УДК 004.056.53

ENHANCING INTEGRITY IN BIOMETRIC DATA WITHIN CLOUD SYSTEMS

Сила А.С. (ИТМО)
Научный руководитель – доктор технических наук, доцент Арустамов С.А.
(ИТМО)

Abstract. The integration of biometric authentication into cloud infrastructures introduces integrity-related risks associated with distributed processing, data transmission, and presentation attacks. It makes the need for integrity controls in cloud-based biometric authentication systems a critical problem because biometric identifiers are non-replaceable once compromised [1]. While usage of deep learning-based methods has greatly assisted in increasing the accuracy of presentation attack detection. Models based on convolutional neural networks (CNNs), attention mechanisms and transformer architectures have been shown to offer good performance in both feature extraction for the user's biometric data and the detection of spoofed attempts [2,3]. But still many current biometric systems are designed only for recognition accuracy, they do not generally contain sufficient structured integrity assessment mechanisms that would assist with adaptive decision-making that takes risks into account in a cloud environment. This research presents a conceptual framework for enhancing integrity in cloud-based biometric authentication systems.

Main Part. Cloud biometric authentication typically involves client-side data acquisition, transmission through network channels, and processing in remote infrastructure. Each step presents the potential for risks (e.g., replay attacks, spoofing, and manipulation of the data or the results) [1]. There has been limited exploration of the implementation of international standards (e.g., ISO/IEC 30107) that define the principles and evaluation criteria for presentation attack detection [4]. The additional uncertainty factors present in cloud-based systems, including transmission stability, model confidence calibration, and infrastructure variability, must also be taken into consideration.

The proposed research aims to design a Cloud Biometric Authentication Framework (CBAF) that improves the integrity of biometric authentication by incorporating machine-learning based biometric verification and providing an additional layer of integrity evaluation. CBAF will produce an integrity score, rather than a binary authentication decision, indicating the reliability of the authentication decision. The integrity score will incorporate each model's confidence level, stability in matching the provided biometric sample, and additional contextual validation factors. The performance of the CBAF will be evaluated based on a comparative analysis of baseline architectures using the following: False Acceptance Rate (FAR), False Rejection Rate (FRR), and Standardized Presentation Attack Detection Metrics.

Conclusion. Integrity-oriented biometric authentication enhances the reliability and robustness of cloud-based identity systems. The combination of machine learning verification with structured integrity assessment against predefined integrity checks reduces risk of both spoofing and tampering with data. The proposed framework serves as a secure and scalable base for the development of biometrics-based security solutions for today's cloud environments.

List of references:

1. Jain A.K., Ross A., Prabhakar S. An Introduction to Biometric Recognition // IEEE Transactions on Circuits and Systems for Video Technology. 2004. Vol. 14, No. 1. Pp. 4–20.
2. Yu Z., Qin X., Li X., Zhao C., Lei Z., Li S.Z. Searching Central Difference Convolutional Networks for Face Anti-Spoofing // Proceedings of the IEEE/CVF CVPR. 2020. P. 5295–5304.
3. Liu Y., Stehouwer J., Jourabloo A., Liu X. Deep Tree Learning for Zero-Shot Face Anti-Spoofing // Proceedings of the IEEE/CVF CVPR. 2020. P. 4680–4689.
4. ISO/IEC 30107-1:2016. Information technology — Biometric presentation attack detection — Part 1: Framework. Geneva: ISO/IEC, 2016. P. 22.