Development of a methodology for creating an automated information processing system with restricted access Internet of Things in a 'smart city': Threats – security technologies*

Valerii Dudykevych[1,†], Halyna Mykytyn[1,*,†], Yaroslava Parchuk[1,†], and Maksym-Stepan Terpeliuk[1,†]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., 79000 Lviv, Ukraine*

Abstract

The paper examines the issue of intellectualization of Ukraine's social infrastructure objects in the Industry 4.0 space at the level of developing an automated restricted access information processing system (ASOI with RA) in the Internet of Things (IoT) security segment smart city (SC) and algorithmic and software implementation using the Python programming language. An analytical review of known methodologies for developing secure automated information processing systems and approaches to ensuring the security of IoT systems was conducted. A qualitative analysis of the segments of a "smart city" – transport, medicine, energy, ecology – was carried out by grouping them at the level of the classification scheme of the subject area according to the "object – threat – protection" concept. A conceptual model of the subject area "Internet of Things in a 'smart city': threats – security technologies" was created based on the principles of system analysis – integrity, hierarchy, and multifacetedness. The criteria for selecting a relational database (RDB), database management system (DBMS) SQLite, and Python programming language have been substantiated, and an RDB information model has been constructed for further algorithmic and software implementation. An algorithm for the secure operation of an automated information processing system at the authentication procedure level is presented and, on this basis, a software implementation of the AIPS "Internet of Things in a Smart City: threats – security technologies" has been developed using Python for the segments: "smart transport", "smart health", "smart energy", "smart ecology" at the web application level.

Keywords

intellectualization of objects; Internet of Things; "smart city"; qualitative analysis; classification scheme; conceptual and information models; relational database; database management system; restricted access; automated information processing system.

1. Introduction

Today, the processes of intellectualization of social infrastructure objects are developing effectively, in particular, those critical in the context of Industry 4.0 and the Cybersecurity Strategy along the following vectors: 1) information and communication technologies (ICT) as the main tool for supporting the functioning of intellectual objects; 2) approaches and methodologies for ensuring ICT security [1, 2, 3]. One of the current areas of infrastructure intellectualization is the "smart city," which is being developed in segments: "smart transport," "smart medicine," "smart energy," and "smart ecology". Among the effective means of supporting the secure functioning of a "smart city" are multi-level cyber-physical technologies (CPT) [4]. The safe operation of intellectualization objects requires the implementation of methodological approaches to ensuring ICT security, in particular multi-level CFT, functionally designed for: 1) selecting information from intellectualization objects in subject areas using the Internet of Things in the physical space of CFT; 2) transmitting information wirelessly, in particular using sensor and wired technologies of the CFT communication environment, into cyberspace; 3) processing, analyzing, and making management decisions using automated information processing systems in the CFT cyberspace.

* *CSDP'2026: Cyber Security and Data Protection, May 07, 2026, Lviv, Ukraine*
* Corresponding author.
† These authors contributed equally.
valerii.b.dudykevych@lpnu.ua (V. Dudykevych); halyna.v.mykytyn@lpnu.ua (H. Mykytyn); yaroslava.parchuk.mkbst.2025@lpnu.ua (Y. Parchuk); maksym-stepan.terpeliuk.mkbst.2025@lpnu.ua (M-S. Terpeliuk)
0000-0001-8827-9920 (V. Dudykevych); 0000-0003-4275-8285 (H. Mykytyn); 0009-0002-7349-7364 (Y. Parchuk); 0009-0001-7015-5855 (M-S. Terpeliuk)

Accordingly, the issue of Internet of Things security for smart infrastructure objects, as one of the levels of CFT, is relevant in the context of Industry 4.0 development in Ukraine, especially in terms of automating the processing of restricted information at the web application level. Many scientific studies, both internationally and in Ukraine, are devoted to the problem of security of infrastructure object intellectualization processes at the level of functioning of secure automated information processing systems and secure IoT devices in the "smart city" segments. Security research covers approaches, models, and methodologies, hardware and software, the application of artificial intelligence, particularly in machine learning technologies, the improvement of cryptographic encryption algorithms, the improvement of methods for protecting wireless networks and information exchange protocols, and the development of integrated security systems. Let us consider some scientific research in the field of secure intellectualization of SC objects along these two vectors, which was conducted at the international level and in Ukraine.

The development of approaches and models for the security of automated information processing systems is presented at the following levels. Publication [5] considers a new approach to the implementation of automation system configurations focused on data security. An analysis of software development life cycle methodologies using NIST cybersecurity techniques is presented in [6]. Work [7] analyzes modern methods of data processing in automated systems, emphasizes the need to integrate the approaches considered to improve the efficiency and adaptability of systems, and justifies the feasibility of creating a conceptual data management model that will contribute to the development of a sustainable and secure digital infrastructure. A conceptual model of information protection in AIPS has been developed, which integrates access control, anomaly detection, and encryption of critical messages, and provides for a formalized assessment of effectiveness based on quantitative metrics [8]. In [9, 10], systematic and comprehensive models of information technology security, in particular automated information processing systems, are developed, and methodologies for the security of cyber-physical technologies in the Industry 4.0 space are proposed.

Improvements to the security methodology of smart city IoT systems have been implemented at the following levels. Article [11] explores approaches to ensuring the cybersecurity of smart city technologies based on artificial intelligence using the latest machine learning algorithms, anomaly detection systems, and predictive analytics to detect and respond to cyber threats in real time. Publication [12] analyzes the challenges of cyber threats to smart city infrastructure technologies and proposes multi-level protection strategies that combine technical solutions, regulatory and legal acts, and the implementation of reliable access control measures and network segmentation to counter potential attacks.

There is a growing trend in researching cybersecurity threats to the functioning of smart city infrastructure segments in space: vulnerabilities of IoT devices; effective solutions for their protection; recommendations for creating a comprehensive approach to security [13, 14]. An interesting trend is the development of IoT systems and cyber-physical technologies in the context of smart city operations for the period 2013-2023, in particular research into aspects of industry standards and the application of machine and deep learning methods [15]. The paper [16] analyzes and investigates the architecture of the Internet of Things and related security threats, classifies vulnerabilities at different levels of IoT, and conducts a comparative analysis of wireless technologies and security approaches. The aspect of integrity in the IoT security space is effective: analysis of factors ensuring the security of smart city technologies based on artificial intelligence and IoT; development of multi-level protection approaches at the application, network, and physical levels of infrastructure; formation of an assessment of the effectiveness of machine learning (ML) and data-driven learning (DL) methods; creation of recommendations for the integration of solutions to improve the security and resilience of urban infrastructure in the context of the latest communication technologies [17].

Publication [18] analyzes and classifies modern methods, models, and software tools for implementing IoT systems, describes the evolution and communication foundations of the Internet of Things, and establishes criteria for efficiency, scalability, and security to optimize modern IoT

solutions. Research at the IoT architecture level is relevant: analysis of the problem of information security of the Internet of Things in the space of threats and vulnerabilities, taking into account the resource limitations of devices; deployment of approaches to improving system security, in particular through the use of a local IoT gateway [19]. The work [20] investigates the limitations of traditional network protocols in the Internet of Things environment, develops elements of standardization and protection of communication technologies, and classifies specialized communication protocols according to IoT architecture levels.

IoT hardware security is developing in space: research into means of improving the hardware security of cloud computing end devices in IoT networks in accordance with cyber threats and hardware attacks; recommendations on the use of standard hardware security platforms to reduce the vulnerability of peripheral IoT systems [21]. Publication [22] presents an approach to designing an information security system for Internet of Things networks, examines the characteristics of IoT traffic and modern attacks, conducts a comparative analysis of the "Decision Tree" and "K-Nearest Neighbor" algorithms for intelligent intrusion detection, and recommends their use in protection systems designed to operate in conditions of limited computing resources. The authors of publication [23] present methods of information protection in IoT technologies and develop effective protection measures to ensure the stability and security of IoT systems against vulnerabilities to attacks, in particular based on WiFi jammers.

A comprehensive model for protecting household IoT devices and a unified methodology for quantitative security assessment, as well as an analysis of the main threats and vulnerabilities of IoT systems and approaches to improving the cyber resilience of household networks in accordance with international standards, are presented in article [24]. The study [25] examines: cyber security technologies in Internet of Things systems and devices; approaches to protecting data transmission channels; proposes comprehensive methods for improving IoT cybersecurity based on a combination of known technologies, which ensures the reliability, security, and development prospects of data exchange architecture in Internet of Things networks. In the context of the development of IoT system security models, the following segments are of interest: a risk-oriented security model for IoT systems closely integrated with physical control processes [26]; Shadow IT risk analysis in public cloud infrastructures and an approach to their identification and assessment in the space of cloud-integrated IoT security models, in which IoT platforms rely on external cloud services for data processing and management [27].

The work [28] considers a universal KFT security platform and proposes a three-level security model for the Internet of Things in the context of the intellectualization of infrastructure objects. The current task of intellectualization is the secure operation of "smart city" technologies, in particular IoT systems, in accordance with the main cybersecurity profiles: confidentiality, integrity, and availability. Accordingly, one of the effective approaches in this direction is the development of a security methodology for IoT segments of SC based on the concept of object – threat – protection and its implementation at the level of an automated information processing system with restricted access.

2. Problem statement

Secure intellectualization of social infrastructure objects involves the implementation of secure CFTs as one of the effective tools for the functioning of "smart objects." Accordingly, the development of comprehensive security systems for multi-level CFTs, in particular IoT systems, requires the creation of secure automated information processing systems at the web application level to represent the dynamics of updates: the latest IoT devices in the SC segments, potential threats, security technologies, and international and national standards in the field of cybersecurity. The Internet of Things, as one of the levels of CFT, is one of the most important technologies of the 21st century, which is currently developing dynamically in the space of "intellectualization objects – IoT devices – random and targeted threats – implementation mechanisms – methods and means of protection." IoT security requires the development of a

methodology for creating AIPS with RA, taking into account the specifics of the industrial park of intelligent objects of the "smart city" segments, the range of IoT systems in accordance with the complex of probable threats and security technologies.

Based on the analysis of recent studies and publications, the objectives of this work have been established: 1) to conduct a qualitative analysis of the subject area "Internet of Things in a smart city: threats – security technologies" as a physical space of the KFT based on the grouping method and, on this basis, to create a classification scheme for building an RDB; 2) to develop a conceptual model of the subject area based on the classification scheme and to build an information model of a relational database; 3) to justify the criteria for selecting the RDB model, the SQLite database management system, and the Python programming language for the implementation of AIPS with RA; 4) develop an algorithmic and software implementation of the secure functioning of the AIPS with RA at the level of a web application that has effective advantages for users: accessibility, ease of use, information updates, integration.

The aim of the work is to create a methodological approach to the development of an automated system for processing information with limited access, "The Internet of Things in a Smart City: Threats – Security Technologies," which is being deployed: a classification scheme for qualitative analysis of the subject area of IoT security segments of SC infrastructure; conceptual and informational models for building a relational database; algorithmic and software implementation of the secure functioning of AIPS with RA at the web application level.

3. Security research results for the Internet of Things in a "smart city"

3.1. Qualitative analysis of data in the subject area "Internet of Things in a 'smart city': threats – security technologies"

The grouping method is one of the basic tools for qualitative data analysis and consists in dividing the studied set of objects of the subject area or phenomena into homogeneous groups according to essential qualitative characteristics. The classification scheme of the subject area "Internet of Things in a 'smart city': threats – security technologies" was created for the infrastructure segments "smart transport," "smart health," "smart energy," and "smart ecology," but only "smart ecology" is developed in the work at the level of monitoring water resources and water quality (Table 1, Table 2).

Table 1
Classification scheme "Internet of Things in a smart city: threats"

Sphere (a)	
	Smart Ecology
Sphere component (b)	2. Water Quality & Resources Monitoring
	Structural and functional description [29, 30]
Architecture (c)	• Distributed architecture: • Measurement (buoys, underwater stations, probes, sensors); • Network (satellite communication, LoRaWAN, 4G); • Edge processing (local controllers); • Central level (monitoring, forecasting); • Application level (alerts, portals, weather integration).
	Table 1 – continued from previous page
	Sphere (a)
	Smart Ecology
Sphere component (b)	2. Water Quality & Resources Monitoring
	Structural and functional description [29, 30]

Purpose (d)	• Continuous monitoring of water quality in rivers, lakes, and reservoirs; • Control of drinking water parameters in water supply systems; • Real-time detection of sources of water pollution; • Water level monitoring for flood prevention; • Control of industrial wastewater before discharge into water bodies; • Assessment of the state of aquatic ecosystems and biodiversity; • Water resource management and water distribution optimization; • Early warning of the population about the unsuitability of water for use; • Scientific research of hydrological and hydrochemical processes.
IoT Devices (e)	• Multiparameter probes (pH, dissolved oxygen, turbidity, temperature); • Water conductivity and salinity sensors; • Nitrate and phosphate analyzers for eutrophication control; • Ultrasonic and radar water level sensors; • Fluorescent sensors for detecting petroleum products; • Heavy metal sensors with voltammetry; • Automatic samplers for laboratory analysis; • Hydrophones for monitoring underwater noise; • GPS buoys for monitoring currents and water mass movements; • Underwater cameras for visual observation; • Weather stations on buoys for comprehensive monitoring.
	Threats (f) [31, 32]
Accidental	• Biofouling of sensors with algae, which distorts measurements; • Damage to equipment due to storms, ice drifts, floods; • Calibration drift of sensors due to prolonged immersion in water; • Loss of satellite communication with buoys due to weather conditions; • Mechanical damage to underwater station cables by ships or fishermen; • Battery discharge due to cold water with increased thermal conductivity.
Targeted	• Physical damage or theft of expensive sensors and buoys; • Cyberattacks on monitoring systems to conceal pollution discharges; • Falsification of water quality data by polluting companies; • Hacking of warning systems to cause panic among the population; • DDoS attacks on hydrological information portals; • Manipulation of water use data for illegal water abstraction; • Sabotage of early flood warning systems.

Table 2
Classification scheme “Internet of Things in a smart city: security technologies”

	Sphere (a)
	Smart Ecology
Sphere component (b)	2. Water Quality & Resources Monitoring
	Security technologies [33, 34]
Protection methods (g)	• Regular cleaning of sensors from biofouling using automatic mechanical or ultrasonic systems;

	Sphere (a)
	Smart Ecology
Sphere component (b)	2. Water Quality & Resources Monitoring
	Security technologies [33, 34]
Protection methods (g)	• Encryption of hydrological data during transmission from stations to centers; • Physical protection of expensive equipment with anchor systems and GPS monitoring; • Redundancy of commun. channels (satellite + cellular networks); • Data integrity control using digital signatures; • Multi-level authentication of monitoring system operators; • Monitoring of anomalies in data to detect falsification of hydrochemical data; • Geographically distributed storage of critical water resource data; • Cross-validation of data between neighboring monitoring stations.
Hardware protection (h)	• Vandal-proof buoys with high-strength housings and bright markings; • Cryptographic modules in underwater stations to protect telemetry; • GPS trackers on equipment with movement alerts; • Automatic sensor cleaning systems (mechanical brushes, UV irradiation); • Protected IP68 cable entries for underwater connections; • High-capacity backup batteries with solar panels on buoys; • Hardware HSMs for storing hydrological data encryption keys; • Protected gateways with built-in firewalls; • Enclosure opening sensors with tamper alerts.
Software protection (i)	• Hydromonitoring platform with built-in encryption and access control; • Machine learning algorithms for detecting abnormal measurements; • Automatic sensor calibration systems with drift compensation; • Blockchain for immutable storage of water quality data; • Data validation systems with hydrological models; • SIEM for monitoring cyber threats in the water sensor network;
	Sphere (a)
	• Secure APIs for integration with water utility systems; • Incident management systems for rapid response to pollution; • Automatic backup systems for hydrological databases.
	Standards (j)
International	• ISO/IEC 30179:2023; • ISO/IEC 27400:2022; • ISO 24512:2024; • NIST CSF 2.0:2024; • NIST SP 800-213:2021; • EN ISO 10523:2012; • IEEE 802.15.4:2020.
Ukrainian National Standards	• DSTU EN ISO 5667-1:2025; • DSTU EN ISO 5667-6:2025; • DSTU EN ISO 5814:2025; • DSTU EN ISO 7887:2025; • DSTU EN ISO 4373:2022; • DSTU ISO/IEC 30141:2019.

3.2. Conceptual model of the subject area and information model of the relational database

Conceptual model of the subject area: principles of integrity, hierarchy, and multifacetedness. The basis for creating a conceptual model of the subject area "Internet of Things in a 'smart city': threats – security technologies" is a classification scheme and the principles of system analysis – integrity, hierarchy, multifacetedness, which systematically allow structuring the IoT components of the "smart city" infrastructure segments, systematizing random and targeted threats, and justifying the compliance of security technologies. The conceptual model of the subject area "Internet of Things in a 'smart city': threats – security technologies" (Figure 1) is built for the following infrastructure segments: "smart transport" (a1), "smart health" (a2), "smart energy" (a3), "smart ecology" (a4) and is the basis for creating an information model database and developing an algorithmic and software implementation of AIPS with restricted access in the space of secure functioning of the information life cycle at the web application level.

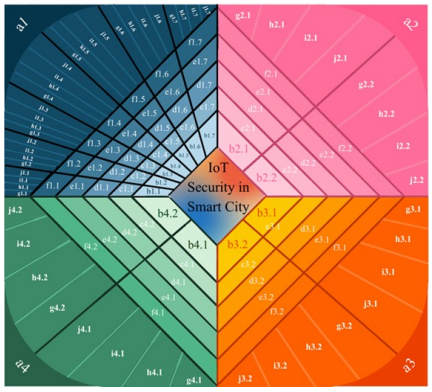


Figure 1: Conceptual model of the subject area "Internet of Things in a smart city: threats – security technologies"

The conceptual model reflects the deployment of infrastructure segments by components: "smart transport": smart railways; smart aviation; smart motorways; smart logistics; smart maritime transport; smart public transport; smart urban mobility (b1.1–b1.7); "smart health": smart hospitals; telemedicine and remote monitoring (b2.1–b2.2); "smart energy": smart power grids; smart energy consumption metering and management (b3.1–b3.2); "smart ecology": air quality monitoring; water resources and water quality monitoring (b4.1–b4.2).

Database information model: justification for choosing a relational database, database management system, and programming language. To develop an AIPS with the subject area "Internet of Things in a Smart City: Threats – Security Technologies," a relational database (RDB) was chosen based on the type of connection between data. In such a model, objects and relationships between them are represented as two-dimensional tables, with relationships between relations also considered as objects. The RDB model is justified by the criteria of data structure, record identification, and efficiency of use. SQLite was chosen as the DBMS for software implementation. This relational database management system uses the Structured Query Language (SQL). The main criteria for choosing SQLite were compatibility and simplicity, support for standards, and portability.

The relational database information model (Figure 2), combined with the SQLite DBMS, is an effective tool for managing the information lifecycle in subsystems of the subject area "Internet of Things in Smart Cities: Threats and Security Technologies."

For the software implementation of AIPS, the criteria for the feasibility of using the high-level programming language Python in terms of functional capabilities in the context of solving applied problems have been substantiated: efficiency of data manipulation; compliance with visualization tasks; optimization of software architecture.

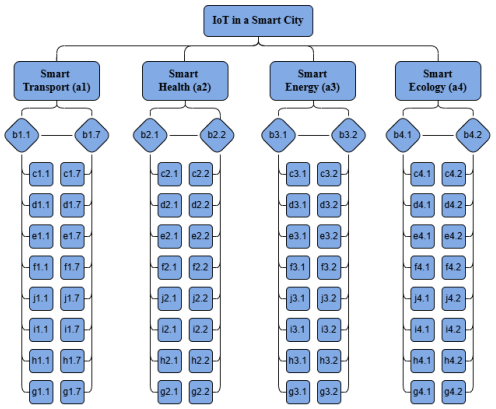


Figure 1: Information model of the relational database "Internet of Things in a smart city: threats – security technologies"

4. Algorithmic and software implementation of secure operation of AIPS with RA "Internet of Things in a smart city: threats – security technologies"

Algorithm for the secure operation of an automated information processing system with restricted access. Let us consider the stages of developing an AIPS "Internet of Things in a 'smart city': threats – security technologies" with restricted access. The automated system is designed to enter, store, process, and display information on critical infrastructure segments of the SC: "smart transport," "smart health," "smart energy," and "smart ecology." A distinctive feature of the developed AIPS with RA is the algorithmic and programmatic implementation of an authorized access mechanism based on an authentication procedure. Technically, the system is implemented as a web application at the level of the following components:

1. Server side (Backend): written in Python using the Flask framework;
2. Client side (Frontend): HTML pages displaying data;
3. Databases: SQLite DBMS for storing accounts and information about critical infrastructure segments of the SC.

The AIPS operates on the basis of client-server architecture. User interaction with the AIPS follows an algorithm that ensures data security:

1. Getting started (Login): When attempting to access any AIPS page, the server checks whether the user is authorized. If not, the user is automatically redirected to the login page. The user enters their email and password, which are verified by the system against the database records;
2. Registration of new users: To gain access, a new user must complete the registration process. The system checks the uniqueness of the email address. During registration, the user's password undergoes cryptographic transformation (hashing) before being recorded in the database, which guarantees its protection against theft;
3. Working with information (Navigation): After logging in, the user is taken to the main panel, where the data is structured by category ("Smart Transport," "Smart Health," etc.). Selecting a category initiates a query to the database, which returns a list of only relevant devices or systems;
4. Security policy (Password change): AIPS implements a password change feature with restrictions – the user is given a limited number of access attempts (in this implementation, 3 attempts). This is done to prevent frequent and uncontrolled changes to account data, which is part of the security policy;
5. Logging out: The user can safely log out of AIPS by clicking "Log out." This terminates the current session and closes access to data until the next password is entered.

For the purpose of secure AIPS operation, an SQLite database structure has been developed, consisting of two main tables, which allows user data and system data to be separated:
Table 1. users. The table is responsible for security and authorization and contains:

- id: Unique user number,
- email: Login for entering the system,
- password: Hashed password (irreversible character conversion),
- changes_left: Counter that controls how many times the user can still change their password.

Table 2. iot_systems (Protection objects). The table is the main information resource of the AIPS and contains a unified set of attributes that allows describing any subsystem of the "Internet of Things of a smart city: threats – security technologies" regardless of its industry affiliation. The table attributes are logically divided into three functional groups:

A. Identification and Architecture Group:

- id (Record identifier): Unique primary key of the record in the system,
- category (Industry category): Industry affiliation identifier that allows subsystems to be classified by area of application (critical infrastructure, utilities, social sphere, etc.),
- name (System name): Name of the KFT in the physical space of the IoT as a tool for the functioning of the "smart city" infrastructure,
- architecture (System architecture): Type and structure of the architecture,
- purpose (Purpose and use): The intended purpose and main functions of the system in the smart city infrastructure,
- devices (Hardware): A set of IoT devices, including sensors, controllers, actuators, and communication devices that enable the CFT to function in the physical IoT space.

B. Group modeling destabilizing factors:

- threats_accidental (Accidental threats): Factors of natural or man-made probable impact on the security profiles of the IoT system (technical failures, environmental impact, personnel errors),
- threts_targeted (Targeted threats): A list of current cyberattack vectors aimed at violating the basic security profiles-confidentiality, integrity, and availability of information—characteristic of this type of IoT system architecture;

C. Group of comprehensive protection systems for the SC segment "Internet of Things in a smart city: threats – protection technologies":

- methods (Protection methods): General organizational and technical strategies used to minimize risks,
- protection_hard (Hardware protection): Information about physical and hardware security measures integrated into IoT system equipment to counter interference and unauthorized access,
- protection_soft (Software protection): Software mechanisms and cryptographic protocols that ensure data protection throughout the information lifecycle in AIPS,
- standards (Regulatory compliance): Information about the compliance of security technologies with information and cybersecurity standards (international, national, and industry).

The secure operation of AIPS with RA is implemented using three methods (Figure 3):

1. Session authentication: A session mechanism is used. This is a kind of "digital pass" that the server issues to the browser after the correct password is entered. With each subsequent request, the server checks this pass, and if it is not present, access is blocked;
2. Password protection: Passwords are not stored in the database in plain text. Instead, hashing is used. Even if an attacker gains access to the database file, they will only see a set of incomprehensible characters from which it is impossible to recover the real password;
3. User action control: Setting a limit on password changes (the changes_left field) is a security policy control that disciplines users and protects the system from abuse of functionality.

Software implementation of an automated information processing system with restricted access. The architecture of the developed AIPS at the web application level is based on the interaction of the client part with the server logic implemented by the Flask microframework. The key stages of the software implementation of the AIPS are ensuring the protection of user credentials and organizing dynamic access to the relational database. In order to ensure the security of the AIPS in terms of confidentiality, integrity, and availability, a mechanism for cryptographic password conversion has been implemented in the user registration module. Instead of storing passwords in plain text, the system uses a hashing algorithm with salting, which is implemented using the werkzeug.security library.

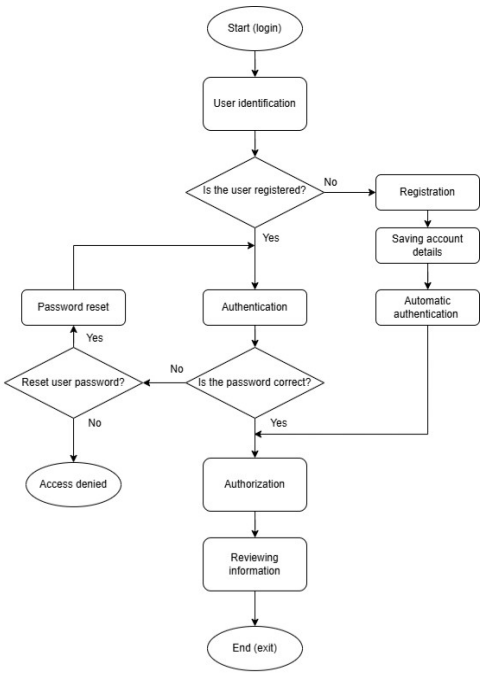


Figure 1: Block diagram of the algorithm for the operation of an automated information processing system with restricted access

The first fragment of the program code shows the procedure for registering a new user, which includes generating a password hash and automatically initializing the session after successfully writing data to the DBMS.

```
from werkzeug.security import generate_password_hash, check_password_hash

@app.route('/register', methods=['POST'])
def register():
   email = request.form['email']
   password = request.form['password']
      hashed_pw = generate_password_hash(password)

   try:
      conn = get_db_connection()
      cursor = conn.execute(
         'INSERT INTO users (email, password) VALUES (?, ?)',
         (email, hashed_pw)
      )
         user_id = cursor.lastrowid
         conn.commit()
         conn.close()
```

```
            session['user_id'] = user_id
            session['email'] = email
            return redirect(url_for('index'))
        except sqlite3.IntegrityError:
            flash('This email is already registered.', 'error')
    return render_template('register.html')
```

The second important component of AIPS is the data visualization module, which is responsible for processing HTTP requests and generating web pages based on information stored in the SQLite database. The Flask architectural model allows for a clear separation of routing logic and data presentation. The second code snippet shows the implementation of a controller for displaying a specific classification category. The algorithm involves checking access rights (the presence of an active session), executing a parameterized SQL query to select the relevant systems, and transferring the resulting objects to the interface template.

```
@app.route('/category/<category_id>')
def show_category(category_id):
    if 'user_id' not in session: return redirect(url_for('login'))

    conn = get_db_connection()
    systems = conn.execute(
        'SELECT id, name FROM iot_systems WHERE category = ? ORDER BY id',
        (category_id,)
    ).fetchall()
    conn.close()

    return render_template('category_list.html', systems=systems)
```

Screenshots of the secure operation of AIPS with RA "Internet of Things in a 'smart city': threats – security technologies" at the web application level are presented in Fig. 4-15.

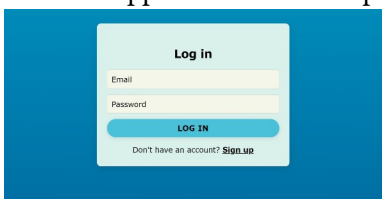


Figure 4: User authorization page

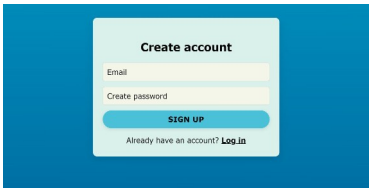


Figure 5: User registration page

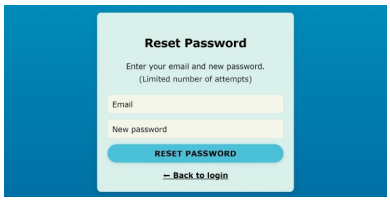


Figure 6: Password change page

Figure 7: Home page of AIPS with RA

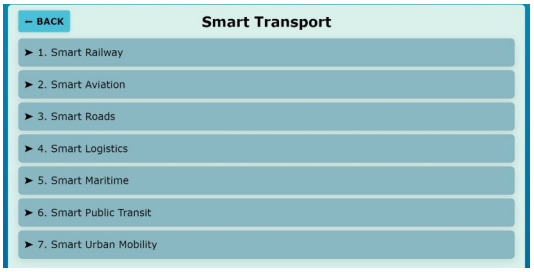


Figure 8: Page of the “Smart Transport” subsystem

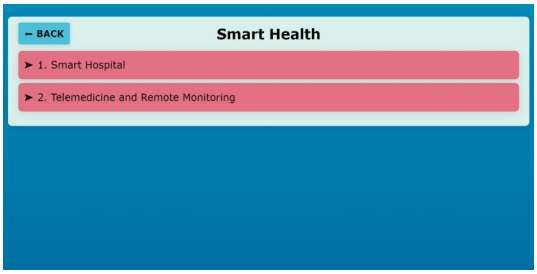


Figure 9: Page of the “Smart Health” subsystem

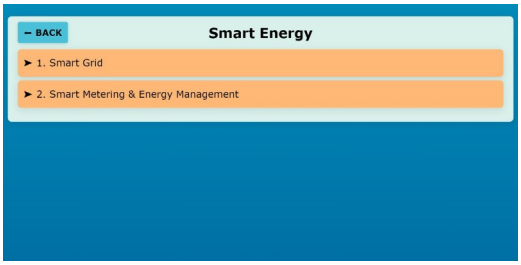


Figure 10: Page of the “Smart Energy” subsystem

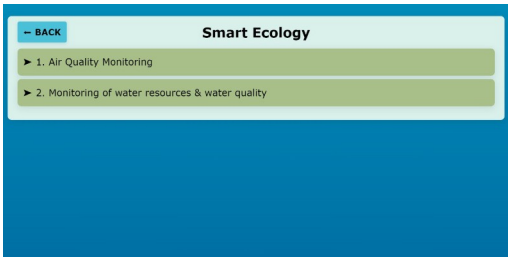
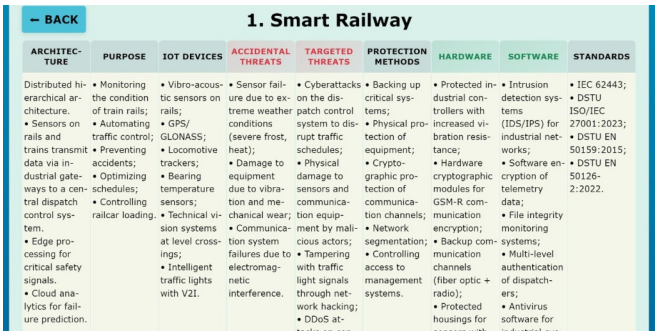


Figure 11: Page of the “Smart Ecology” subsystem

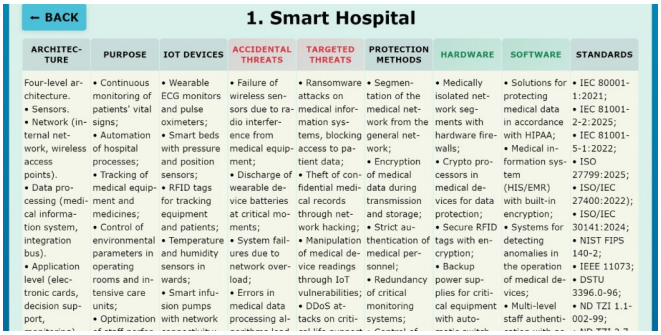


← BACK

1. Smart Railway

ARCHITECTURE	PURPOSE	IOT DEVICES	ACCIDENTAL THREATS	TARGETED THREATS	PROTECTION METHODS	HARDWARE	SOFTWARE	STANDARDS
Distributed hierarchical architecture. • Sensors on rails and trains transmit data via industrial gateways to a central dispatch control system. • Edge processing for critical safety signals. • Cloud analytics for failure prediction.	• Monitoring the condition of train rails; • Automating traffic control; • Preventing accidents; • Optimizing schedules; • Controlling railcar loading.	• Vibro-acoustic sensors on rails; • GPS/GLONASS; • Locomotive trackers; • Bearing temperature sensors; • Technical vision systems at level crossings; • Intelligent traffic lights with V2I.	• Sensor failure due to extreme weather conditions (severe frost, heat); • Damage to equipment due to vibration and mechanical wear; • Communication system failures due to electromagnetic interference.	• Cyberattacks on the dispatch control system to disrupt traffic schedules; • Physical damage to sensors and communication equipment by malicious actors; • Tampering with traffic light signals through network hacking; • DDoS at-	• Backing up critical systems; • Physical protection of equipment; • Cryptographic protection of communication channels; • Network segmentation; • Controlling access to management systems.	• Protected industrial controllers with increased vibration resistance; • Hardware cryptographic modules for GSM-R communication encryption; • Backup communication channels (fiber optic + radio); • Protected housings for	• Intrusion detection systems (IDS/IPS) for industrial networks; • Software encryption of telemetry data; • File integrity monitoring systems; • Multi-level authentication of dispatchers; • Antivirus software for	• IEC 62443; • DSTU ISO/IEC 27001:2023; • DSTU EN 50159:2015; • DSTU EN 50126-2:2022.

Figure 12: Page of the “Smart Railway” subsystem

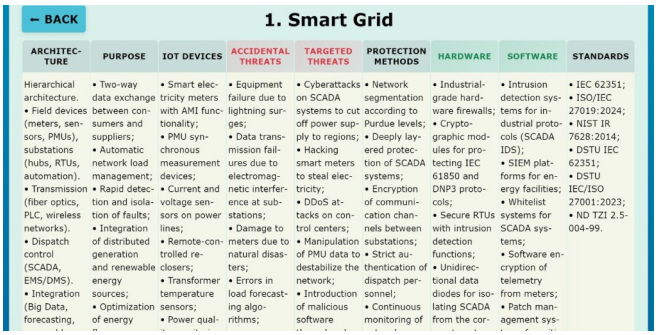


← BACK

1. Smart Hospital

ARCHITECTURE	PURPOSE	IOT DEVICES	ACCIDENTAL THREATS	TARGETED THREATS	PROTECTION METHODS	HARDWARE	SOFTWARE	STANDARDS
Four-level architecture. • Sensors. • Network (internal network, wireless access points). • Data processing (medical information system, integration bus). • Application level (electronic cards, decision support,	• Continuous monitoring of patients' vital signs; • Automation of hospital processes; • Tracking of medical equipment and medicines; • Control of environmental parameters in operating rooms and intensive care units; • Optimization	• Wearable ECG monitors and pulse oximeters; • Smart beds with pressure and position sensors; • RFID tags for tracking equipment and patients; • Temperature and humidity sensors in wards; • Smart infusion pumps with network	• Failure of wireless sensors due to radio interference from medical equipment; • Discharge of wearable device batteries at critical moments; • System failures due to network overload; • Errors in medical data processing al-	• Ransomware attacks on medical information systems, blocking access to patient data; • Theft of confidential medical records through network hacking; • Manipulation of medical device readings through IoT vulnerabilities; • DDoS attacks on criti-	• Segmentation of the medical network from the general network; • Encryption of medical data during transmission and storage; • Strict authentication of medical personnel; • Redundancy of critical monitoring systems;	• Medically isolated network segments with hardware firewalls; • Crypto processors in medical devices for data protection; • Secure RFID tags with encryption; • Backup power supplies for critical equipment with auto-	• Solutions for protecting medical data in accordance with HIPAA; • Medical information system (HIS/EMR) with built-in encryption; • Systems for detecting anomalies in the operation of medical devices; • Multi-level staff authenti-	• IEC 80001-1:2021; • IEC 81001-2-2:2025; • IEC 81001-5-1:2022; • ISO 27799:2025; • ISO/IEC 27400:2022); • ISO/IEC 30141:2024; • NIST FIPS 140-2; • IEEE 11073; • DSTU 3396.0-96; • ND TZI 1.1-002-99;

Figure 13: Page of the “Smart Hospital” subsystem

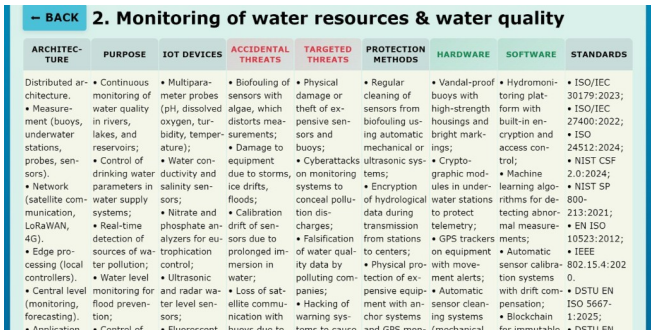


← BACK

1. Smart Grid

ARCHITECTURE	PURPOSE	IOT DEVICES	ACCIDENTAL THREATS	TARGETED THREATS	PROTECTION METHODS	HARDWARE	SOFTWARE	STANDARDS
Hierarchical architecture. • Field devices (meters, sensors, PMUs), substations (hubs, RTUs, automation). • Transmission (fiber optics, PLC, wireless networks). • Dispatch control (SCADA, EMS/DMS). • Integration (Big Data, forecasting,	• Two-way data exchange between consumers and suppliers; • Automatic network load management; • Rapid detection and isolation of faults; • Integration of distributed generation and renewable energy sources; • Optimization of energy	• Smart electricity meters with AMI functionality; • PMU synchronous measurement devices; • Current and voltage sensors on power lines; • Remote-controlled reclosers; • Transformer temperature sensors; • Power qual-	• Equipment failure due to lightning surges; • Data transmission failures due to electromagnetic interference at substations; • Damage to meters due to natural disasters; • Errors in load forecasting algorithms;	• Cyberattacks on SCADA systems to cut off power supply to regions; • Hacking smart meters to steal electricity; • DDoS attacks on control centers; • Manipulation of PMU data to destabilize the network; • Introduction of malicious software	• Network segmentation according to Purdue levels; • Deeply layered protection of SCADA systems; • Encryption of communication channels between substations; • Strict authentication of dispatch personnel; • Continuous monitoring of	• Industrial-grade hardware firewalls; • Cryptographic modules for protecting IEC 61850 and DNP3 protocols; • Secure RTUs with intrusion detection functions; • Unidirectional data diodes for isolating SCADA from the cor-	• Intrusion detection systems for industrial protocols (SCADA IDS); • SIEM platforms for energy facilities; • Whitelist systems for SCADA systems; • Software encryption of telemetry from meters; • Patch management sys-	• IEC 62351; • ISO/IEC 27019:2024; • NIST IR 7628:2014; • DSTU IEC 62351; • DSTU IEC/ISO 27001:2023; • ND TZI 2.5-004-99.

Figure 14: Page of the “Smart Grid” subsystem



← BACK

2. Monitoring of water resources & water quality

ARCHITECTURE	PURPOSE	IOT DEVICES	ACCIDENTAL THREATS	TARGETED THREATS	PROTECTION METHODS	HARDWARE	SOFTWARE	STANDARDS
Distributed architecture. • Measurement (buoys, underwater stations, probes, sensors). • Network (satellite communication, LoRaWAN, 4G). • Edge processing (local controllers). • Central level (monitoring, forecasting).	• Continuous monitoring of water quality in rivers, lakes, and reservoirs; • Control of drinking water parameters in water supply systems; • Real-time detection of sources of water pollution; • Water level monitoring for flood prevention;	• Multiparameter probes (pH, dissolved oxygen, turbidity, temperature); • Water conductivity and salinity sensors; • Nitrate and phosphate analyzers for eutrophication control; • Ultrasonic and radar water level sensors;	• Biofouling of sensors with algae, which distorts measurements; • Damage to equipment due to storms, ice drifts, floods; • Calibration drift of sensors due to prolonged immersion in water; • Loss of satellite communication with	• Physical damage or theft of expensive sensors and buoys; • Cyberattacks on monitoring systems to conceal pollution discharges; • Falsification of water quality data by polluting companies; • Hacking of warning sys-	• Regular cleaning of sensors from biofouling using automatic mechanical or ultrasonic systems; • Encryption of hydrological data during transmission from stations to centers; • Physical protection of expensive equipment with anchor systems	• Vandal-proof buoys with high-strength housings and bright markings; • Cryptographic modules in underwater stations to protect telemetry; • GPS trackers on equipment with movement alerts; • Automatic sensor cleaning systems	• Hydrometeorological platform with built-in encryption and access control; • Machine learning algorithms for detecting abnormal measurements; • Automatic sensor calibration systems with drift compensation; • Blockchain	• ISO/IEC 30179:2023; • ISO/IEC 27400:2022; • ISO 24512:2024; • NIST CSF 2.0:2024; • NIST SP 800-213:2021; • EN ISO 10523:2012; • IEEE 802.15.4:2020. • DSTU EN ISO 5667-1:2025;

Figure 15: Page of the “Monitoring of water resources & water quality” subsystem

5. Conclusions

A qualitative analysis of the subject area of Internet of Things security in the “smart city” segments was conducted, and on this basis, a classification scheme was constructed using the grouping method and a conceptual model “IoT in a smart city: threats – security technologies” was created. An algorithmic and software-based implementation for the secure operation of an automated information processing system “Internet of Things in a Smart City: Threats and Security Technologies” has been developed, incorporating session-based authentication methods, password

protection mechanisms, and user activity control based on an information model of a relational database, implemented using the SQLite database management system and the Python programming language. The proposed methodological approach to the development of ASOI with OD "Internet of Things in a smart city: threats – security technologies" can be effectively used to solve applied problems of secure intellectualization of social infrastructure objects, taking into account current trends in cyber challenges in the era of Industry 5.0, which involves the integration of physical, digital, and biological systems in the space of providing secure technologies to counter cyber threats.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Association of Industrial Automation Enterprises of Ukraine. (2018). Ind. 4.0 dev. strategy.

[2] EU Agency for Cybersecurity. (2021). Int. strategy EU Agency Cybersecur.

[3] National SeBcurity and Defense Council of Ukraine. Cybersecur. Strategy Ukr. 2021-2025.

[4] H. Mykytyn, V. Dudykevych, A. Rebets, Quintessence CyberPhysical Syst. Secur., Inf. Syst. Networks, 887, 2018, 58-68.

[5] A. Asatiani, T. Hakkarainen, K. Paaso, E. Penttinen, Security by envelopment — A novel approach to data-security-oriented configuration of lightweight-automation systems, Eur. J. Inf. Syst., 33 (2024), 631-653. doi:10.1080/0960085X.2023.2217362.

[6] O. Balocon, Prioritizing information security: Analysis of software development life cycle method-ologies using the nist cybersecurity framework, Ignatian Int. J. Multidiscip. Res., 2 (2024) 1495-1508. doi:10.5281/zenodo.11069707.

[7] D. Smyk, N. Burak, Methods and means of data processing in modern automated systems, Bull. Lviv State Univ. Life Saf., 31 (2025), 41-49. doi: 10.32447/20784643.31.2025.05.

[8] U. Panovyk, Information security in automated systems based on a conceptual model with formalized efficiency assessment, Cybersecur.: Educ. Sci. Technol., 4 (2025) 307-320. doi:10.28925/2663-4023.2025.28.798.

[9] Y. Bobalo, V. Dudykevych, H. Mykytyn, Information Technologies for Data Collection: Concept, Methodol. Approaches, Secur. Monogr., (2024) 148.

[10] S. Milevskyi, et al., Development of the sociocyberphysical systems` multi-contour security methodology, EasternEuropean J. Enterp. Technol., 1/9 (127) (2024) 34-51. doi: 10.15587/1729-4061.2024.298844.

[11] D. Chirra, Ai-enabled cybersecurity solutions for protecting smart cities against emerging threats, 2024.

[12] J. Oliha, P. Biu, O. Obi, Securing the smart city: A review of cybersecurity challenges and strategies, Eng. Sci. & Technol. J., 5 (2024) 496-506. doi:10.53022/oarjms.2024.7.1.0013.

[13] A. Mohammed, Cybersecurity in smart cities: As cities become smarter, new vulnerabilities arise research can focus on securing iot devices, smart infrastructure, and privacy concerns associated with smart city data, Pioneer Res. J. Comput. Sci., 1 (2024) 75-82.

[14] A. Mohammed, Cybersecurity in smart cities: Securing iot and smart infrastructure, J. ofInnovative Technol., 5 (2022).

[15] K. Chui, et al., A survey of internet of things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions, Inf., 14 (2023). doi:10.3390/info14070388.

[16] R. Sharma, R. Arya, Security threats and measures in the internet of things for smart city infrastructure: A state of art, Trans. Emerg. Telecommun. Technol., 34 (2023). doi: 10.1002/ett.4571.
[17] J. Ali, et al., A deep dive into cybersecurity solutions for ai-driven iot-enabled smart cities in advanced communication networks, Comput. Commun., 229 (2025), doi:10.1016/j.comcom.2024.108000.
[18] Y. Khomenko, Modern methods, models and software tools for implementation and optimization of IoT systems (Internet Of Things), J. Inf. Technol. Educ. (ITE), (2024) 72-84. doi:10.14308/ite000782.
[19] A. Kovalenko, R. Yaroshevych, O. Balenko, Internet of things: information security issues and improvement methods, Control, Navig. Commun. Syst., 2 (2021) 78-80. doi:10.26906/SUNZ.2021.2.078.
[20] P. Klimushyn, S. Petro, Communication Technologies and Specialised Communication Protocols for Ensuring Cybersecurity of the Internet of Things, Law Saf., 97 (2025) 52-68. doi:10.32631/pb.2025.2.05.
[21] O. Zhurylo, O. Liashenko, K. Avetisova, Review of hardware security solutions for fog computing edge devices in the Internet of Things, Adv. Res. Ind. Technol., 1 (2023) 57-71. doi:10.30837/ITSSI.2023.23.057.
[22] I. Andrushchak, V. Kosheliuk, Specific aspects of designing information security systems for protecting IoT networks from attacks, Int. Sci. J. Eng. Agric., 4 (2025) 27-39. doi:10.46299/j.isjea.20250405.03.
[23] Y. Oliinyk, A. Platonenko, V. Cherevyk, M. Vorokhob, Y. Shevchuk, Methods of information protection in IoT technologies, Cybersecur. Educ. Sci. Technol., 3 (2025). doi:10.28925/2663-4023.2025.27.705.
[24] V. Yashchuk, U. Panovyk, S. Cherkas, A. Ivanusa, R. Tkachuk, Comprehensive IoT device protection model in a domestic environment: threats, vulnerabilities and mitigation methods, Bulletin of Lviv State University of Life Safety 32 (2025) 125-140. doi:10.32447/20784643.32.2025.10.
[25] V. Malinovskyi, L. Kupershtein, V. Lukichov, A. Dudatiev, Challenges and approaches to improving security levels in data transmission channels of IoT systems and devices, Bulletin of Vinnytsia Polytechnic Institute, 4 (2024) 104-114. doi:10.31649/1997-9266-2024-175-4-104-114.
[26] V. Yuzevych, A. Obshta, I. Opirskyy, O. Harasymchuk, Algorithm for assessing the degree of information security risk of a cyber-physical system for controlling underground metal constructions, CEUR Workshop Proc., 3702 (2024) 400-412.
[27] Y. Martseniuk, et al., Shadow IT risk analysis in public cloud infrastructure, 3800 (2024) 22-31.
[28] V. Dudykevych, H. Mykytyn, T. Stosyk, P. Skladannyi, Platform for the security of cyber-physical systems and the IoT in the intellectualization of society, 3654 (2024) 449-457.
[29] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst., 29 (2013) 1645-1660. doi: 10.1016/j.future.2013.01.010.
[30] F. Alaba, M. Othman, I. Hashem, F. Alotaibi, Internet of Things security: a survey, J. Netw. Comput. Appl., 88 (2017) 10-28. doi:/10.1016/j.jnca.2017.04.002.
[31] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed Internet of Things, Comput. Networks, 57 (2013) 2266-2279. doi:10.1016/j.comnet.2012.12.018.
[32] R. Weber, Internet of Things – new security and privacy challenges, Comput. Law & Secur. Rev., 26 (2010) 23-30. doi:10.1016/j.clsr.2009.11.008.
[33] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, Comput. Networks, 76 (2015) 146-164. doi:10.1016/j.comnet.2014.11.008.
[34] T. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the Internet of Things, IEEE Access, 6 (2018) 32979-33001. doi:10.1109/ACCESS.2018.2842685.