEEE International Conference on Robotic Computing (IRC)*, Taichung, Taiwan, pp. 432-435, 2020.

[9] H. Pu, L. He, P. Cheng, M., Sun, and J. Chen, "Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations", *IEEE Network*, Vol. 37, No. 1, pp. 111-117, 2022.

[10] K. Murugappan and T. Sree Kala, "An enhanced security framework for robotic process automation", In: *Proc. of Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, pp. 231-238, 2022.

[11] D. Servos and S. L. Osborn, "Current research and open problems in attribute-based access control", *ACM Computing Surveys (CSUR)*, Vol. 49, No. 4, pp. 1-45, 2017.

[12] R. White, H. I. Christensen, G. Caiazza, and A. Cortesi, "Procedurally provisioned access control for robotic systems", In: *Proc. of 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Madrid, Spain, pp. 1-9, 2018.

[13] Y. Zong, Y. Guo, and X. Chen, "Policy-based access control for robotic applications", In: *Proc. of 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, San Francisco, CA, USA, pp. 368-3685, 2019.

[14] B. Liu, Y. Chen, E. Blasch, K. Pham, D. Shen, and G. Chen, "A holistic cloud-enabled robotics system for real-time video tracking application", *Future Information Technology*, pp. 455-468, Springer, Berlin, Heidelberg, 2014.

[15] Y. Bouteraa, I. B. Abdallah, A. E. Mogy, A. Ibrahim, U. Tariq, and T. Ahmad, "A Fuzzy Logic Architecture for Rehabilitation Robotic Systems", *International Journal of Computers, Communications, and Control*, Vol. 15, No. 4, pp. 1-17, 2020.

[16] N. Tusing and R. Brooks, "Access Control Mechanisms and Requirements for Autonomous Robotic Fleets", *SAE Technical Paper*, No. 2023-01-0104, 2023.

[17] K. K. Coelho, E. T. Tristão, M. Nogueira, A. B. Vieira, and J. A. Nacif, "Multimodal biometric authentication method by federated learning", *Biomedical Signal Processing and Control*, Vol. 85, pp. 105022, 2023.

[18] X. Wang, W. Cai, and M. Wang, "A novel approach for biometric recognition based on

ECG feature vectors", *Biomedical Signal Processing and Control*, Vol. 86, pp. 104922, 2023.

[19] B. Adhikari, X. Ni, E. Rahtu, and H. Huttunen, "Towards a Real-Time Facial Analysis System", In: *Proc. of 2021 IEEE 23rd International Workshop on Multimedia Signal Processing (MMSP)*, Tampere, Finland, pp. 1-6, 2021.

[20] A. Hassouneh, A. M. Mutawa, and M. Murugappan, "Development of a real-time emotion recognition system using facial expressions and EEG based on machine learning and deep neural network methods", *Informatics in Medicine Unlocked*, Vol. 20, pp. 100372, 2020.

[21] A. Scheidler, A. Brutschy, E. Ferrante, and M. Dorigo, "The k-Unanimity Rule for Self-Organized Decision-Making in Swarms of Robots", *IEEE Transactions on Cybernetics*, Vol. 46, No. 5, pp. 1175-1188, 2015.

[22] A. Rimélé, M. Gamache, M. Gendreau, P. Grangier, and L. M. Rousseau, "Robotic mobile fulfillment systems: a mathematical modeling framework for e-commerce applications", *International Journal of Production Research*, Vol. 60, No. 11, pp. 3589-3605, 2022.

[23] A. S. Fadeev, A. Y. Zarnitsyn, A. V. Tsavnin, and A. S. Belyaev, "Cyber-physical system prototype development for control of mobile robots group for general mission accomplishment", In: *Proc. of AIP Conference Proceedings*, Vol. 2195, No. 1, p. 020020, 2019.

[24] C. X. B. León, D. S. S. Ferrer, P. L. I. Rey, F. J. M. Solano, and D. M. Melia, "Methodology for Pumping Station Design Based on Analytic Hierarchy Process (AHP)", *Water*, Vol. 13, No. 20, p. 2886, 2021.

[25] E. Mu and M. P. Rojas, "Understanding the analytic hierarchy process". *Practical Decision Making*, pp. 7-22, 2017.

[26] K. T. Atanassov and G. Gargov, "Intuitionistic fuzzy logic", Berlin: *Springer International Publishing*, 2017.

[27] H. T. Nguyen, C. Walker, and E. A. Walker, *A first course in fuzzy logic*, Chapman and Hall/CRC, 2018.