Fuzzy logic-based methodology for building access control systems based on fuzzy logic

Vasyl Lytvyn[1,†], Anna Bakurova[2,*,†], Oleh Zaritskyi[3,†], Anatoliy Gritskevich[2,†], Pavlo Hrynchenko[2,†], Elina Tereschenko[2,†] and Dmytro Shyrokorad[2,†]

1 Lviv Polytechnic National University, 12 Bandera Street, 79013 Lviv, Ukraine
[2] National University "Zaporizhzhia Polytechnic", 64, Zhukovsky str., Zaporizhzhia, 69063, Ukraine
[3] National Aviation University, 1, Liubomyra Huzara Ave, Kyiv, 0358, Ukraine

Abstract

The article considers topical issues of analyzing the level of risks of access control systems using the fuzzy set apparatus. This work aims to improve the efficiency of managing the access control system of the system components of IoT networks by developing a methodology that combines modern tools and methods for analyzing data and states of information systems to determine the risk level of the access control system. In the paper, the information system is considered from the point of view of system analysis as the interaction of subjects and objects of the system, the relationships between which are described by access control policies. This paper, for the first time, proposes using object vulnerability indicators and monitoring anomalies in the system to assess the risk level of the existing access control system. This approach allows to consider the real state of objects based on the system architecture and its vulnerability, changes in the system state over time, and to adjust access policies based on the level of risks assessed using the specified data. The methodology involves the use of modern tools and software, such as intrusion detection systems (IDS), fuzzy testing, User and Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), SBOM, and machine learning approaches. Relevant libraries and databases: CIS Benchmark, Common Vulnerabilities and Exposures (CVEs), Common Platform Enumeration (CPE) Dictionary, and Common Vulnerability Scoring System (CVSS) are an integral part of the methodology, ensuring standardization and integration of the methodology with other approaches and methods of controlling and monitoring information systems.

Keywords

Access control system, fuzzy logic, vulnerability scoring system

CEUR-WS.org/Vol-3723/paper7.pdf

1. Introduction

As organizations expand their use of computing servers and software, malicious insiders and attackers' technical skills increase. This has led to an increase in the number and variety of cyberattacks and advanced persistent threats, resulting in a very labor-intensive process of analyzing access control policies to ensure that overly restrictive permissions are identified and removed.

The implementation of access control policies is aimed at managing the activities of entities or subjects (users or processes performed for users) to passive entities or objects (devices, files, data, records, etc.). Several access control models are used in information systems and provide different implementations in terms of administration and enforcement of access policies: Mandatory Access Control (MAC), Discretionary access control policies (DAC), and Role-based access control (RBAC) [1].

MoDaST-2024: 6th International Workshop on Modern Data Science Technologies, May, 31 - June, 1, 2024, Lviv-Shatsk, Ukraine

vasyl17.lytvyn@gmail.com (V. V. Lytvyn); abaka111060@gmail.com (A. V. Bakurova); olegzaritskyi@gmail.com (O. V. Zaritskyi); anatolii.hrits@gmail.com (A. A. Gritskevich); horrnetss@gmail.com (P. V. Hrynchenko); elina_vt@ukr.net (E. V. Tereschenko); hoveringphoenix@gmail.com (D. V. Shyrokorad)

0000-0002-9676-0180 (V. V. Lytvyn); 0000-0001-6986-3769 (A. V. Bakurova); 0000-0002-6116-4426 (O. V. Zaritskyi); 0000-0002-7676-2808 (A. A. Gritskevich); 0000-0002-0347-0265 (P. V. Hrynchenko); 0000-0001-6207-8071 (E. V. Tereschenko); 0000-0002-2784-4081 (D. V. Shyrokorad)

© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Mandatory Access Control (MAC) is a policy suitable for information systems that are highly critical in terms of security, in which its administration and control are implemented by the central administrator of the system. MAC is a type of non-discretionary access control. MAC policy restricts the actions of entities concerning information received from objects to which they already have access.

Discretionary access control policies (DAC) are characterized by certain rules in terms of the rights and possible actions of the subject with the object. DAC can be used in combination with MAC.

Role-based access control (RBAC) is a policy for controlling access to objects and system functions based on roles (functions that correspond to the work performed) defined for each subject (user). The role-based model simplifies administration because there is no need to grant rights to each user separately; all rights are already described in the roles.

The paper aims to improve the efficiency of managing the access control system to the system components of IoT networks by developing a methodology that combines modern tools and methods for analyzing data and states of information systems to determine the risk level of the access control system. The influence of factors in the subject-object system caused by various aspects, including incorrect user actions, is considered. The methodology is based on fuzzy logic with the subsequent implementation in the MATLAB package [2, No. 41196424].

2. Related works

Analysis of recent research results has shown the active use of fuzzy mathematics methods to address security issues in various systems. This is because security factors, such as trust, sensitivity, etc., are poorly formalized. Below are some examples of developments in this area.

The authors of [3] note that an organization's access control policy does not have a standard definition of what constitutes permission with excessive rights. This situation, in their opinion, complicates the development of automated rule-based approaches. They also note that there is no universal approach to determining permissions if an employee receives more permissions than necessary, so the authors propose to determine their individual risk. The authors of the paper developed an approach using fuzzy logic to determine an overall risk rating, which can then be used to make a more informed decision about whether a user has excessive rights and poses a risk to the organization.

Article [4] addresses the issue of service providers providing users with trust-based access to protect cloud resources from intruders. The authors propose trust models based on user and service provider behavior. Fuzzy logic is used to calculate the trust values of cloud users and service providers in the cloud environment. The authors use the fuzzy Mamdani method with a Gaussian membership function for fuzzification and a triangular membership function for defuzzification. Parameters such as performance and elasticity are used to evaluate the trust of a resource.

To improve network security and obtain real-time information, [5] proposes a method for controlling access to network security authentication information based on a fuzzy reasoning algorithm. The authors use the concept of multi-level security and role inheritance to control access.

Article [6] discusses the issue of information security risk assessment in the industrial Internet of Things (IoT) environment. The authors emphasize that the assessment process is complicated by several factors: the complexity and heterogeneity of the system, the dynamic nature of the system, the distributed network infrastructure, the lack of standards and recommendations, and the increasing consequences of security breaches. Three fuzzy inference systems are used to assess information security risks in IoT: to assess the probability of a threat, to assess the probable damage, and to assess the information security risk of the IoT system.

Security management in the IoT is also addressed in [7]. It presents a fuzzy approach to trust-based access control (FTBAC) for identity management. A fuzzy approach is also used to calculate trust, which guarantees scalability and is energy efficient.

The problems of threats when using cloud services are discussed in [8]. These include insufficient identity and access management, insecure interfaces and application interfaces (APIs), theft, advanced persistent threats, data threats, etc. Traditional access control mechanisms cannot track user actions on the cloud platform and are susceptible to attacks that affect data integrity. The authors of the paper proposed a trust-based access control mechanism that analyzes user, network, demand, and security behavior data to calculate a trust value before granting access to users. The method that calculates the final trust value uses a fuzzy logic algorithm. Policies based on the trust value are defined for the access control mechanism, and based on the result of the trust value, access control is granted or denied.

In this paper, we present a generalized methodology for testing an access control system for system components of IoT networks based on fuzzy logic and the use of standardized vulnerability libraries: CIS Benchmark, Common Vulnerabilities and Exposures (CVEs), Common Platform Enumeration (CPE) Dictionary, Common Vulnerability Scoring System (CVSS).

3. Our Approach

The main concept of testing an access control system using fuzzy logic methods is outlined in the following steps.

1. Primary selection of criteria is the stage of determining the main indicators that characterize the system and, by which the risk assessment will be carried out, and subsequent grouping of these indicators. At the initial stage, the key indicators are identified through a survey of experts.
2. The table of indicators is scalable depending on the specifics of the system under test.
3. For each of the selected indicators, the current state within the system under test is assessed according to a predefined scale that determines its risk level. The number of assessment levels for each indicator depends on the system's specifics and heterogeneity.
4. Calculations based on the fuzzy inference system for assessing the risk of granting access to a user.

3.1. Subject-object model of the information system

The subject-object model of an information system is considered from the perspective of system analysis and can be represented by the components described below.

A subject is an entity that interacts with the system and is endowed with certain rights to perform actions with system objects, for example, a system user or a process. A subject is characterized by the degree of trust in its qualifications and actions in the system.

An object is an entity (often a resource) represented by elements of an information system that are also characterized by their attributes. Objects include software, file systems, services, hardware, such as IoT sensors, etc. All objects are characterized by the ability to interact with them (change, add, update, etc.).

Access control policy determines the level of communication between the object and the subject, which is described by the Access Control List (ACL) indicator.

The "Subject" element of the model is described by the following groups of indicators.

1. Password management level (PML).
2. Strong customer authentication (SCA). SCA is a technical standard for an authentication system [9,10].
3. Availability and level of access to the object (services, equipment) (Access control list, ACL). It is determined by the access rights matrix. The access control list describes the levels of permissions (access rights) that subjects (users) have to system objects. The following

levels of access rights are defined. Read (R) - the subject has the right only to view objects determined by the nature of his work. Add (A) - the subject has the right to add or create objects in the system, for example, new files in the database, data in the enterprise resource planning system, etc. Delete (D) - the subject has the right to delete objects from the system or move them. Edit (E) - the subject has the right to change both the objects themselves and their attributes and to create versions of objects. Privilege (P) - the subject has full rights and can perform any actions with the object in the system, including updating firmware and software, managing the rights of other subjects, etc. The permission (PRM) indicator is considered to model access rights.

4. Abnormal user behavior in the system. The indicator is determined by systems that monitor user activity and detect abnormal states in the system, such as IDS, UEBA systems, and systems using ML.

The Object element of the model is considered at several levels, the first is the network level, and the second is the hardware and software level, which involves auditing systems and building SBOM.

1. Object vulnerability level (OVL). The indicator is determined based on the results of penetration tests, Fuzz testing systems, and analysis of relevant databases, such as the Common Vulnerability Scoring System (CVSS) [11].
2. The frequency of access to the object (Object access frequency, OAF) by system entities. The indicator is calculated using data from the UAM and UEBA logging systems as the ratio of the number of accesses to an object to the total number of accesses to all objects in the system.
3. Level of object dependency/influence (LOD/I) on other system objects. The indicator is assessed by the CVSS metrics and affects the overall vulnerability assessment in the Common Vulnerability Scoring System (CVSS).
4. Data sensitive levels (DSL). In the Critical Sensitivity Level**,** we group the frequency of requests, the sensitivity of the object, and the impact on other objects, which is the basis for assessing vulnerability by the degree of sensitivity of information or service and taking this into account when determining the OVL. For example, The European Union General Data Protection Regulation (GDPR) came into effect in 2018, affecting privacy and data protection practices globally. Data classification with the GDPR uses the four data classification levels: public data, internal data, confidential data, and restricted data. In addition to using these levels, the GDPR requires companies to delete any data that is unnecessary or not being used, so it is important to understand what types of unstructured data your business possesses.
5. Characterization of a network (system) in terms of its type (Network type, NT): Personal Area Network (PAN), Local Area Network (LAN), Campus Area Network (CAN), Wide Area Network (WAN), Global Area Network (GAN). From the point of view of its security: public unprotected (Open); protected, for example, with a VPN (Virtual Private Network); closed, physically limited, without access to the world wide web (Closed). The Network Characteristics indicator is used to refine the “Attack Vector” Base Matric Group indicator by considering the actual architecture of the enterprise network in the “Attack Vector” Modified Base Matric Environmental Matric Group indicator.
6. Network Anomaly (NA). Determined using intrusion detection and anomaly monitoring systems, such as Snort, Wazuh, and Federated learning methodologies (BACON network anomaly detection), etc.

All these indicators affect the two main ones that determine the degree of risk of the access granted.

1. Attack Likelihood (AL) is an assessment of the possibility that an entity will attempt to exploit an object's vulnerabilities, taking into account the impact of the entity's reliability indicators, the depth and privileges of its access, as well as the degree of network closure, the possible attack vector and the history and maturity of potential abuses in the network under test.
2. Attack severity level (ASL). It is the main indicator for the object in the methodology. The maximum value of the indicator indicates catastrophic consequences for the IT structure, enterprise, or organization. We evaluate it using the Common Vulnerability Scoring System

(CVSS) scale as a fairly universal template for assessing security vulnerabilities and use the Base Temporal Environmental methodology to refine the assessment.

Fig. 1 shows the structure of the relationships between the described indicators of the access control testing system, considering the dynamics, dependencies, and impact on the risk of granting access. The outer contour of the scheme determines the possibility of risk assessment without additional analysis of the behavior of the structure's Objects and Subjects before/after/during the granting of access, which, together with the evaluation of the risk of the granted access, will give a dynamic risk assessment.

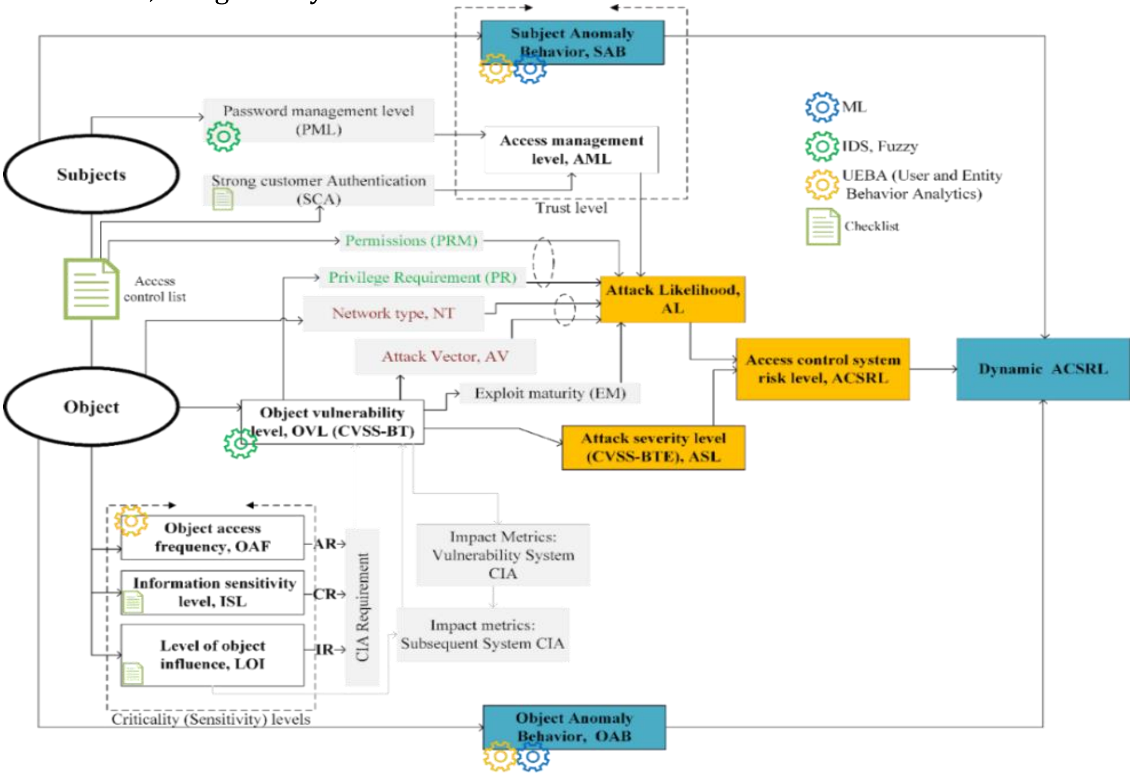
Subject Anomaly Behavior, SAB
Password management level (PML)
Access management level, AML
Subjects
Strong customer Authentication (SCA)
Trust level
ML
IDS, Fuzzy
UEBA (User and Entity Behavior Analytics)
Checklist
Permissions (PRM)
Access control list
Privilege Requirement (PR)
Attack Likelihood, AL
Network type, NT
Attack Vector, AV
Access control system risk level, ACSRL
Dynamic ACSRL
Object
Exploit maturity (EM)
Object vulnerability level, OVL (CVSS-BT)
Attack severity level (CVSS-BTE), ASL
Object access frequency, OAF
AR
Information sensitivity level, ISL
CR
Level of object influence, LOI
IR
CIA Requirement
Impact Metrics: Vulnerability System CIA
Impact metrics: Subsequent System CIA
Criticality (Sensitivity) levels
Object Anomaly Behavior, OAB

Figure 1: Structure of relationships between access control testing system indicators

The main target indicator of the Object-Subject model is the risk level (in percentage terms) (Access control system risk level). The risk level is calculated using intermediate and additional indicators that characterize the impact on the main indicators of the Object-Subject system.

1. Access management level (AML) is a parameter that is calculated according to the relevant rules of the knowledge base using the Password management level (PML) and Strong Customer Authentication (SCA) parameters.
2. The combination of Privilege Requirement (PR) and Permissions (PRM) indicators significantly affects the probability of an attack if an attacker gains access to the system with the appropriate rights.
3. The Network type (NT) indicator modifies the Attack Vector (AV) metric, affecting the probability of an attack.
4. When calculating the impact of the network architecture on the attack vector, the state of network security must be taken into account, and the probability indicators must be adjusted.

The general concept of the methodology for testing the system of access control to the system components of the IT structures of the information system is shown in Fig. 2

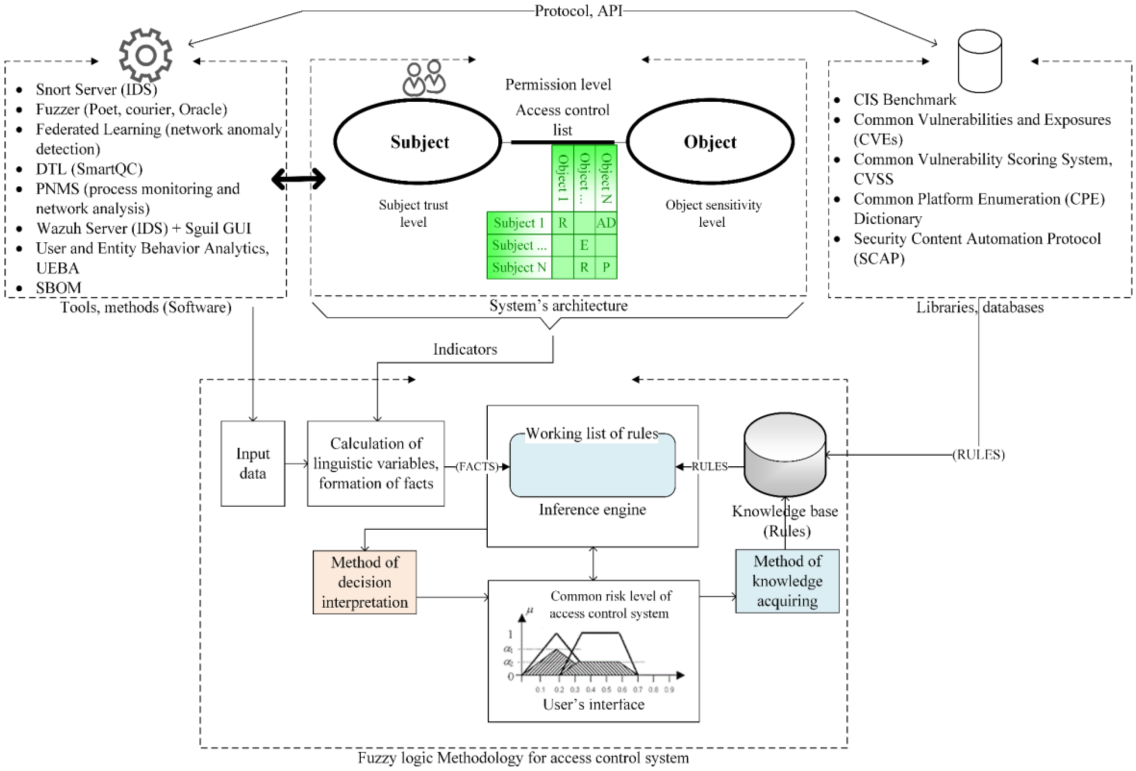
Protocol, API
Snort Server (IDS)
Fuzzer (Poet, courier, Oracle)
Federated Learning (network anomaly detection)
DTL (SmartQC)
PNMS (process monitoring and network analysis)
Wazuh Server (IDS) + Sguil GUI
User and Entity Behavior Analytics, UEBA
SBOM
Tools, methods (Software)
Permission level
Access control list
Subject
Object
Object 1
Object ...
Object N
Subject 1
Subject ...
Subject N
R
AD
E
R
P
Subject trust level
Object sensitivity level
System's architecture
CIS Benchmark
Common Vulnerabilities and Exposures (CVEs)
Common Vulnerability Scoring System, CVSS
Common Platform Enumeration (CPE) Dictionary
Security Content Automation Protocol (SCAP)
Libraries, databases
Indicators
Input data
Calculation of linguistic variables, formation of facts
(FACTS)
Working list of rules
Inference engine
RULES
Knowledge base (Rules)
(RULES)
Method of decision interpretation
Common risk level of access control system
μ
1
α1
α2
0
0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9
User's interface
Method of knowledge acquiring
Fuzzy logic Methodology for access control system

Figure 2: Загальна концепція методології тестування системи контролю доступу

We've covered the first three steps of the main testing concept. Now, let's move on to the fourth step, which involves building a product model.

3.2. Product model of the access control system testing methodology

The input data of the fuzzy inference product system are the facts of certain system states obtained at certain discrete points in time and dynamic indicators, taking into account the results of continuous monitoring of anomalies in the system, which are provided by modern tools and software, such as intrusion detection systems (IDS), fuzz testing, User and Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), SBOM. Input data is fuzzified based on a predefined Permission level access control list. The knowledge base is formed considering standardized requirements for the security of information systems, such as CIS Benchmark, Common Vulnerabilities and Exposures (CVEs), Common Platform Enumeration (CPE) Dictionary, and Common Vulnerability Scoring System (CVSS). The use of appropriate libraries and databases ensures standardization and integration of the methodology with other approaches and methods of control and monitoring of information systems.

The hierarchical structure of the developed fuzzy inference system is shown in Fig. 3.

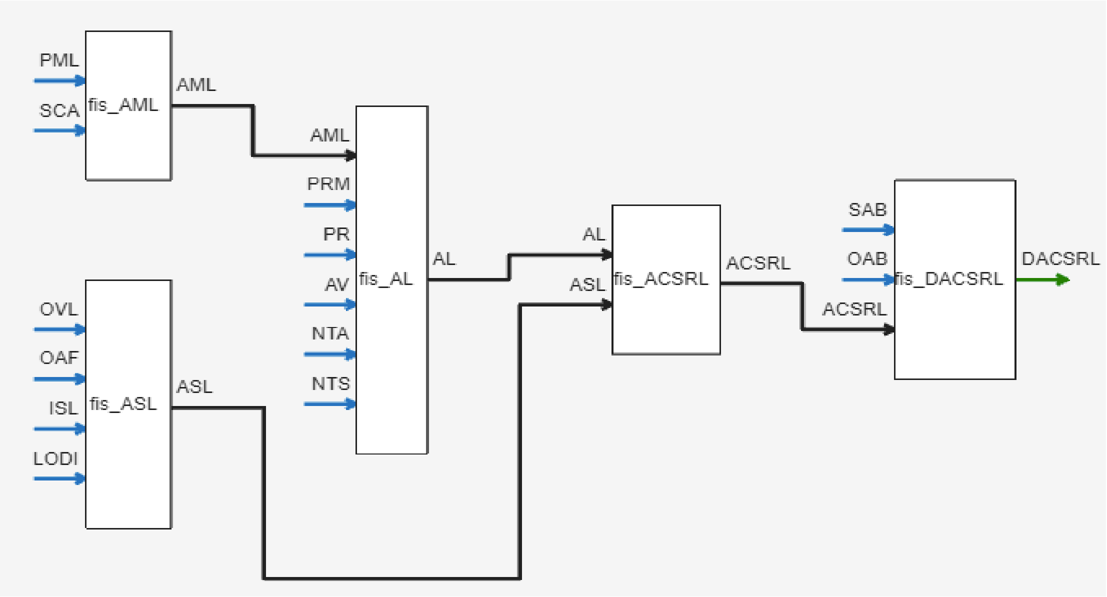

Figure 3: Structure of the fuzzy inference system

The product system's output linguistic variable is the Dynamic Access control system risk level DACSRL, which consists of the static component ACSRL and takes into account the impact of abnormal behavior of the subject (SAB) and object (OAB).

4. Experiments

The purpose of our demonstration experiment is to obtain the Access control system risk level ACSRL as a result of fuzzy inference according to the values of a certain subset of input parameters shown in Fig. 3.

Let's build a fuzzy product system for Access control system risk level ACSRL for the input parameters OVL, PML, SCA, PRM, and PR, the block diagram of which is shown in Fig. 4. According to this block diagram (Fig. 4), ACSRL is the result of products based on the input parameters AL and ASL. From the input parameters selected for the demonstration experiment, we consider the influence of AML (which is formed by PML and SCA), PRM, and PR on AL. The ASL parameter is determined by OVL.

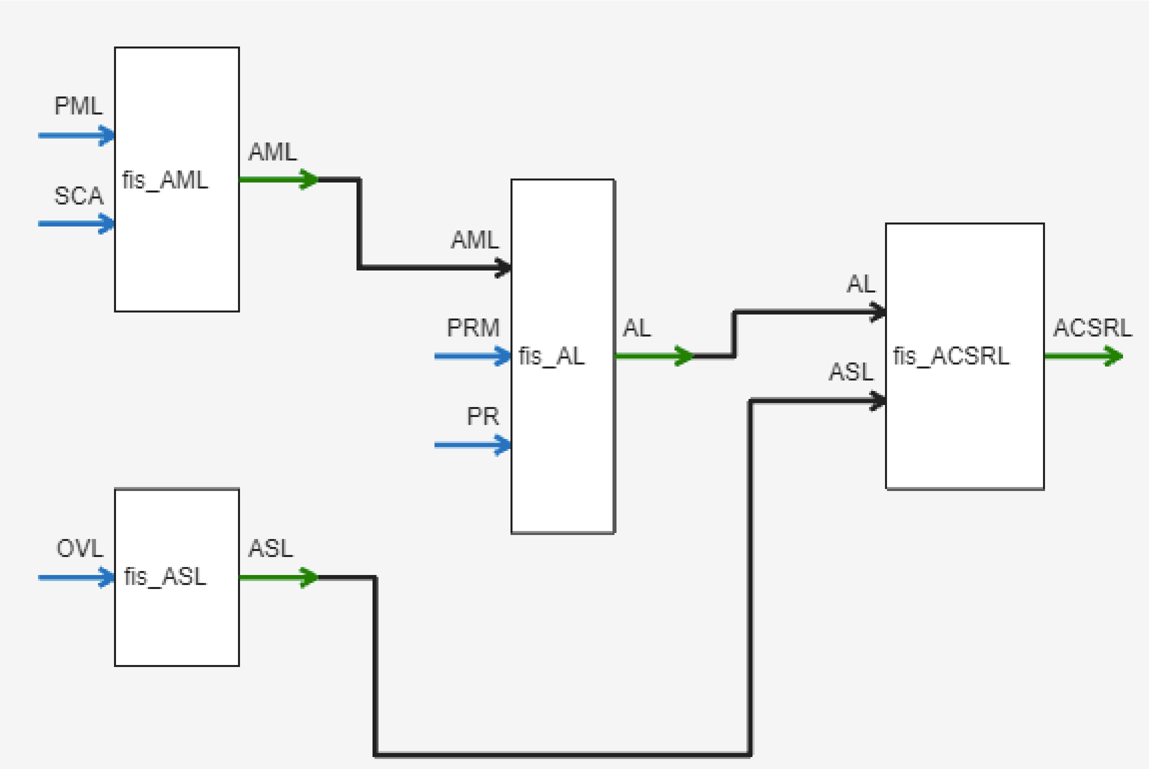

Figure 4: Structure of the fuzzy inference product system implemented in the experiment

To assess the Access control system risk, we introduce the corresponding linguistic variable ACSRL of the product system, the terms and membership functions of which are defined in Table 1, according to [12].

Table 1
Linguistic variable Access control system risk level

ACSRL terms	The membership function of terms
Very high (VH)	s (70 90)
High (H)	Pi (50 65 82 90)
Substantial (S)	Pi (30 42 58 70)
Possible (P)	Pi (10 18 35 50)
Slight (S)	s (10 30)

The corresponding membership functions are shown in Fig. 5.

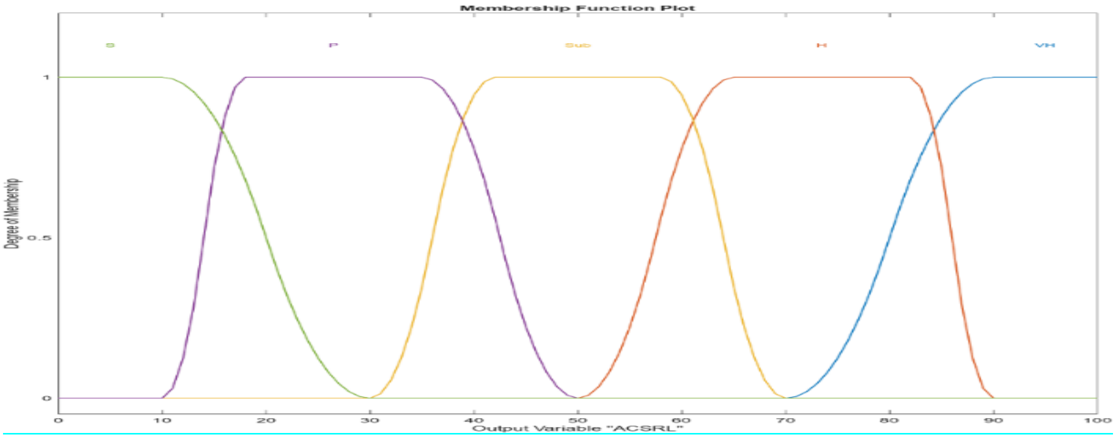

Figure 5: Access control system risk level membership function

According to the block diagram (Fig. 4), ACSRL is the result of products based on the input parameters ASL and Attack likelihood AL.

For the demonstration experiment, we assume that the ASL parameter is determined by the Object vulnerability level (OVL). Object vulnerability level, OVL, is determined by the results of penetration tests, fuzz testing systems, and analysis of relevant databases, such as the Common Vulnerability Scoring System (CVSS) [11]. The terms of the OVL are defined in Table 2. For the demonstration experiment, we assume that the OVL parameter is set to High.

Table 2
Linguistic variable Object vulnerability level, OVL

Terms.	Scale	The membership function of terms
Low, L	(0,1 - 3,9)	z (0 4)
Medium, M	(4,0 - 6,9)	PI (2 3 6,9 8)
High, H	(7,0 - 8,9)	PI (5 7 8,9 9,5)
Critical, C	(9,0 -10,0)	s (9 10)

To evaluate Attack likelihood, we introduce the corresponding linguistic variable Attack likelihood (AL). The terms and membership functions of the Attack likelihood AL are defined in Table 3. They correspond to the introduced levels of attack assessment [13].

Table 3
Linguistic variable Attack likelihood AL

Term.	Probability	Comment	The membership function of terms
Very high | Very likely (VL)	0,8 - 1,0	Not Defined	s (0,8 0,9)
High | Likely (L)	0,64 - 0,79	Attacked	PI (0.63 0.64 0.79 0.84)
Average | Possible (P)	0,37 - 0,63	Proof-of-Concept	PI (0.36 0.37 0.63 0.69)
Low | Unlikely (UL)	0,20 - 0,36	Unreported	PI (0,1 0,2 0,36 0,42)
Very low | Impossible (IMP)	0 - 0,19	Unreported	z (0 0,2)

From the input parameters selected for the demonstration experiment, we will consider the impact of AML, PRM, and PR on AL. Let's introduce the Access management level (AML) with the terms and membership functions presented in Table 4.

Table 4
Linguistic variable Access management level (AML)

Terms.	The membership function of terms
Low, L	z (2.5 4)
Average, A	PI (2 3 5 7)
High, H	s (6 7)

The access management level (AML) is calculated according to the knowledge base's product rules using the Password management level and Strong Customer Authentication (SCA) parameters of the Subject model element indicator group.

To describe the linguistic variable Password management level (PML), we calculated the weighting coefficients of the password management parameters using pairwise comparisons and obtained the following characteristics (Table 5). The total number of points obtained by the password management system is calculated as the sum of the weighting coefficients of the activated parameters, which take values from 0 to 10.

Table 5
Weight characteristics of password management parameters

Indicator	Code	Active, a_i	Score, s_i
Reset account lockout counter after	RAL	Yes (1) | No (0)	0,41
Minimum password age	MPA	Yes (1) | No (0)	0,61
Account Lockout Duration	ALD	Yes (1) | No (0)	0,61
Maximum password age	MPA	Yes (1) | No (0)	0,75
Enforce password history	EPH	Yes (1) | No (0)	0,87
Account Lockout Threshold	ALT	Yes (1) | No (0)	1,11
Minimum password length	MPL	Yes (1) | No (0)	1,16
Password must meet complexity requirements	PCR	Yes (1) | No (0)	2,07
Store passwords using reversible encryption	SPE	Yes (1) | No (0)	2,41
Common score			10,00

The linguistic variable characterizing the level of password management takes values described by terms in a three-digit scale with corresponding membership functions, which are presented in Table 6 and Figure 6.

Table 6
Linguistic variable Password management level (PML)

Terms.	The membership function of terms
Low, L	z (2.5 4)
Average, A	PI (2 3 5 7)
High, H	s (6 7)

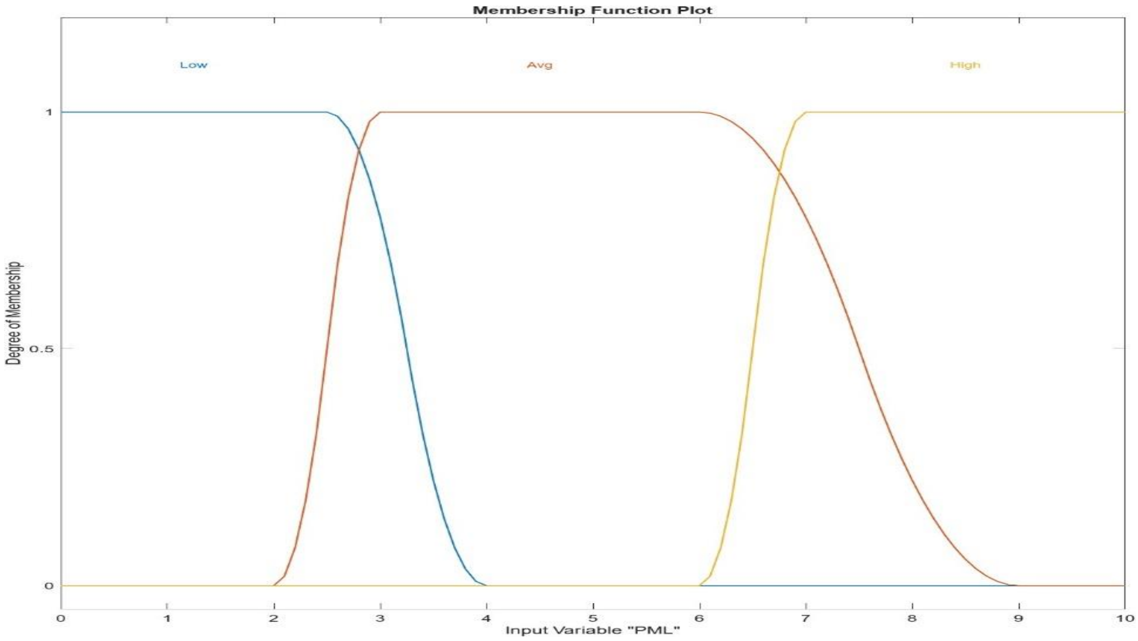

Figure 6: Membership function Password management level

The construction of Strong customer authentication (SCA) is based on the requirements of the recently updated NIST Digital Identity Guidelines4 (SP 800-63-3) standard [14], which standardizes the definition and assigns levels of assurance (security) for various authentication solutions Authenticator Assurance Level (AAL). Table 7 shows the correspondence between the AAL assurance levels and the introduced terms of Strong customer authentication (SCA).

Table 7
Linguistic variable Strong customer authentication (SCA)

Terms. SCA	The membership function of terms	Comment type
AAL-1	s (6 8)	PW (provided by client, server) - SF
AAL-2	PI (2 5)	PW (provided by client, server) + SF-OTP|OOB-SW|D or MF
AAL-3	z (2 4)	MF - Crypto - Device

In Table 7, the following abbreviations are used: PW - direct password, SF - Single factor - activation not required, MF - Multi-factor - PIN/password or Biometric Activation (MF), OTP - one-time password, OOB - Out-of-Band, SW - Software, D - Device.

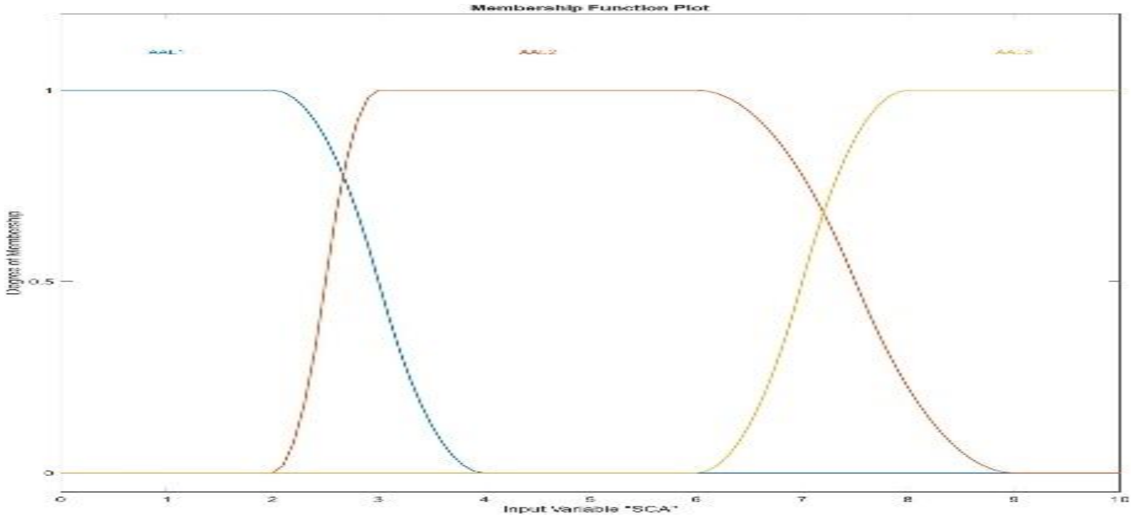

Figure 7: Membership function Strong customer authentication (SCA)

The introduced linguistic variables of the Password management level and Strong Customer Authentication (SCA) indicators allow us to build a fuzzy productive inference to determine the linguistic variable Access management level (AML) according to rules 1-9:

If PML is Low and SCL is AAL1 then AML is H 1 rule1,
If PML is High and SCL is AAL3 then AML is L 1 rule2,
If PML is Low and SCL is AAL2 then AML is H 1 rule3,
If PML is Low and SCL is AAL3 then AML is A 1 rule4,
If PML is Avg and SCL is AAL1 then AML is H 1 rule5,
If PML is Avg and SCL is AAL2 then AML is A 1 rule6,
If PML is Avg and SCL is AAL3 then AML is A 1 rule7,
If PML is High and SCL is AAL1 then AML is A 1 rule8
If PML is High and SCL is AAL2 then AML is A 1 rule9.

Fig. 8 shows the corresponding response surface for the output of the block defining the linguistic variable Access management level (the first level of the hierarchical system).

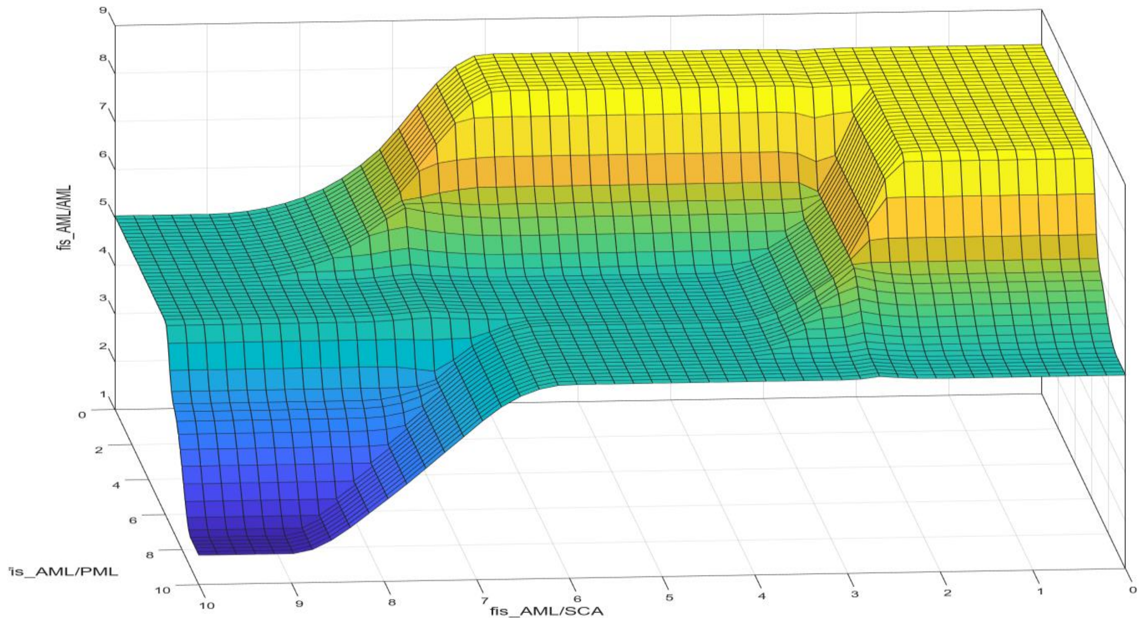

Figure 8: AML fuzzy inference surface from PML and SCL parameters

For the Privilege Requirement (PR) indicator, we select the terms according to the description in [11], presented in Table 8.

Table 8
Linguistic variable Privilege Requirement (PR)

PR terms	Definition	The membership function of terms
None(N)	The attacker is unauthenticated prior to the attack and, therefore, does not require any access to the settings or files of the vulnerable system to carry out an attack	z (2.5 4)
Low (L)	The attacker requires privileges that provide basic capabilities that are typically limited to settings and resources owned by a single low-privileged user. Alternatively, an attacker with low privileges has the ability to access only non-sensitive resources	PI (2 3 5 7)
High (H)	The attacker requires privileges that provide significant (e.g., administrative) control over the vulnerable system, allowing full access to the vulnerable system's settings and files.	s (6 7)

The Permissions (PRM) has terms of type string (Read (R), Add (A), Delete (D), Edit (E), Privilege (P)), for which membership functions are constants.

Table 9 presents the impact of the combination of Access management level (AML) (Table 4) and a pair of indicators, Privilege Requirement (PR) & Permissions (PRM), on the level of an Attack likelihood (AL) (Table 3) if an attacker gains access to the system with the appropriate rights. This information is the basis for building fuzzy product rules.

Table 9
Attack likelihood (AL) dependence on AML&PR&PRM

	AML	Privilege (PR)	Requirement	Permissions (PRM)	Terms Attack likelihood (AL)
1	L	None(N)		Read (R)	Low | Unlikely (UL)
2	L	None(N)		Add (A)	Average | Possible (P)
3	L	None(N)		Delete (D)	Average | Possible (P)
4	L	None(N)		Edit (E)	Average | Possible (P)
5	L	None(N)		Privilege (P)	high | likely (L)
6	H	None(N)		Read (R)	Very low | Impossible (IMP)
7	H	None(N)		Add (A)	Very low | Impossible (IMP)
8	H	None(N)		Delete (D)	Low | Unlikely (UL)
9	H	None(N)		Edit (E)	Low | Unlikely (UL)
10	H	None(N)		Privilege (P)	Low | Unlikely (UL)
11	H	Low (L)		Read (R)	Low | Unlikely (UL)
12	H	Low (L)		Add (A)	Low | Unlikely (UL)
13	H	Low (L)		Delete (D)	Low | Unlikely (UL)
14	H	Low (L)		Edit (E) or Privilege(P)	Average | Possible (P)
15	H	High (H)		Read (R)	Low | Unlikely (UL)
16	H	High (H)		Add (A)	Average | Possible (P)
17	H	High (H)		Delete (D)	Average | Possible (P)
18	H	High (H)		Edit (E)	Average | Possible (P)
19	H	High (H)		Privilege (P)	high | likely (L)
20	L	Low (L)		Read (R)	Average | Possible (P)
21	L	Low (L)		Add (A)	Average | Possible (P)
22	L	Low (L)		Delete (D)	high | likely (L)
23	L	Low (L)		Edit (E) or Privilege(P)	high | likely (L)
24	L	High (H)		Read (R)	high | likely (L)
25	L	High (H)		Add (A)	high | likely (L)
26	L	High (H)		Delete (D)	high | likely (L)
27	L	High (H)		Edit (E)	Very high | Very likely (VL)
28	L	High (H)		Privilege (P)	Very high | Very likely (VL)
29	A	Low (L)		Read (R)	Low | Unlikely (UL)
30	A	Low (L)		Add (A)	Low | Unlikely (UL)
31	A	Low (L)		Delete (D)	Average | Possible (P)
32	A	Low (L)		Edit (E) or Privilege(P)	Average | Possible (P)
33	A	High (H)		Read (R)	Average | Possible (P)
34	A	High (H)		Add (A)	Average | Possible (P)
35	A	High (H)		Delete (D)	high | likely (L)
36	A	High (H)		Edit (E)	high | likely (L)
37	A	High (H)		Privilege (P)	high | likely (L)

Fragment of fuzzy product rules for a certain level of the output variable of the second block AL:

If AML is L and PRM is R and PR is N then AL is UL 1rule1
If AML is L and PRM is A and PR is N then AL is P1rule2
If AML is L and PRM is D and PR is N then AL is P1rule3
If AML is L and PRM is E and PR is N then AL is P1rule4
If AML is L and PRM is P and PR is N then AL is L1rule5
…
If AML is H and PRM is R and PR is N then AL is IMP 1rule41

If AML is H and PRM is A and PR is N then AL is IMP 1rule42
If AML is H and PRM is D and PR is N then AL is UL1rule43
If AML is H and PRM is E and PR is N then AL is UL1rule44
If AML is H and PRM is P and PR is N then AL is UL1rule45

The corresponding response surface for the output of the second block, which determines the linguistic variable Attack likelihood (AL) in the PRM & PR space, is shown in Fig. 9.

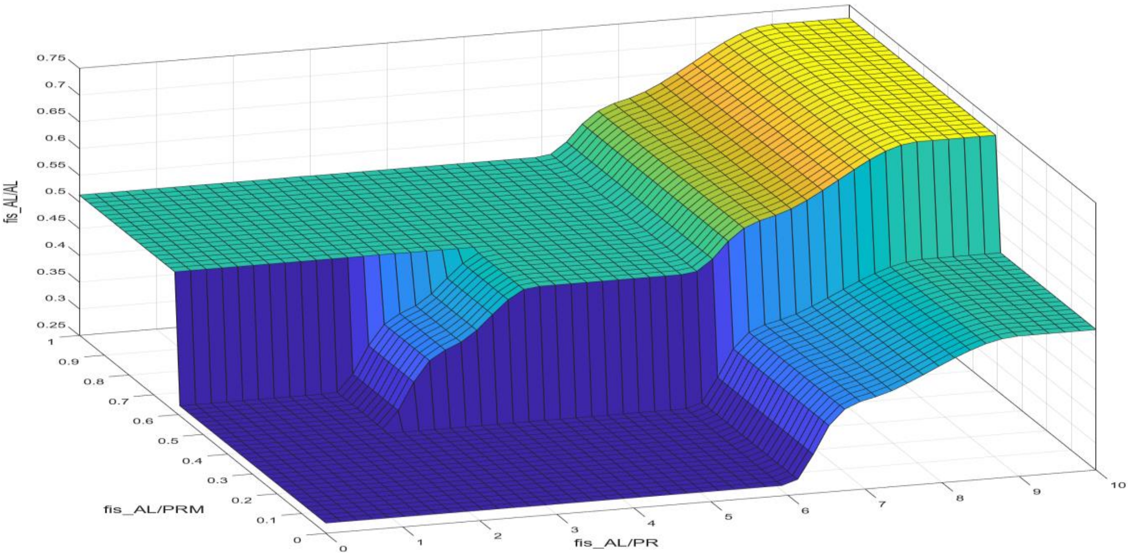

Figure 9: AL fuzzy inference surface from the parameters PRM & PR

The introduction of AL and ASL defined by OVL allows us to build a fuzzy product inference of the ACSRL output parameter according to the rules formed based on Table 10.

Table 10
Output linguistic variable ACSRL dependence on AL&ASL

	Terms Attack likelihood (AL)	ASL defined by OVL	ACSRL
1	Very high | Very likely (VL)	high	High
2	High | Likely (L)	high	High
3	Average | Possible (P)	high	Substantial
4	Low | Unlikely (UL)	high	Substantial
5	Very low | Impossible (IMP)	high	Possible
6	Very high | Very likely (VL)	Critical	Very High
7	High | Likely (L)	Critical	High
8	Average | Possible (P)	Critical	High
9	Low | Unlikely (UL)	Critical	Substantial
10	Very low | Impossible (IMP)	Critical	Substantial
11	Very high | Very likely (VL)	Low	Substantial
12	High | Likely (L)	Low	Possible
13	Average | Possible (P)	Low	Possible
14	Low | Unlikely (UL)	Low	Slight
15	Very low | Impossible (IMP)	Low	Slight
16	Very high | Very likely (VL)	Medium	High
17	High | Likely (L)	Medium	Substantial
18	Average | Possible (P)	Medium	Substantial
19	Low | Unlikely (UL)	Medium	Possible
20	Very low | Impossible (IMP)	Medium	Possible

Fragment of the rules of the third level knowledge base of the hierarchical fuzzy products of the built ACSRL evaluation system:

If (AL is VL) and (ASL is High) then (ACSRL is H) (1)

If (AL is L) and (ASL is High) then (ACSRL is H) (1)

If (AL is P) and (ASL is High) then (ACSRL is Sub) (1)

If (AL is UL) and (ASL is High) then (ACSRL is Sub) (1)

If (AL is IMP) and (ASL is High) then (ACSRL is P) (1)

Figure 10 shows the fuzzy inference surface of ACSRL from the AML/PML and AL/PR parameters.

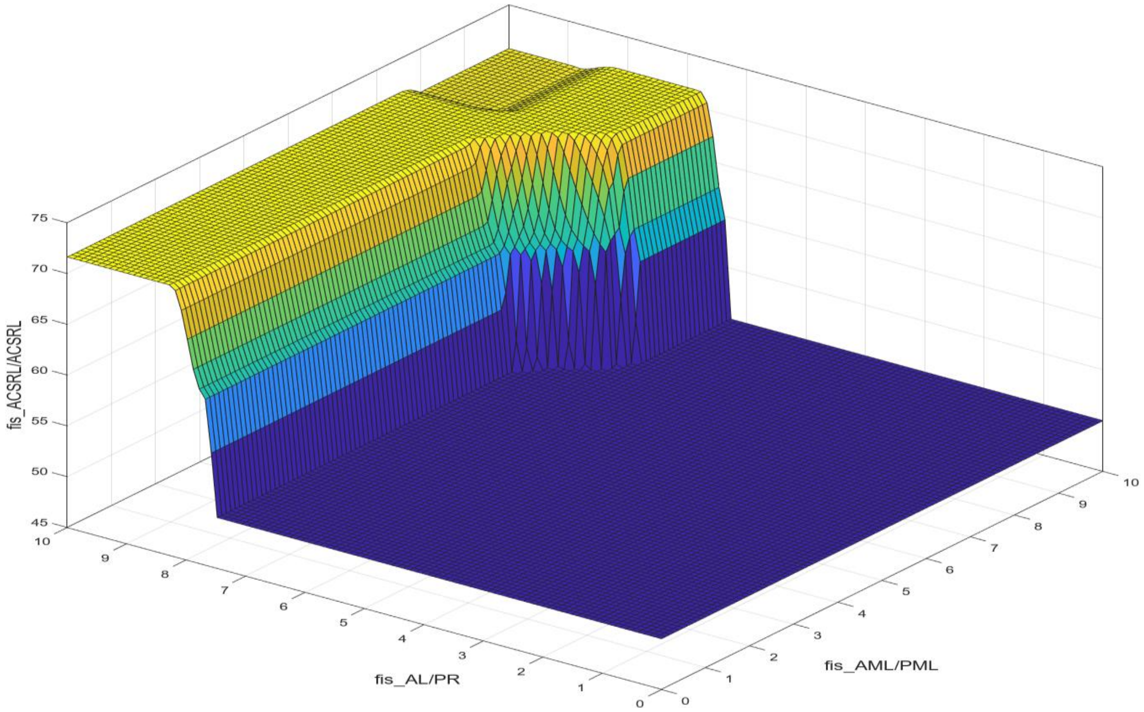

Figure 10: ACSRL fuzzy output surface from AML/PML and AL/PR parameters

According to Fig. 10, we can see that the presented system allows for the assessment of the access control system risk level exceeding 50%. This restriction is artificial, as it appeared in the conditions of the demonstration experiment with restrictions on the OVL parameter, which was set to high. This means that only the first five rules from Table 10 were entered.

5. Discussions

By combining modern network control tools, up-to-date vulnerability libraries, and comprehensive analysis of IT infrastructure data using fuzzy logic, a more objective and effective risk assessment is achieved compared to other existing approaches and methodologies or to analysis in the absence of any of these components.

The test results of the proposed methodology can help improve the applied access policies and the access control system itself, including the human-machine level.

We see the research perspective in the necessity to increase the adaptability of the methodology to different IT infrastructures by testing various systems operating in enterprises with relevant issues, including expanding the analysis by types and range of indicators of subjects and objects of systems.

In addition, to increase the practicality and adaptability of solving the tasks mentioned in the article, we see the practicality of developing appropriate AI tools based on further research on the methodology and test results that will allow monitoring and responding to dynamic changes in the system components of IT structures.

We also consider it promising to study the adaptation of the methodology to various IT structures of operating enterprises with the possible use of a wider range of indicators to describe them, such as the assessment of the entity's network, which is defined by ISO/IEC/IEEE 8802 ISO/IEC 27033 standards, Security of the working environment (RMM systems / Remote agents), Access to critical services (Corporate standards (RBAC based)), Level of knowledge in cybersecurity (ISO 27002:2022 6.3 - Information Security Education), Level of importance/criticality (Corporate standards (ISO 22301:2019 based).

6. Conclusions and Further Research

The scientific novelty of the obtained results is the creation of a methodology for testing the access control system to the system components of IT structures, which uses modern tools and software, such as intrusion detection systems (IDS), fuzz testing, User and Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), SBOM and machine learning approaches. An integral part of the methodology is the relevant libraries and databases: CIS Benchmark, Common Vulnerabilities and Exposures (CVEs), Common Platform Enumeration (CPE) Dictionary, and Common Vulnerability Scoring System (CVSS), which ensure standardization and integration of the methodology with other approaches and methods for controlling and monitoring system components of IoT networks. The impact of factors in the subject-object system caused by various aspects, including incorrect user actions, is considered. The methodology is based on fuzzy logic with subsequent implementation in the MATLAB package.

The proposed system allows you to identify vulnerabilities in access control, considering the real architecture of the information system and the mutual influence of objects, regulate access policies following the identified risks, and improve the quality of incident response at the software level.

The next stage of research is to introduce a dynamic component in assessing the Access control system risk level, taking into account abnormal behavior in the subject-object system.

Acknowledgments

This work has been supported by the Horizon Europe project TELEMETRY.

References

[1] Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Revision 5 (2020). doi:10.6028/NIST.SP.800-53r5.

[2] MathWorks, 2024. URL: https://www.mathworks.com/products/matlab.html.

[3] S. Parkinson, S. Khana, Identifying high-risk over-entitlement in access control policies using fuzzy logic, Cybersecurity 5:6 (2022) 1-17. doi:10.1186/s42400-022-00112-1.

[4] A. Kesarwani, P. M. Khilar, Development of trust based access control models using fuzzy logic in cloud computing, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 5 (2022) 1958-1967. doi:10.1016/j.jksuci.2019.11.001.

[5] R. Zhang, Z. Hu, Access control method of network security authentication information based on fuzzy reasoning algorithm, Measurement, Volume 185 (2021) 110103. doi:10.1016/j.measurement.2021.110103.

[6] S. Kerimkhulle, Z. Dildebayeva, A. Tokhmetov, A. Amirova, et al, Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things, Symmetry, 15(10), (2023). doi:10.3390/sym15101958.

[7] P. N. Mahalle, P. A.Thakre, N. R. Prasad, R. Prasad, A fuzzy approach to trust based access control in internet of things, in: 2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), Atlantic City, NJ, United States, 2013, Article 6617083 IEEE. doi:10.1109/VITAE.2013.6617083.

[8] A. J. Khan, S. Mehfuz, Fuzzy User Access Trust Model for Cloud Access Control, Computer Systems Science and Engineering, 44(1) (2023) 113-128. https://doi.org/10.32604/csse.2023.023378.

[9] CIS Password Policy Guide. Center for Internet Security, 2021. URL: https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide.

[10] Selecting Security Multi-factor Authentication Solutions. National Security Agency, cybersecurity information, 2020. URL: https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/Multifactor_Authentication_ Solutions_UOO17091520_V1.1%20-%20Copy.PDF.

[11] Common Vulnerability Scoring System version 4.0. User Guide. FIRST, 2023. URL: https://www.first.org/cvss/.