Implement biometric authentication of users enhancement model and algorithm research

Avezov Erkinjon Sherimmatovich

Named after Muhammad al-Khwarizmi
Tashkent University of Information Technologies
Urgench branch "Telecommunications
Dean of the Faculty of Technology
avazoverkinjon@ubtuit.uz
+998919191300

Bekchanov Faxriddin Atabekovich

Named after Muhammad al-Khwarizmi
Tashkent University of Information Technologies
Urgench branch M951-21 master group
bekchanov_faxriddin@ubtuit.uz
+998973631353

Boburbek Babajanov Farhodovich

Named after Muhammad al-Khwarizmi
Tashkent University of Information Technologies
Urgench branch 912-19 group student
babaj onovboburbek@gmail.com
+998914321545

Musayeva Mukhtasar Zayirjon qizi

Named after Muhammad al-Khwarizmi
Tashkent University of Information Technologies
Urgench branch 912-18 group student
babajonovboburbek@gmail.com
+998938611133

ABSTRACT

This article analyzes the importance of biometric authentication, which is currently evolving, to ensure information technology and security.

Keywords: Authentication, identification, fingerprints, password, PIN, communication lines, connection, GSM, biometric technology.

The areas of computer network automation are developing and expanding, and the importance of data is growing steadily. State secrets, trade, legal and medical secrets As usual, local and corporate networks, in turn, feel the need for these computer technologies. The global network, on the one hand, opens up huge opportunities for e-commerce, but on the other hand, creates the need for reliable security tools to protect corporate data from external access.

For many services, online authentication is still largely done using usernames and passwords. Text password - based authentication suffers from several important security issues, such as low password entropy and poor password management. In addition, several studies have shown that it is difficult to remember passwords that are sufficiently protected, often leading users to choose presumptive structures when creating their passwords.

Authentication is the process of verifying the authenticity of a known user, process, or device. This verification allows the user (process or device) to make sure that it is indeed itself . In the process of authentication , the auditing party is convinced that the audited party is genuine, and the audited party is actively involved in the exchange of information. Typically, a user verifies identification by entering unique, unknown information about themselves (such as a password or certificate).

The purpose of biometric authentication is the automated verification of the identity of a living person by proving that he or she has a unique trait. One type of biometric authentication is physiologically oriented, such as **fingerprint** , **retina** , **face** , **ear** , **hand** or **finger** geometry, and so on. This is usually called "static modality" because it is as if these biological properties change very little or not at all. In addition, biometric features are based on immobile surfaces of the body, whether it is an image of the palm of the hand or a pattern of blood vessels in the hand.

Mutual authentication of subjects in the protection of data channels is performed, ie mutual authentication of subjects communicating with each other via **communication lines** , the authentication procedure is usually performed at the beginning of the session when the connection is established; The term " **connection** " refers to a logical connection (possibly two-way) between two network objects. The purpose of this procedure is to establish contact with the legal entity and ensure that all information reaches the destination.

Any biometric system allows you to recognize a specific pattern and determine the authenticity of the user's specific physiological or behavioral characteristics. The logical biometric system can be divided into two modules: the registration module and the identification module. The first is that the system is responsible for teaching how to identify a particular person. At the registration stage, biometric senometric sensors scan the necessary physiological or behavioral characteristics of a person and create their digital representation. A special module separates the characteristic features of this image and gives it a more compact and expressive look called a template. For facial imaging, such features may be the size and relative position of the eyes, nose, and mouth. The template for each user is stored in a database of biometric systems.

The following features should be considered when comparing and selecting authentication protocols.

- mutual authentication - this reflects the need for mutual authentication between the parties to the exchange of property authentication;
- computational efficiency - the number of operations required to perform the protocol;
- communication efficiency - this feature reflects the number of messages required for authentication and their length;
- the presence of a third party - a trusted symmetric key distribution server or a server that implements a certificate tree for public key distribution;
- The basis of security guarantees - for example, protocols with zero knowledge evidence;
- Confidentiality - This is a way of storing important information.

In the fall of 2016, Kaspersky Lab found at least 12 vendors offering skimmers who could steal fingerprint data on the black market, and at least three researchers working on wrist and rainbow vein detection systems. According to experts, in September 2015, pre-sale testing of the first versions of biometric skimmers on the black market has already been conducted. Then a few errors were found, but the main problem was the use of **GSM** modules for the transmission of biometric data - they could not withstand large amounts of data, that is, newer versions of such skimmers use different, faster data. The company believes that transmission technology.

"Unlike passwords or PINs, which can be easily changed in case of damage, fingerprints or iris patterns cannot be changed. Accordingly, if biometric data once falls into the wrong hands, their subsequent use is fraught with serious risks. That's why they need very reliable protection, "said Olga Kochetova ***, an information security specialist at Kaspersky Lab*** *. " Almost all the information that can be used to identify an individual ."*

Obviously, the quality and reliability of authentication tools should be directly related to the importance of the data. In addition, increasing the performance of the complex is usually accompanied by its growth. Fingerprints In recent years, the process of fingerprint detection has attracted attention as the most widely used biometric technology in the future

Government and civil society organizations around the world have used fingerprints as key personal identifiers. In addition, printed publications are the most accurate, user - friendly and economical biometric biometric feature of computer system identification. This technology protects in the U.S., for example, vehicle administrations, MasterCard, FQI, the Secret Service, the Department of the Treasury, and more. By eliminating the need for passwords for users, fingerprint recognition technology reduces the number of requests to support the service and reduces network management costs.

References:

1. V.F.Shangin Complex protection of information in corporate systems. Moscow ID " FORUM " - INFRA - M 2010.-591 p .
2. G'aniev S. _ K. , Karimov M. _ M. , Tashev K. _ A. _ A xborot security _ Security of information and communication systems. Tashkent, 2009.
3. S.K. G'aniev, M.M. Karimov, K.A. Tashev Information Security. "ALOKACHI" - 2008.-381 pages.

Websites used:

1. https://link.springer.com/search?query=An+algorithm+that+performs+biometric+authentication+of+users&showAll=false .
2. https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=An+algorithm+that+performs+biometric+authentication+of+users&btnG
3. https://newtravelers.ru/uz/asus/klassifikaciya-biometricheskih-sistem-zashchity-informacii-osnovy.html
4. https://answer-id.com/uz/62046585