Технічні науки

UDC 004

Dashevskyi Artem

Independent Researcher

Дашевський Артем

незалежний дослідник

INTELLIGENT AUTHENTICATION BASED ON USER BEHAVIOR AND BIOMETRICS
ІНТЕЛЕКТУАЛЬНА АВТЕНТИФІКАЦІЯ НА ОСНОВІ ПОВЕДІНКИ КОРИСТУВАЧА ТА БІОМЕТРІЇ

Summary. *Intelligent authentication based on user behavior and biometrics is becoming a vital tool for ensuring data security. This article focuses on the advantages and disadvantages of these technologies, as well as their application in various fields, including financial services, healthcare, and government institutions. Issues such as reliability, accuracy, and usability are explored, alongside potential risks associated with biometric data breaches and violations of privacy. The article also presents statistical data on the use of various biometric authentication methods, the prevalence of these technologies, and the number of biometric data leaks.*

Key words: *biometrics, authentication, intelligent systems, cybersecurity, user profile, social sectors, human behavior.*

Анотація. *Інтелектуальна автентифікація на основі поведінки користувача та біометрії стає важливим інструментом забезпечення інформаційної безпеки. У статті розглянуто переваги та недоліки відповідних технологій, а також сфери їх застосування, включно з фінансовими сервісами, охороною здоров'я та державними установами.*

Аналізуються питання надійності, точності й зручності використання, а також потенційні ризики, пов'язані з витоком біометричних даних і порушенням конфіденційності. Представлено статистичні дані щодо використання різних методів біометричної автентифікації, їх поширеності та випадків витоку даних.

Ключові слова: *біометрія, автентифікація, інтелектуальні системи, кібербезпека, профіль користувача, соціальні сфери, поведінка людини.*

Introduction. *Modern society is increasingly dependent on digital technologies. Under these conditions, information protection becomes a critically important task for individuals, companies, and government organizations. Cybersecurity is aimed at protecting computer systems, networks, and data from unauthorized access, alteration, destruction, or theft. This field includes both technical and organizational measures that regulate digital behavior and prevent potential incidents. According to ISO/IEC 27001, information security is defined as the preservation of confidentiality, integrity, and availability of information. Over the past decade, the field of computer security has evolved alongside the changing nature of technologies. Computer security encompasses measures and control mechanisms that ensure the achievement of information security objectives—such as confidentiality, integrity, and availability—regarding hardware and software, firmware, and processed, stored, or transmitted information.*

Authentication is the process of verifying whether a user truly is who they claim to be. This includes methods such as unlocking a smartphone using a fingerprint or confirming a transaction via FaceID. Nowadays, user authentication presents both a problem and a challenge that is becoming increasingly relevant [5]. For an online banking system, it is crucial to ensure the security of user accounts and protect their assets and personal information from intruders, as the data stored in the system is highly confidential.

There are many authentication methods. In general, they can be classified into knowledge-based, possession-based, and biometric-based methods. Naturally, each method has its own characteristics (strengths and weaknesses), and the choice of the most suitable authentication approach depends on the environment. Identification, in turn, is a process in which the system attempts to determine who is in front of it by comparing personal data to an existing database. Examples of such systems include video cameras with facial recognition capabilities and automated access control systems in office buildings. The main goal of identification is to establish a person's identity, rather than merely confirm it. Biometric data is used in a wide range of fields—from mobile applications and government institutions to private companies and transportation systems. Biometrics can be applied for information protection, building access control, and many other purposes.

Information systems accumulate, process, and transmit various types of information, the loss or distortion of which can lead to significant consequences [1, p. 86]. Therefore, it is critically important to ensure reliable user authentication. This article will examine in detail the approach based on biometric authentication. Biometric authentication systems are becoming increasingly popular in today's security solutions market. A statistical analysis will be conducted on the volume of biometric authentication usage.

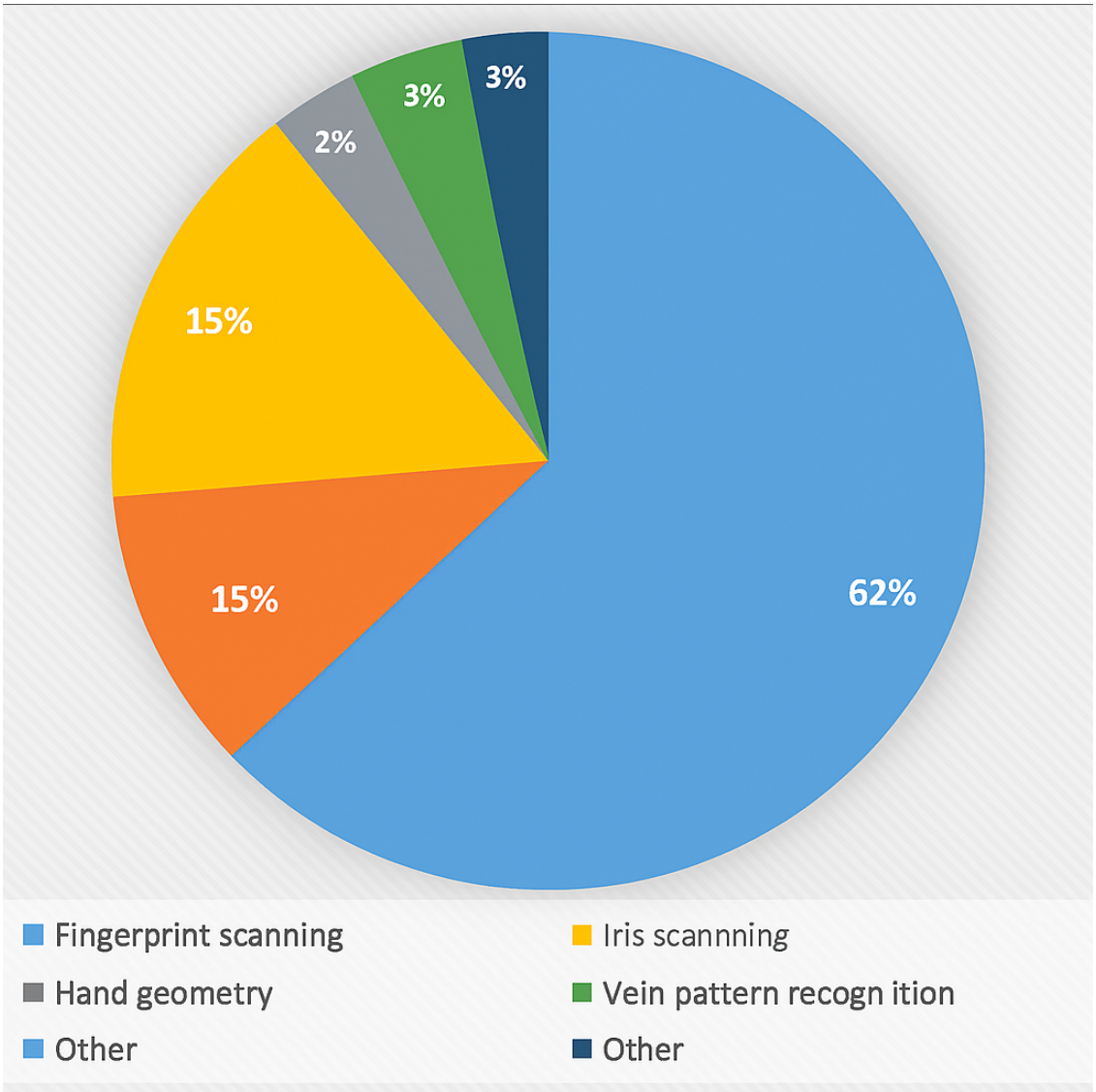


Fig. 1. Percentage Distribution of Various Biometric Authentication Methods

Biological biometrics include unique traits inherent to a person that remain virtually unchanged throughout life—for example, DNA. This method is more commonly used in forensics and scientific research than in cybersecurity, making it more characteristic of investigative scenarios.

Morphological biometrics are based on external physical characteristics, such as fingerprints, facial structure, ear contours, or iris patterns. This type of biometrics is widely applied in modern technologies, including smartphones, video surveillance systems, and banking services.

Behavioral biometrics are associated with a person's individual habits and mannerisms, which can be recorded both in real-world activities and through

interaction with devices. This category includes traits such as handwriting, typing speed, voice timbre, and cursor movements.

Specialized automated programs have been developed to analyze behavioral biometrics by generating a user profile based on behavioral patterns. These systems are used in the banking sector and large corporations to monitor employees and prevent cyberattacks.

Such systems can track which files a user opens on a work computer, at what time they typically access applications, and how fast they type. If significant deviations from habitual patterns are detected, the system alerts cybersecurity personnel. In addition, these programs may automatically block access and request additional authentication [1].

All biometric authentication systems operate on a common principle [3]. During the registration process, a scanner captures a sample of a biometric trait, which is used to create a biometric template for subsequent authentication. This template is stored in a database alongside the user's identifier. During authentication, the sample provided by the user is transformed into a template and compared with the one stored in the database during registration. However, the biometric template database can be subject to risks such as theft, modification, or destruction. In practice, the most common attacks are carried out through the injection of malicious content [4, p. 60]. Therefore, special attention must be paid to the security of such systems.

The collection of biometric data without the subject's consent is unacceptable, except in certain cases stipulated by law. However, in practice, biometric information is often collected without users' knowledge, and there are many reasons for this. Private companies use such data for targeted advertising and for subsequent sale to other organizations and marketers, while government agencies populate their internal databases [4].

Another serious issue lies in the lack of regulation and absence of clear legal standards. In many countries, it remains unclear who is responsible for

protecting biometric data, under what circumstances it may be collected, and how long it may be stored. Due to inadequate safeguards, biometric information may fall into the hands of malicious actors, who then sell this data and use it to carry out cyberattacks.

To improve the reliability of authentication, combined systems are recommended, which involve two-factor authentication—such as combining a biometric scanner with a character-based password or PIN code.

Modern biometric authentication systems are subject to two primary types of errors [5]. A Type I error occurs when the system fails to recognize a legitimate user, resulting in denial of access. A Type II error happens when an attacker is mistakenly identified as an authorized user. These errors can be caused by various factors, which are generally divided into natural limitations and adversarial attacks.

Unlike traditional authentication systems, which require an exact match between the entered password and the one stored during registration, biometric systems grant access based on a sufficient degree of similarity between the provided and stored biometric sample. Because biometric data can vary between the enrollment and authentication phases, this variability may lead to either Type I or Type II errors. A Type I error may occur if two samples from the same user exhibit low similarity. A Type II error can arise if biometric samples from different users show high enough similarity for the system to mistakenly accept an unauthorized user.

Intelligent authentication continues to expand into more areas of daily life, and Figure 2 shows statistical data on the adoption of this technology across various sectors.

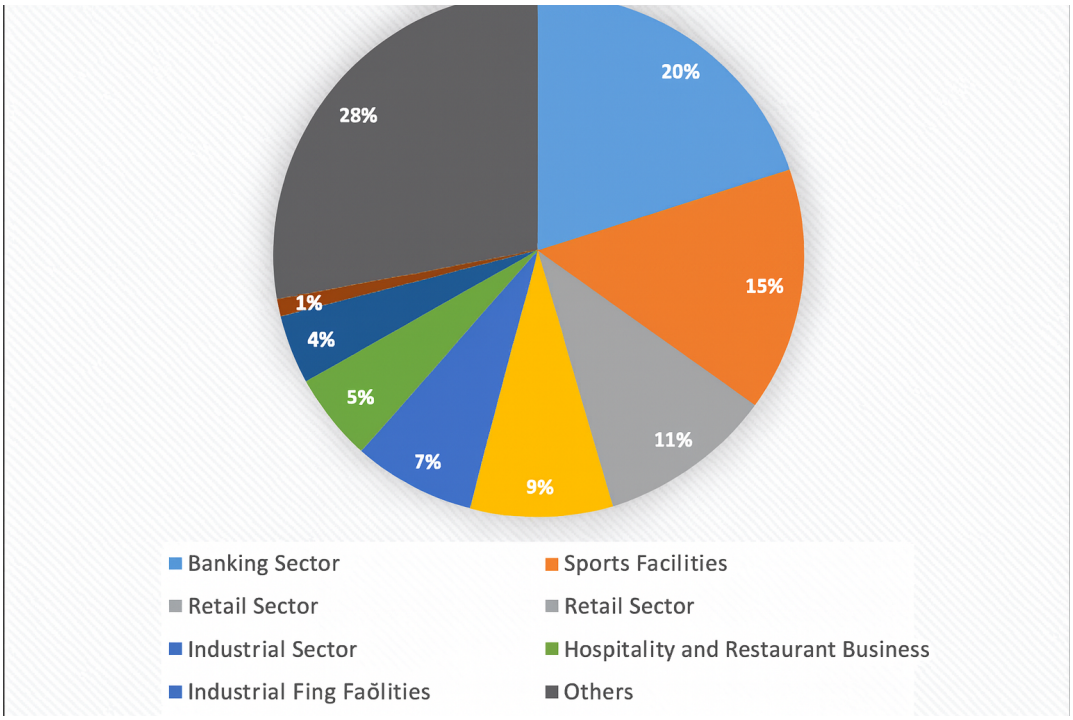


Fig. 2. Prevalence of Intelligent Authentication Deployment

At present, biometric technologies have not yet become a widely demanded service among the general population, and their implementation is mainly initiated by government bodies. The primary global application of biometrics is in access control. The state acts as the main operator in this domain, issuing international passports and managing data within the Unified Biometric System. Government support and the introduction of new regulations in the field of biometrics are driving the active development of this market within the country [6].

Currently, the range of biometric technology applications is expanding. In the near future, users will have access to services such as fare payments in regional subway systems, boarding long-distance trains, service at multifunctional government centers without passports, age verification when purchasing age-restricted products, and hotel check-ins without presenting documents. In these cases, biometrics serves as an alternative to traditional paper documents, cards, passes, and physical visits to public service offices.

Due to the widespread implementation of intelligent authentication and the

accumulation of large volumes of biometric data, the risks of data breaches have significantly increased in recent times. (See Figure 3.)

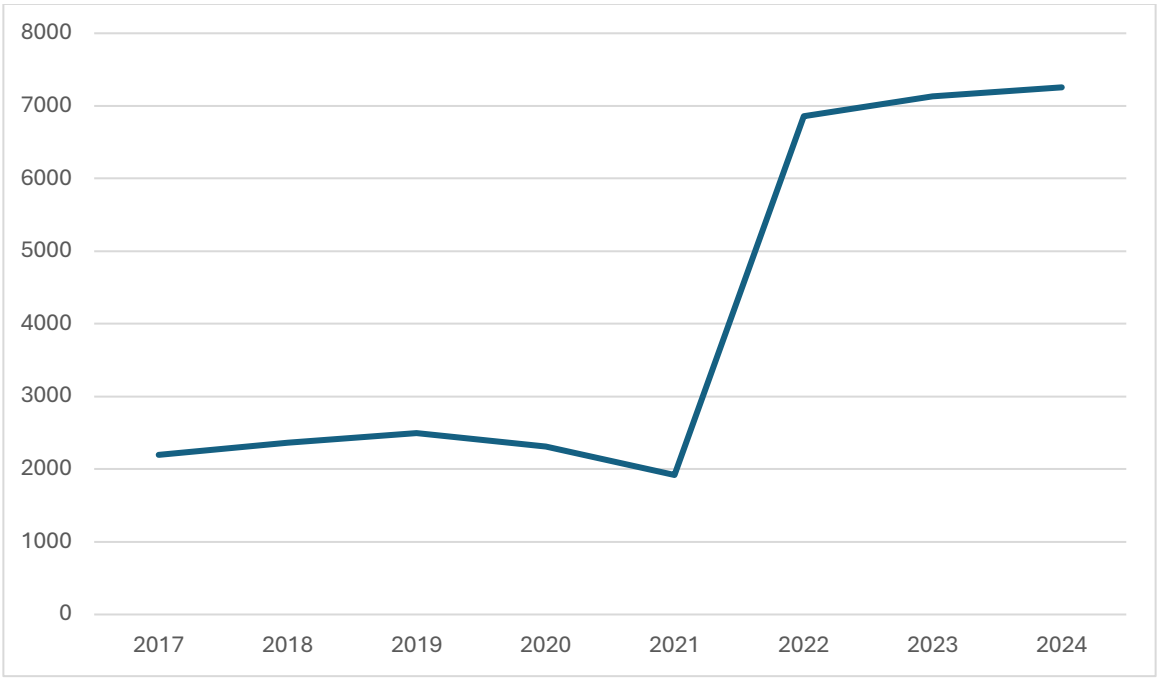


Fig. 3. Number of Biometric Data Breaches Worldwide

Information protection requires not only compliance with legislative obligations by data operators, but also vigilance from the data subjects themselves.

The following measures are recommended:

Implementation of firewalls to restrict unauthorized access to large volumes of data.

Deployment of identification and authentication systems for employees with data access privileges.

Maintaining logs of all actions performed by data handlers to track operations conducted on protected information.

Installation of antivirus software to protect against malware.

Application of cryptographic techniques to encrypt data both at rest and in transit.

Adoption of physical data leakage prevention measures, such as protection against screen capturing, audio recording, and interception of electromagnetic

emissions.

While these measures require significant financial investment, they have already been implemented in most government institutions and large enterprises. However, small companies—especially those providing services to citizens—remain at risk. Often, they are overlooked by supervisory authorities like Roskomnadzor, as they may not register as data operators. Even if registered, developing a technical protection system for personal data repositories may be prohibitively expensive for many. This highlights the need for individuals to exercise caution when choosing service providers and engaging with them.

References

1. Kissel, R. (2013). *Glossary of Key Information Security Terms*. Maryland: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7298r2

2. Stapleton, J. J. (2014). *Security without Obscurity: A Guide to Confidentiality, Authentication and Integrity*. Boca Raton: CRC Press.

3. Clarke, N. (2011). *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling*. London: Springer Science & Business Media.

4. Committee on National Security Systems (CNSS). (2015). *CNSSI No. 4009 – National Information Assurance Glossary*. Retrieved from https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

5. Ahmed, A. A., & Traore, I. (2007). A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure Computing, 4*(3), 165–179.

6. Bours, P., & Fullu, S. J. (2009). Login system using mouse dynamics. In *5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2009)* (pp. 1072–1077).

7. Jorgensen, Z., & Yu, T. (2011). On mouse dynamics as a behavioral biometric for authentication. In *Proceedings of the 6th ACM Symposium on*

Information, Computer and Communications Security (ASIACCS '11) (pp. 476–480).

8. Gorodnichy, D. O. (2009). Evolution and evaluation of biometric systems. In *IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009)*.