ANALYSIS OF CLOUD AUTHENTICATION SYSTEMS FOR BIOMETRIC DATA

Assylbek D.O.

Almaty Technological University, Almaty, Kazakhstan

Abstract. This article analyzes cloud authentication systems that use biometric data to enhance security. Cloud technologies enable efficient management of biometric data, providing high security and user convenience. However, these systems face challenges related to data storage security, privacy, and infrastructure reliability.

Keywords: Cloud, Biometric Data, Authentication, Security, Privacy, Scalability, Financial Transactions, Encryption

Introduction. This article is dedicated to exploring the use of cloud technologies in biometric authentication, aimed at protecting user data from unauthorized access. The relevance of this topic is due to the fact that cloud-based solutions in biometrics enable the efficient and secure management of biometric data, such as fingerprints, facial recognition, voice, and iris scans. They create a convenient and secure environment for storing and processing data, especially in the context of digital financial transactions, where the speed and accuracy of authentication are crucial in preventing fraud.

Modern cloud systems offer flexibility and scalability to handle a growing number of users, which is vital for large organizations and services with extensive customer bases. These systems also allow for multi-factor authentication and the use of advanced encryption methods to protect data. Cloud-based biometric authentication benefits both organizations and users by providing a high level of security, ease of use, and eliminating the need to remember passwords, which can be easily forgotten or stolen. However, the topic also raises concerns about the privacy and security of biometric data, as such unique data requires high-level protection and compliance with modern information security standards.

Overview. Cloud-based biometric authentication systems cover a wide range of technologies and methods aimed at enhancing access security and preventing unauthorized actions. In recent years, cloud-based biometric technologies have become especially in demand in the financial sector, where security plays a critical

role. Biometrics ensures a high level of security by using unique characteristics of users. The main biometric parameters include fingerprints, facial recognition, voice patterns, iris identification, and behavioral characteristics such as typing speed and movement patterns. These parameters are difficult to forge or steal, making biometric authentication significantly more resistant to hacking than traditional methods.

Cloud technologies provide an additional advantage by allowing biometric data to be stored on remote servers, which ensures scalability and access to data from various devices. For example, in fingerprint authentication, the user's data is first scanned, then transmitted to a cloud server, where it is compared with pre-registered biometric samples. This process may involve encrypting data to protect it from interception and other threats. Similarly, facial recognition, voice, and behavioral data are processed and matched in the cloud, providing convenience and flexibility to the user.

Despite the advantages, cloud-based biometric systems face several challenges. Key issues include ensuring data security and privacy since biometric data cannot be replaced in case of a leak, unlike passwords. Additionally, there is a risk of privacy violations, especially when biometric data may be used by third parties without permission. Another significant concern is the system's resilience: in case of server failure or an attack on cloud infrastructure, access to biometric data may be temporarily restricted, leading to service disruptions and authentication failures. To mitigate these risks, cloud providers use encryption, access control systems, and intrusion detection tools to help prevent data leakage.

Analysis. The advantages and disadvantages of cloud-based biometric authentication systems require careful analysis. The main advantages of these systems are the high level of security and user convenience. Biometric data, such as fingerprints, iris scans, or typing style, are unique to each person, minimizing the risk of forgery. This avoids many vulnerabilities inherent in passwords and other traditional authentication methods that can be stolen, forgotten, or easily hacked. Moreover, using cloud-based biometric authentication provides access to

data from different devices, making this method especially convenient for users who need secure access to their accounts and services from anywhere.

However, cloud-based biometric systems also have drawbacks and challenges. First, an essential aspect is data storage and transmission security. Biometric data is highly sensitive information, so data must be encrypted and protected by access control systems to prevent cyberattacks and leaks. It is critical that biometric information is securely protected not only during transmission but also in storage, especially if it is stored on remote cloud servers vulnerable to attacks by malicious actors. Additionally, strong encryption protocols and regular security updates are essential to ensure that data integrity is maintained. Without adequate protective measures, any breach could lead to significant privacy violations and loss of user trust in the system. Without adequate protective measures, any breach could lead to significant privacy violations and loss of user trust in the system. Furthermore, regulatory compliance, such as adherence to GDPR and other data protection standards, is vital for legally safeguarding sensitive biometric information in cloud environments.

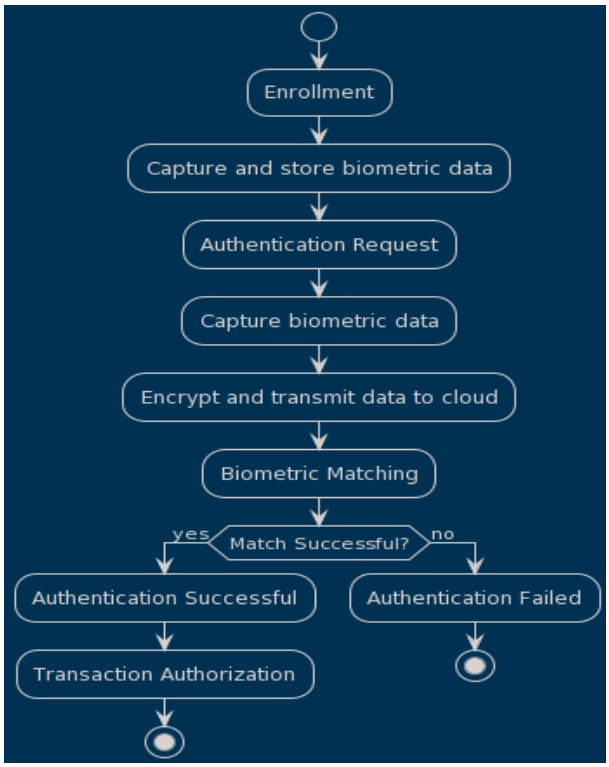

Figure 1. Process of Cloud-Based Biometric Authentication for Financial Transactions

Second, a significant issue is user privacy. Biometric data is unique, and in the event of compromise, it cannot be replaced like a password or PIN code. This creates a high risk for users, especially if data can be used to identify them without their knowledge. Cloud providers offering biometric solutions must strictly adhere to privacy rules and ensure that access to biometric data is only available to authorized persons. Modern encryption methods and multi-factor authentication can help mitigate the risk of unauthorized access and data leakage.

Finally, the third issue is the reliability and resilience of cloud infrastructure. Dependence on cloud servers means that in the event of technical failures or cyberattacks, access to biometric data may be temporarily limited or completely suspended. This can cause problems with authentication and denial of access for users, which is critically important for financial and other sensitive services. To minimize these risks, cloud-based biometric authentication systems must include backup and disaster recovery systems, which will ensure continuous access to biometric data even in the case of temporary disruptions.

In conclusion, cloud-based biometric authentication systems offer numerous benefits in terms of convenience and security, but to achieve effective implementation, issues of privacy, data protection, and resilience must be addressed.

References:

1. Q. Xiao, “Security issues in biometric authentication,” in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, 2005, pp. 8–13.

2. P. Ambalakat, “Security of biometric authentication systems,” *21st Computer Science Seminar*, 2005.

3. S. Venkatraman and I. Delpachitra, “Biometrics in banking security: a case study,” *Inf. Manage. Comput. Secur.*, vol. 16, no. 4, pp. 415–430, Jan. 2008.

4. R. C. Agidi, “Biometrics: the future of banking and financial service industry in Nigeria,” *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 91–105, 2018.

5. S. Ghosh, “Financial inclusion, biometric identification and mobile: unlocking the JAM trinity,” *International Journal of Development Issues*, vol. 16, no. 2, pp. 190–213, Jan. 2017.

6. S. M. Matyas and J. Stapleton, “A Biometric Standard for Information Management and Security,” *Comput. Secur.*, vol. 19, no. 5, pp. 428–441, Jul. 2000.

7. G. L. Masala, P. Ruiu, and E. Grosso, “Biometric Authentication and Data Security in Cloud Computing,” in *Computer and Network Security Essentials*, K. Daimi, Ed. Cham: Springer International Publishing, 2018, pp. 337–353.

8. D. Shah and V. Haradi, “IoT Based Biometrics Implementation on Raspberry Pi,” *Procedia Comput. Sci.*, vol. 79, pp. 328–336, Jan. 2016.