UDC 004.056.53

EFFICIENCY OF USER AUTHENTICATION METHODS IN MOBILE NETWORKS

Forostianko K.Y., AstrakhantsevA.A.
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: forostiankokarina@gmail.com, aastrakhantsev@its.kpi.ua

ЕФЕКТИВНІСТЬ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В МОБІЛЬНИХ МЕРЕЖАХ

Віддалена автентифікація користувачів у мобільних мережах 4G/5G є ключовим елементом забезпечення безпеки в мережах зв'язку. Однак, з огляду на швидкий розвиток технологій та зростання кількості підключених пристроїв, необхідно вдосконалювати методи автентифікації для забезпечення максимальної захищеності. У цій роботі проаналізовані характеристики способів віддаленої біометричної автентифікації користувачів в мобільних мережах і визначений найбільш ефективний за сукупністю критеріїв.

Remote authentication of users in mobile networks is a key element of ensuring security in communication networks. However, given the rapid development of technology and the growing number of connected devices, it is necessary to improve authentication methods to ensure maximum security. This article will analyze various methods of providing remote user authentication in mobile networks.

The threat of attacks on mobile networks and online payment systems is real, and the need for protection has become more pressing than ever. To address these challenges, biometric authentication has emerged as a promising solution for remote authentication. Biometric authentication uses a person's unique biological characteristics to verify their identity. This type of authentication is much more secure than traditional password-based systems, which can easily be compromised by hackers.

The purpose of implementing biometric authentication in mobile networks and online payment systems is to provide users with a higher level of security and to reduce the risk of fraud and other security threats. By using biometric authentication, businesses and individuals can ensure that only authorized users have access to sensitive information and transactions. There are several biometric authentication methods that are suitable for mobile devices, including:

- *Fingerprint recognition.* This method is one of the most commonly used

biometric authentication methods on mobile devices. It works by scanning the user's fingerprint to verify their identity.

- *Facial recognition.* This method uses the front-facing camera of a mobile device to capture and analyze the user's facial features. It is becoming increasingly popular on mobile devices due to its ease of use.
- *Iris recognition.* This method uses the unique patterns of the user's iris to verify their identity. It requires specialized hardware and is not as widely available as other methods.
- *Voice recognition*. This method uses the user's voice to verify their identity. It can be used for speaker verification or speaker identification.

When comparing different biometric authentication methods for mobile devices, several characteristics should be considered. These include:

1. Universality: This refers to the percentage of the population that can use the biometric method.
2. Uniqueness: This refers to the degree of distinctiveness of the biometric trait.
3. Permanence: This refers to the stability of the biometric trait over time.
4. Performance: This refers to the accuracy and speed of the biometric method.
5. Acceptability: This refers to the level of comfort and ease of use of the biometric method by users.
6. Ease of use: This refers to the simplicity and convenience of the biometric method for users.
7. Long-term stability: This refers to the ability of the biometric method to maintain its accuracy and reliability over an extended period of time.

When making decisions about choosing the best option for a biometric authentication system, it is necessary to determine the importance (priority) of the requirements that apply to the parameters of the biometric authentication system. Algorithms of comparison methods are similar, but if there are differences between them, different criteria for the importance of criteria can be given, which in time can lead to obtaining an incorrect result. Another problem is the degree of consistency of experts' assessments. In the methods of pairwise comparison (tab. 1), the expert expresses his opinion about the ratio of importance of all possible pairs of criteria in the form of intensity of relative importance, which is quantified using a scale of relative importance. The relative degree of superiority (dominance) of one criterion over another is set by the expert based on his knowledge of the real processes that take place in the nodes of the system with biometric characteristics of a person, that is, this quantitative assessment is subjective. Therefore, the vector of priority

coefficients will depend on the number of experts and the level of their experience and qualifications.

Table 1. Comparison of biometric identification methods.

Biometric	Universality	Uniqueness	Permanence	Performance	Acceptability	Ease of use
Face	High	Low	Medium	Low	Medium	Medium
Fingerprint	Medium	High	High	High	Medium	High
Hand geometry	Medium	Medium	Medium	Medium	Medium	High
Iris Scanning	High	High	High	High	Medium	Medium
Retinal Scanning	High	High	Medium	High	Medium	Low
Voice Recognition	Medium	Low	Low	Low	High	High
Signature	Low	Low	Low	Low	High	High
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium
DNA	High	High	High	Low	Low	Medium

According to the method of pairwise comparisons, table 1 was modified to the numeric form and based on it, the best methods was defined. The result showed in table 2:

Table 2. Result of comparisons.

Face	10,3
Fingerprint	**13**
Hand geometry	8,8
Iris Scanning	**11,4**
Retinal Scanning	8,4
Voice Recognition	8,2
Signature	7,3
Hand Vein	7,5
DNA	9,8

Conclusion. According to the results, showed in tab.2, the best biometric authentication method for remote authentication via mobile device would be a fingerprint scan. This method gives the highest result for the criteria listed above and can be recommended for use in mobile networks. The iris method also provides good value and can be used as additional way or for multifactor authentication.

References

1. Private eyes: Secure remote biometric authentication: Ewa Syta; Michael J. Fischer; David Wolinsky; Abraham Silberschatz; Gina Gallegos-García; Bryan Ford. Published in: 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE).
2. A Remote Biometric Authentication Protocol For On-Line Banking: Anongporn Salaiwarakul. DOI: 10.5769/C2013002 OR HTTP://DX.DOI.ORG/10.5769/C2013002.
3. Chen, L., Pearson, S., Vamvakas, A.: Trusted Biometric System. Available at URL http://www.hpl.hp.com/techreports/2002/HPL-2002- 185.pdf (2002).
4. Salaiwarakul, A., Ryan, M.: Analysis of a Biometric Authentication Protocol for Signature Creation Application. Third International Workshop on Security (2008) 231-245.