http://www.moderntechno.de/index.php/meit/article/view/meit38-01-003
DOI: 10.30890/2567-5273.2025-38-01-003

UDC 004.056.55:004.312.6

THE IMPACT OF BIOIDENTIFICATION ON THE SECURITY AND EFFICIENCY OF ACCESS CONTROL SYSTEMS IN CLOUD INFRASTRUCTURE

Denys Drofa
Specialist, Senior Software Developer, Engineering Department,
Smart Barrel, Inc, 7251 NE 2nd Ave Suite 102, Miami, FL 33138,
ORCID: 0009-0000-3721-6460

Abstract. *The relevance of the study is due to the need to improve the security of cloud access control systems in the face of increasingly large amounts of data and risks of unauthorized access. The purpose of the study is to investigate the impact of biometric methods on the security and efficiency of access control systems in cloud infrastructures, as well as to develop recommendations for their integration, taking into account modern challenges and standards. To achieve this goal, system analysis, comparison, and synthesis were used. An analysis of modern scientific sources and practical cases was carried out, which made it possible to assess the effectiveness of biometric technologies and highlight their advantages and limitations. The study found that biometric systems significantly increase the level of identification accuracy and reduce the risks of phishing attacks and abuse typical of traditional methods. It is found that the main problems remain the cost of implementation, technical requirements for data storage and processing, and the risks of compromising biometric information. Ethical issues related to user privacy and legal aspects, in particular the need to harmonize the regulatory framework, are also investigated. The conclusions emphasize the importance of using multi-level encryption, multi-factor authentication, and blockchain to enhance protection. It is recommended that international standards be created to regulate the processing of biometric data and a transparent policy for their use be developed. Prospects for further research include optimization of algorithms for processing heterogeneous data, implementation of hybrid solutions, and expansion of the practical use of biometrics in various fields, such as medicine, finance, and public administration.*

Keywords: *bioidentification, biometric methods, cloud infrastructure, access control, data security, privacy, technical challenges, ethical aspects, legal regulation.*

Introduction.

Modern cloud infrastructure is increasingly dependent on efficient and secure access control systems, as the amount of data stored and processed is growing rapidly. In this context, bioidentification is one of the leading technologies that can provide an increased level of reliability and protection of information resources. The use of biometric data, such as fingerprints, face recognition, or iris analysis, creates new opportunities to improve user identification and authentication processes in access control systems. At the same time, the integration of such technologies into cloud environments is accompanied by a number of technical, legal, and ethical issues that need to be addressed [1]. The significance of this study is due to the need to ensure a

high level of cybersecurity in the face of increasingly high risks of unauthorized access to cloud resources. The scientific interest is to study the impact of bioidentification technologies on the accuracy, efficiency and usability of access control systems. The practical significance is determined by the need to develop innovative approaches to integrating bioidentification that will ensure adaptation to scalable cloud architectures and compliance with modern security standards. As a result of the study, it is expected to obtain practical recommendations that will contribute to the improvement of existing solutions and further development of the industry.

Literature review.

The study of the impact of bioidentification on the security and efficiency of access control systems in cloud infrastructure covers a wide range of aspects related to the use of biometric technologies. In the work of K. Chyzhmar, O. Dniprov, O. Korotiuk, R. Shapoval, and O. Sydorenko, the information security challenges caused by the rapid development of information technology are investigated. It has been established that the integration of biometrics significantly reduces the risks of unauthorized access and improves access control to confidential data [1].

K. Merkulova and E. Zhabska focus on the technical implementation of bioidentification systems. In particular, they emphasize the effectiveness of biometrics in rapid user identification and its ability to adapt to scalable systems [2]. O. Lungol analyzes the prospects for the use of biometrics, pointing out its key role in ensuring high authentication accuracy in cloud environments [3].

Z. Rui and Z. Yan emphasize the aspects of security and confidentiality, stressing that the main risk is the possibility of compromising biometric data, but the introduction of multi-level encryption can reduce these risks [4]. S. Harakannanavar and his colleagues, exploring the challenges in biometric systems, emphasize that effective management of biometric databases is a key factor in increasing their reliability [5].

The paper by V. Carmel and D. Akila assesses how biometric technologies in the cloud environment help to counteract identity theft. The authors note that the integration of biometrics provides a high level of protection, especially in remote

environments [6]. R. Alrawili, A. Alqahtani, and M. Khan highlight the practical use of biometrics in healthcare and finance, emphasizing its effectiveness in improving security [7].

The impact of biometric methods on reducing the number of unauthorized accesses is considered by N. Yusuf and his co-authors, confirming their effectiveness in large cloud systems [8]. A. Sarkar and B. Singh emphasize the need to protect biometric templates, revealing that weak protection mechanisms are the main vulnerability of modern systems [9]. U. Gawande and Y. Golhar compare uni- and multimodal systems, finding that multimodal approaches are more effective for complex cloud environments [10].

P. Khare and S. Srivastava analyze the use of artificial intelligence and its impact on the accuracy of voice biometrics, emphasizing its advantages for integration into remote services [11]. S. Hemalatha conducts a systematic analysis of fingerprints, revealing their high accuracy and convenience for corporate cloud systems [12].

S. Sharma and his colleagues study ways to protect the privacy of biometric data, emphasizing the importance of a transparent information management policy [13]. O. Ogbanufo and D. Kim analyze the benefits of using biometrics in financial transactions, establishing a significant reduction in fraud through biometric authentication [14]. G. Dahia and co-authors explore the concept of continuous authentication, which provides dynamic access control in cloud systems [15].

The analysis shows that biometrics significantly improves security, reduces the risk of unauthorized access, and ensures the scalability of access control systems.

Despite significant progress in the research of bioidentification systems, there are still important aspects that require further study. In particular, standardized criteria for comparing the effectiveness of traditional and biometric access control methods have not been developed, which makes it difficult to evaluate them in different scenarios.

The study of modern bioidentification technologies has shown insufficient attention to their impact on cloud system performance, in particular, to the issues of latency and scalability when processing large amounts of biometric data. There is also no detailed analysis of the impact of biometric methods on preventing various types of

attacks, such as database compromise.

Technical, ethical and legal challenges related to privacy and biometric data management remain unaddressed. The diversity of international legislation and the risks of information misuse require the development of uniform approaches. It is important to create adaptive models for integrating biometric systems that take into account the increased workload and ensure compliance with security standards.

This research aims to fill these gaps by developing recommendations for integrating biometric systems, standardizing performance criteria, and creating adaptive solutions that optimize their use in cloud infrastructure, which will help improve the security and efficiency of access control systems.

The purpose of the article is to study the impact of bioidentification technologies on improving the security and efficiency of access control systems in cloud infrastructure, as well as to identify ways to optimize their integration with due regard to modern challenges and requirements.

Objectives of the article:

1) to conduct a comparative analysis of the effectiveness of traditional and biometric access control methods, including their impact on improving security and minimizing the risks of unauthorized access;

2) to analyze modern bioidentification technologies, their application in cloud-based access control systems, and the challenges that arise during implementation, including technical, ethical, and legal ones;

3) to develop recommendations for improving the integration of bioidentification systems into the cloud environment, taking into account their scalability, compliance with security standards, and data privacy.

Results and Discussion.

Traditional access control methods, such as the use of passwords, PINs, and access cards, have long been the basis for ensuring security in information systems. However, their effectiveness is significantly limited by their vulnerability to phishing attacks, theft, or forgery, as well as the need for users to memorize large amounts of data. Biometric methods, such as fingerprints, and face and iris recognition, offer a

more reliable alternative due to the uniqueness of the user's physical characteristics. In a cloud infrastructure, the integration of such technologies can increase security but raises a number of issues related to data privacy, technical requirements, and costs (Table 1).

Table 1- Comparative characteristics of traditional and biometric access control methods in cloud infrastructure

Comparison criteria	Traditional methods	Biometric methods
Reliability	Vulnerable to attacks and abuse	High accuracy and resistance to counterfeiting
Convenience.	Dependence on user memory and physical media	No need for external media
Scalability	Easy to integrate, but difficult to adapt to growth	Require significant resources to scale
Cost.	Low initial costs	High implementation and support costs
Data privacy	Minimal risks	High risk of biometric information leakage

Source: compiled by the author based on [4; 5; 9; 10].

In practice, biometric methods demonstrate significantly higher efficiency in providing access to confidential data, especially in large cloud systems with high security requirements. For example, companies operating in the financial sector are actively implementing bioidentification to protect customer data and transactions. At the same time, traditional methods remain popular for small businesses or low-risk environments due to their affordability and ease of integration. The main advantage of biometrics is its ability to provide a personalized level of protection, but it is accompanied by significant challenges, including privacy and legal regulation. Biometric methods help to reduce unauthorized access by using unique characteristics that cannot be reproduced or faked by conventional means. In cloud infrastructures, this significantly reduces the likelihood of security system bypasses. One of the most important advantages is that these methods significantly complicate attempts at social engineering attacks, such as phishing, which are the main threat to traditional identification systems (Table 2).

Table 2- The impact of biometric methods on security in cloud access control systems

Security aspect	Before the introduction of biometrics	After the introduction of biometrics
Frequency of unauthorized accesses	High due to the possibility of password theft or forgery	Significantly reduced due to the requirement of physical presence
Protection against social engineering attacks	Limited, depends on user awareness	High, excludes the possibility of using stolen data
Identification reliability	Depends on the complexity of the credentials	Guaranteed by unique physical characteristics
Level of threat of data leakage	High due to vulnerability to password database hacking	Depends on the protection of biometric information databases

Source: compiled by the author based on [6; 7; 8].

In today's environment, biometric systems provide a critical level of security, especially in areas where only authorized access to confidential data needs to be guaranteed, such as finance, medicine, or government agencies. For example, the introduction of biometrics in large organizations can reduce the number of attempts to hack into systems through passwords or stolen accounts. In addition, biometrics is actively used to protect remote access to cloud environments, which is key in today's digital landscape. However, the implementation of such systems is accompanied by the risk of compromising biometric databases, which requires the implementation of encryption, two-factor authentication, and other additional security mechanisms. As a result, the impact of biometric methods is manifested in a significant reduction of risks and increased access reliability, but requires a responsible approach to integration.

The main areas of biometric technologies include face, fingerprint, iris, and voice recognition. These methods are being actively integrated into cloud infrastructures due to their potential to automate access processes and reduce the risk of unauthorized intrusion (Table 3).

In practice, these technologies are used to optimize access to confidential information and resources in cloud environments. For example, facial recognition is

used to access accounts in large companies operating in the financial and healthcare sectors, providing both speed and convenience. Fingerprint technology remains the most common due to its relative ease of integration and high accuracy, especially in corporate environments. At the same time, the iris is popular among organizations with high-security requirements, such as government agencies and the military. Voice recognition is being actively integrated into remote services, such as online banking systems, although its effectiveness is limited by its dependence on environmental conditions. In general, biometrics is becoming an integral part of modern cloud systems, but its integration requires significant investment and consideration of data privacy issues.

Table 3 - Modern bioidentification technologies and their characteristics for use in cloud access control systems

Type of biometric technology	Characteristics	Advantages of using in cloud systems	Limitations.
Face recognition	Analyze unique facial features of a user using cameras	High end-user convenience, fast authentication	Vulnerability to counterfeiting through the use of images or videos
Fingerprints	Determining the unique pattern on your fingertips	High accuracy, wide application in devices	Requires physical contact, which can be uncomfortable in some environments
The iris of the eye	Recognizing unique iris patterns with an infrared scanner	The highest level of accuracy among biometric methods	High cost of equipment, low availability for small organizations
Voice recognition	Analysis of unique voice acoustic parameters	Possibility of remote use, does not require additional equipment	Sensitivity to noise background, dependence on the health of the vocal cords

Source: compiled by the author based on [2; 3; 11; 12; 13].

The implementation of bioidentification in the cloud infrastructure is accompanied by a number of challenges that can be divided into technical, ethical and legal aspects [4, pp. 5996-5997]. Technical challenges relate to the integration of complex biometric systems into existing cloud environments. These systems require significant computing resources for processing and storing biometric data, which can cause delays in system operation and reduce its performance [5, p. 3960-3962]. It is also important to ensure the security of the transmission and storage of this data, since any compromise of biometric information databases has much more serious consequences than the leakage of traditional credentials such as passwords.

Ethical challenges are associated with maintaining the privacy of users, as biometric data is unique and cannot be changed in case of theft. This raises questions about the transparency of the collection, processing, and storage of such data, as well as their possible use without the user's consent [10, p. 164-165]. In particular, there is a risk of excessive surveillance of people, which may contradict the principles of privacy and freedom.

Legal challenges include the lack of a clear legal framework for regulating the processing of biometric data in cloud infrastructures. In many countries, data protection laws do not cover specific aspects of biometrics, which creates gaps in regulation [6, p. 549]. In addition, the international nature of cloud systems complicates legal control, as different countries have different approaches to personal data protection. This is especially true for global companies that have to comply with many jurisdictions that sometimes contradict each other.

Thus, the technical, ethical, and legal challenges of implementing bioidentification in the cloud infrastructure are multidimensional and interrelated. Overcoming them requires the development of comprehensive approaches, including the improvement of data protection technologies, the creation of transparent mechanisms for information processing, and the harmonization of legal and regulatory frameworks at the international level.

Improving the integration of bioidentification systems into the cloud environment requires a comprehensive approach that takes into account technical, organizational,

and regulatory aspects. One of the key areas is to optimize the architecture of the systems to ensure their scalability. This may include the use of distributed computing resources and the implementation of containerization technologies to increase flexibility and performance. The integration of biometric methods should take into account the possibility of dynamic load growth, which is especially important for large corporate or public cloud platforms.

Another important aspect is the improvement of data protection standards. It is recommended to introduce multi-level encryption of biometric information both during its transmission and storage. In addition, multifactor authentication systems should be used that combine biometric methods with other forms of verification, such as one-time passwords or tokens. This greatly reduces the risk of data compromise even in the event of data theft.

From an ethical perspective, it is recommended that transparent data processing policies be developed to ensure that users are fully informed about how their biometric data is collected, stored and used. In particular, it is necessary to provide mechanisms for obtaining users' consent and allowing them to withdraw it at any time. It is also important to include measures to minimize the amount of data stored, leaving only the necessary information.

Harmonization of the regulatory framework is also critical. For this purpose, it is advisable to cooperate with international organizations to develop unified standards for the protection of biometric data. In addition, it is necessary to create tools for auditing and certifying bioidentification systems that will confirm their compliance with modern security requirements.

Thus, the integration of bioidentification systems into the cloud environment should be based on innovative technological solutions, transparent data handling policies, and clear legal mechanisms that allow for a balance between efficiency, scalability, and security.

Conclusions and Prospects for Further Research.

It has been established that bioidentification systems have a significant impact on improving the security and efficiency of access control systems in cloud

infrastructures. Biometric methods provide a high level of identification accuracy, reduce the risks of unauthorized access, and minimize the influence of the human factor. The main implementation issues include technical challenges, such as the need for computing resources to process biometric data, ethical issues of privacy, and legal aspects related to the imperfection of the regulatory framework.

It is recommended to improve existing approaches to the integration of biometric systems into cloud platforms through the introduction of multi-level encryption, the use of multi-factor authentication, and the development of biometric data protection standards. The importance of a transparent data processing policy and harmonization of regulatory requirements at the international level is also emphasized.

Further research is aimed at optimizing algorithms for dealing with heterogeneous biometric data, developing adaptive models for processing large amounts of information, and integrating the latest technologies such as blockchain to enhance security. Particular attention should be paid to analyzing the impact of bioidentification systems on various industries, as well as developing hybrid solutions that combine the advantages of traditional and biometric methods.

References

1. Chyzhmar K., Dniprov O., Korotiuk O., Shapoval R., Sydorenko O. State Information Security as a Challenge of Information and Computer Technology Development // Journal of Security and Sustainability Issues. – 2020. – Vol. 9, No. 3. – P. 819-828. DOI: 10.9770/jssi.2020.9.3(8)

2. Merkulova K.V., Zhabska E.O. Systema biometrichnoi identyfikatsii osoby [Biometric Identification System] // Zbirnyky naukovykh prats profesorsko-vykladatskoho skladu DonNU imeni Vasylia Stusa – Collected Scientific Works of the Academic Staff of Donetsk National University named after Vasyl Stus. – 2019. – P. 164-166. Retrieved from: https://jpvs.donnu.edu.ua/article/view/7277 [in Ukrainian] (date of access: 02.01.2025).

3. Lungo O. Biometrychni tekhnolohii v systemakh avtentefikatsii: vykorystannia ta perspektyvy [Biometric Technologies in Authentication Systems: Usage and

Prospects] // Nauka i tekhnika sohodni – Science and Technology Today. – 2024. – Vol. 5 (33). – P. 731-741. DOI: 10.52058/2786-6025-2024-5(33)-731-741 [in Ukrainian]

4. Rui Z., Yan Y. A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification // IEEE Access. – 2019. – Vol. 7. – P. 5994-6009. DOI: 10.1109/ACCESS.2018.2889996

5. Harakannanavar S.S., Renukamurthy P.C., Raja K.B. Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends // International Journal of Advanced Networking and Applications. – 2019. – Vol. 10, No. 4. – P. 3958-3968. Retrieved from: https://www.researchgate.net/publication/333266096_Comprehensive_Study_of_Biometric_Authentication_Systems_Challenges_and_Future_Trends

6. Carmel V., Akila D. A Survey on Biometric Authentication Systems in Cloud to Combat Identity Theft // Journal of Critical Reviews. – 2020. – Vol. 7, No. 3. – P. 540-547. Retrieved from: https://www.researchgate.net/publication/339974479_A_SURVEY_ON_BIOMETRIC_AUTHENTICATION_SYSTEMS_IN_CLOUD_TO_COMBAT_IDENTITY_THEFT

7. Alrawili R., Alqahtani A.A.S., Khan M.K. Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion // Computers and Electrical Engineering. – 2024. – Vol. 119. – P. 109485. DOI: 10.1016/j.compeleceng.2024.109485

8. Yusuf N., Mamman H., Ahmed M. A Survey of Biometric Approaches of Authentication // International Journal of Advanced Computer Research. – 2020. – Vol. 10, No. 47. – P. 96-104. Retrieved from: https://www.researchgate.net/publication/340322823_A_survey_of_biometric_approaches_of_authentication

9. Sarkar A., Singh B.K. A Review on Performance, Security and Various Biometric Template Protection Schemes for Biometric Authentication Systems // Multimedia Tools and Applications. – 2020. – Vol. 79. – P. 27721-27776. DOI:

10.1007/s11042-020-09197-7

10. Gawande U., Golhar Y. Biometric Security System: A Rigorous Review of Unimodal and Multimodal Biometrics Techniques // International Journal of Biometrics. – 2018. – Vol. 10, No. 2. – P. 142-175. DOI: 10.1504/IJBM.2018.091629

11. Khare P., Srivastava S. Enhancing Security with Voice: A Comprehensive Review of AI-Based Biometric Authentication Systems // International Journal of Research and Analytical Reviews. – 2023. – Vol. 10, No. 2. – P. 398-403. Retrieved from: https://www.researchgate.net/publication/382623983_Enhancing_Security_with_Voice_A_Comprehensive_Review_of_AI-Based_Biometric_Authentication_Systems

12. Hemalatha S. A Systematic Review on Fingerprint-Based Biometric Authentication System // 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE). – 2020. – P. 1-4. DOI: 10.1109/ic-ETITE47903.2020.342

13. Sharma S.B., Dhall I., Nayak S.R., Chatterjee P. Reliable Biometric Authentication with Privacy Protection // Advances in Communication, Devices and Networking. – Springer. – 2023. – Vol. 902. – P. 285-299. DOI: 10.1007/978-981-19-2004-2_21

14. Ogbanufo O., Kim D. Comparing Fingerprint-Based Biometrics Authentication Versus Traditional Authentication Methods for E-Payment // Decision Support Systems. – 2018. – Vol. 106. – P. 1-14. DOI: 10.1016/j.dss.2017.11.003

15. Dahia G., Jesus L., Pamplona Segundo M. Continuous Authentication Using Biometrics: An Advanced Review // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2020. – Vol. 10, No. 4. – P. e1365. DOI: 10.1002/widm.1365

The article has been submitted: 12.02.2025