SECTION: COMPUTER SCIENCE, COMPUTING AND AUTOMATION.
SEKCJA: INFORMATYKA, OBLICZENIA I AUTOMATYZACJA.

How to cite: Drofa, D. (2023). Integrate Bio-Identification to Strengthen Data Protection in Multi-Tenant Cloud Systems. *Global Innovations and Collaborative Solutions in Contemporary Science* (pp. 444-447). Futurity Research Publishing. https://futurity-publishing.com/international_conference_3

Integrate Bio-Identification to Strengthen Data Protection in Multi-Tenant Cloud Systems

Denys Drofa

Specialist, Senior Software Developer, Engineering Department, Smart Barrel, Inc, 7251 NE 2nd Ave Suite 102, Miami, FL 33138, https://orcid.org/0009-0000-3721-6460

Accepted: December 4, 2023 | **Published**: December 15, 2023 | **Language:** English

Abstract. The paper is devoted to the study of the process of integrating bioidentification to enhance data protection in multi-user cloud systems. A brief overview of the use of biometrics to eliminate the main security problem of cloud services - leakage of personal data of users is given.

Keywords: cybersecurity, biodata, biometrics, authorization, cybercriminals.

Introduction. Nowadays, the number of potential threats to software and Internet users is constantly growing. Especially dangerous are the activities of organized groups of cybercriminals who can use stolen personal information to gain access to data from multi-user cloud services. Since cloud systems are used in all software applications that allow online activities, attackers can cause severe damage to users in this way: from hijacking accounts of gaming platforms to debiting funds to other people's accounts. To protect users, cybersecurity experts have proposed integrating

bioidentification (biometrics) tools into cloud service protection systems, which determines the relevance of this research paper.

Literature review. Currently, the issue of integrating bioidentification to enhance data protection in multi-user cloud systems is not sufficiently studied in Ukrainian academia, although in Ukraine, due to digitalization, it is widely used in all spheres of society. The consequences of neglecting cybersecurity during (and on the eve of) the Russian-Ukrainian war were the failure of the Diia service in January 2022 [3] and the state registers of Ukraine in December 2024.

Results. Cloud systems are based on cloud computing technology, which provides access to services on demand regardless of the time and location of the user. These services include data storage, computing power, and infrastructure for organizations and the IT industry. Based on operational requirements, organizations can scale up or down the service. While cloud computing offers a number of benefits, it lags behind in terms of security protection and stability, which is a major concern for many cyber threat professionals. This leads to the fact that users of cloud systems are reluctant to store important and confidential information in the cloud because of security threats [2]. The use of biometrics as a consequence of biodata integration is constantly growing, as human physical modalities are truly unique, making them an effective barrier to cybercriminals trying to insidiously impersonate users. Unlike names, ID numbers, email addresses, and passwords, biodata is relatively stable, so it is almost impossible to reproduce, as it is based on the unique characteristics of the human body. Imitating biometric data requires specialized equipment, access to which is usually limited by law and the technical capabilities of cybercriminals themselves.

The main characteristics used by cybersecurity specialists to integrate bioidentification into multi-user cloud systems, are shown in Fig. 1.

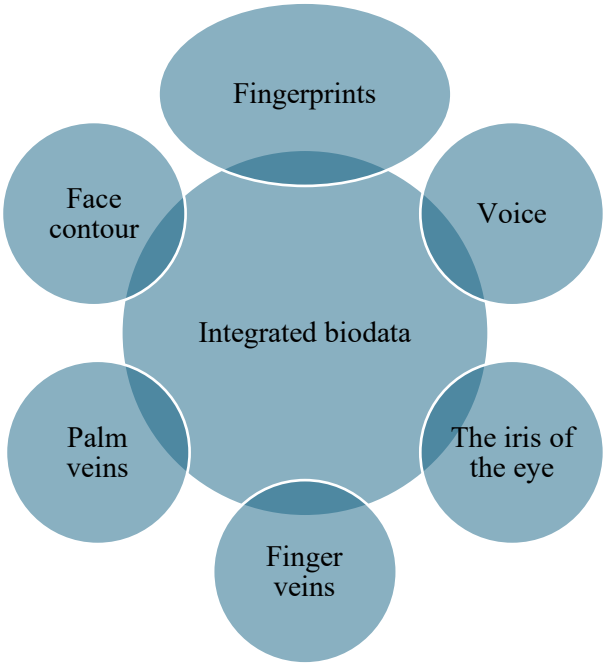

Figure 1. Biological data that can be used for bioidentification

Source: developed based on [4].

The integration of bioidentification into multi-user cloud systems and requires the collection of user biodata into a separate database to be used for further comparison, which creates inconvenience and raises ethical issues. Although all the processes of comparing input data received from a user's device and database elements that record their physical or behavioral characteristics are usually automated, the integration of bioidentification itself imposes additional responsibilities on cloud system operators. The solution to the problem of database security with physical and behavioral characteristics of users is encryption and separation of access rights to information.

The algorithm of the bioidentification process when trying to access a multi-user cloud system is shown in Fig. 2.

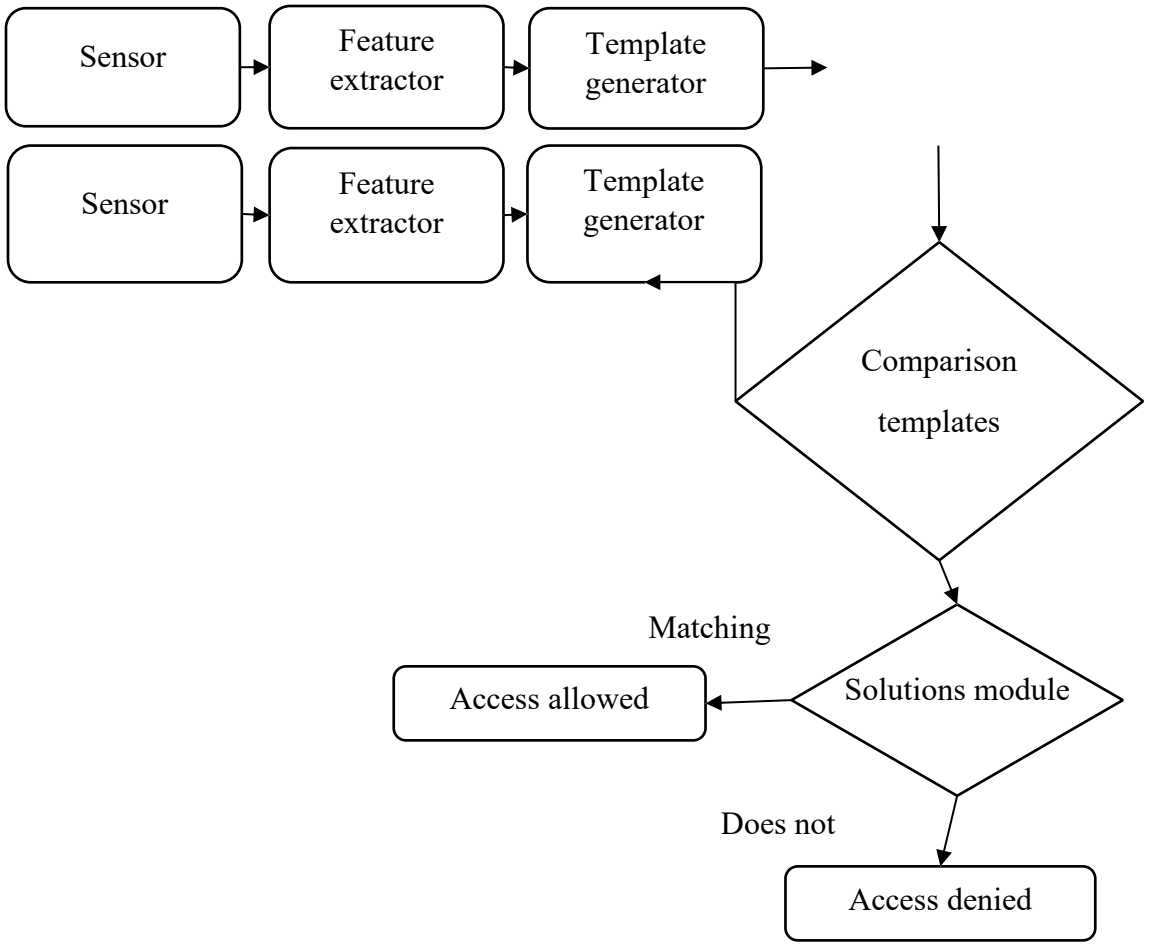

Fig. 2. Algorithm for bio-identification of user of a multi-user cloud system

Source: developed based on [1].

When access to multi-user cloud systems is denied, it is usually possible to log in only with a password and login for a certain period of time, and in some cases, after confirming a code contained in a letter sent to the user's email or phone number.

Conclusions. Thus, as our research has shown, the process of integrating bioidentification to strengthen data protection in multi-user cloud systems is quite complex and requires the availability of technical means with special sensors on users and software capabilities in of cloud service

providers. We have also determined that the main task of bioidentification is to prevent the theft of users' personal data, which is realized by comparing the templates contained in the database on the cloud service operator's server and those provided by users during the biodata scanning process during authorization.

References:

1. 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.

2. Fog computing: Mitigating insider data theft attacks in the cloud /A. Choudhary et al. *International Journal of Advance Research, Ideas and Innovations In Technology.* 2018. Vol. 4. no. 2. P. 1143-1148.

3. Thompson A. Russian National Charged For Conspiring With Russian Military Intelligence To Destroy Ukrainian Government Computer Systems And Data. *United States Department of Justice*. URL: https://www.justice.gov/usao-md/pr/russian-national-charged-conspiring-russian-military-intelligence-destroy-ukrainian

4. Wajhal A., Gupta S. S. Analysis of Biometric Modalities. *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2019)*. Cham, 2020. P. 281-289.