***I. Vovk**, BA student*
***O. Pasichnyk**, PhD in Ped., As. Prof.*
Khmelnytskyi National University

DEVELOPMENT OF A MULTI-FACTOR AUTHENTICATION MODEL FOR IOT-BASED ACCESS CONTROL SYSTEMS

Introduction. Access control systems have progressed from purely mechanical devices to sophisticated cyber-physical systems [1]. Modern trends in IoT development demonstrate a transition from isolated devices to an integrated ecosystem with distributed data processing and centralized security management. The architecture of cyber-physical systems security provides a multi-layered approach that combines physical protection, network isolation and software-based access control mechanisms.

Modern access control tools are sophisticated cyber-physical devices where the reliability of physical protection is integrated with intelligent identification mechanisms. The primary goal of these systems is to eliminate the human factor and automate security protocols.

Theoretical framework of multi-factor authentication. The modern security concept of intelligent access control systems is based on the theory of multi-factor authentication (MFA) [2, 3]. The core idea is that access is granted only after verifying the user's identity through several independent categories of evidence.

According to classification of information security tools, three fundamental classes of factors are distinguished: the knowledge factor, the possession factor and the inherence factor.

The knowledge factor refers to the information that the user must remember. In context of access control systems, this is usually a digital PIN or graphical key. It is the most flexible, yet simultaneously the most vulnerable method, as the password can be compromised through observation or guessing.

The possession factor refers to a physical object that the user possesses. This can include electronic key tablets, contactless cards, key fobs (RFID/NFC), or even a smartphone with appropriate software. This method is highly reliable, as an intruder requires physical access to the object in order to compromise the system. The use of unique hardware identifiers and secure element technology ensures that the device cannot be cloned even if physical access to the hardware platform is obtained [4].

The inherence factor refers to the user's personal biometric parameters [5]. These include fingerprints, retinal patterns, or facial geometry. It represents the most personalized layer of protection, as biometric data cannot be shared with another person or forgotten.

The use of multiple factors allows the system to be configured for high sensitivity, as an error on a single protection layer can be compensated by verification on another layer. This creates a reliable barrier that makes intrusion very difficult, since an intruder would need to possess diverse skills, both digital and physical.

Beyond user identification, physical integrity of the device can be maintained through the use of accelerometers and gyroscopes (e.g., vibration sensors) allows to notice not only door opening, but also an attempt of unauthorized mechanical intrusion (drilling or hitting).

Integration of Wi-Fi and Bluetooth modules enables the owner to receive push notifications about the system status in real-time that fundamentally distinguishes smart lock from a traditional autonomous lock.

However, data transmission through wireless networks creates additional cybersecurity risks related to the possibility of traffic interception, man-in-the-middle attacks, and substitution of network nodes. Therefore, to ensure the integrity and confidentiality of data exchange, modern cryptographic transport-layer protocols, such as TLS 1.3, must be used [6].

Proposed cascade identification model. In view of the above, the main focus is the development of a formalized model for multi-factor verification that minimizes the influence of the human factor and technical vulnerabilities.

The key approach to solving the problem of unauthorized access is the deployment of a multi-factor authentication model. Unlike standard solutions where security relies on a single factor (e.g., passwords or keys), this paper proposes a cascade identification method. It is based on a combination of three independent types of factors.

The model architecture ensures that access to the actuator control is granted only if all factors are sequentially and successfully verified within a specified time interval.

In the first stage, the user must verify the knowledge factor. For this purpose, a PIN or password can be used. In theory, input could be provided not only via a keyboard but also through a microphone or camera – for example, by pronouncing the password aloud or performing a specific gesture. However, due to the limited resistance of this layer to social engineering attacks and data interception, it is advisable to use a numerical or symbolic password and to restrict the number of authentication attempts to minimize the likelihood of compromise.

The next stage is the verification of the possession factor. The simplest and most convenient methods for this purpose are the use of RFID/NFC tags or verification via Bluetooth. This stage is more reliable, as intrusion requires physical possession of the item. However, there is a risk of theft or loss, which may result in either denial of access for the owner or unauthorized access for a third party.

Theoretically, the most reliable stage is the verification of the inherence factor. However, in practice, the use of biometric methods can lead to unpredictable situations. The most common type of biometric identification is fingerprint recognition. Low-cost scanners operate on the principle of capturing an image of the finger and comparing it with a stored template, which makes them vulnerable to forgery and can sometimes complicate access for the legitimate user. More advanced scanners analyze the capacitance resulting from the contact between the ridges and valleys of the finger and the sensor. Such scanners are more resistant to deception, but recognition may fail if the finger is heavily soiled or damaged.

A similar situation occurs with face and voice recognition: imperfect algorithms may grant access based on a photo or recording, or deny access if the user's appearance or voice has changed.

Although biometric identification is the most personalized method, potential non-standard situations must be taken into account. Therefore, if these risks cannot be minimized, it is advisable to employ an additional independent authentication method based on the knowledge or possession factor, such as verification via SMS or a messaging app.

Mathematical reliability and ways to improve model. The system security increases not linearly but exponentially with the addition of each independent factor. Such systems typically use a combination of "something I know" with "something I am" (e.g., a password and a fingerprint) or "something I possess" with "something I

am" (e.g., an RFID tag and a fingerprint) [3]. In the proposed model, the probability of intrusion P can be calculated using the formula:

$$P=P1P2P3, \quad (1)$$

where P_1, P_2, P_3 are the probabilities of intrusion at each respective stage.

To integrate all subsystems, a centralized management approach is proposed, utilizing energy-efficient microcontrollers, such as the ESP32. This allows the implementation of an energy-management system, in which most of the device remains in deep-sleep mode and wakes up only in response to sensor events or external commands [7]. In addition to energy optimization, optimized cryptographic algorithms and streamlined key procedures provide a sufficient level of security while imposing minimal computational load on the microcontroller, thereby enhancing the device's autonomy.

The final stage of the approach is the establishment of a reliable communication channel between the system and its owner. In modern IoT architectures, the zero-trust model is increasingly applied, requiring continuous verification of every request regardless of its source [8]. The use of modern network protocols and edge computing ensures the journaling of interaction history, minimizes the risk of system component compromise, and reduces reaction delays.

Additionally, one of the most promising approaches to enhancing system reliability is the application of anomaly detection algorithms to sensor data streams, enabling rapid responses to atypical events or intrusion attempts. The integration of statistical methods with AI algorithms significantly improves the effectiveness of access monitoring systems for IoT devices [9].

The use of machine learning techniques allows the creation of adaptive models of user behavior and the identification of atypical access scenarios. Classification and anomaly detection algorithms increase the accuracy of threat detection compared to rigid rule-based mechanisms, creating conditions under which the compromise of a single factor (e.g., password exposure) does not result in the compromise of the entire system.

This approach addresses two key identification challenges: the false acceptance rate (FAR) – the probability of mistakenly granting access to a third party – and the false rejection rate (FRR) – the probability of denying access to the owner [5].

Conclusion. The proposed methods establish a holistic development model in which mechanical reliability is complemented by intelligent event analysis and multi-factor user verification. The reliability of the model is ensured through the sequential use of three independent authentication factors, as well as AI-based anomaly detection algorithms applied to both data streams and system operation. This approach helps mitigate issues such as FAR and FRR. An important feature of the model is its solution to the energy-efficiency challenge through the use of modern energy-efficient microcontrollers, such as the ESP32, operating in deep-sleep mode. This enables the creation of an access control system that effectively counters both traditional intrusion techniques and modern security threats.

REFERENCES

1. Novais L., Naia N., Azevedo J., Cabral J. Let's Get Cyber-Physical: Validation of Safety-Critical Cyber-Physical Systems. *IEEE Access*. 2024. Vol. 12. pp. 142569-142581. URI: https://doi.org/10.1109/ACCESS.2024.3470216.
2. Bamashmos S., Chilamkurti N., Shahraki A.S. Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment. *Sensors*. 2024. Vol. 24. Art. 3575. URI: https://doi.org/10.3390/s24113575.

3. Sarbishaei G., Masoud A.M.A., Jowshan F., Khakzad F.Z., Mokhtari H. Smart Home Security: An Efficient Multi-Factor Authentication Protocol. *IEEE Access*. 2024. Vol. 12. pp. 106253-106272. URI: https://doi.org/10.1109/ACCESS.2024.3437294.
4. Alotaibi A., Aldawghan H., Aljughaiman A. A review of the authentication techniques for internet of things devices in smart cities: opportunities, challenges, and future directions. *Sensors*. 2025. Vol. 25. No. 6. Art. 1649. URI: https://doi.org/10.3390/s25061649.
5. Ayeswarya S., Singh K.J. A Comprehensive Review on Secure Biometric-Based Continuous Authentication and User Profiling. *IEEE Access*. 2024. Vol. 12. pp. 82996-83021. URI: https://doi.org/10.1109/ACCESS.2024.3411783.
6. Lastre J.K., Ko Y., Kwon H., You I. Evaluating Transport Layer Security 1.3 Optimization Strategies for 5G Cross-Border Roaming: A Comprehensive Security and Performance Analysis. *Sensors*. 2025. Vol. 25. No. 19. Art. 6144. URI: https://doi.org/10.3390/s25196144.
7. Serepas F., Papias I., Christakis K., Dimitropoulos N., Marinakis V. Lightweight embedded IoT gateway for smart homes based on an ESP32 microcontroller. *Computers*. 2025. Vol. 14. No. 9. Art. 391. URI: https://doi.org/10.3390/computers14090391.
8. Hasan S., Amundson I., Hardin D. Zero-trust design and assurance patterns for cyber-physical systems. *Journal of Systems Architecture*. 2024. Vol. 155. Art. 103261. URI: https://doi.org/10.1016/j.sysarc.2024.103261.
9. Dhanushkodi K., Thejas S. AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. *IEEE Access*. 2024. Vol. 12. pp. 173127-173136. URI: https://doi.org/10.1109/ACCESS.2024.3493957.