УДК 004.93.056.5 Student V.A. Yaskevich
Scientific supervisor V.Y. Dokurno (Department of ICC&TT (Intercultural Communication and Technical Translation, BSTU)

BIOMETRIC AUTHENTICATION IN SOFTWARE

In today's dynamically developing digital world, where data breaches and identity theft are upcoming threats, the traditional methods of authentication like passwords and PINs don’t provide adequate security. In response to this challenge, biometric authentication has emerged as a revolutionary solution that harnesses the unique characteristics of individuals to verify their identities. Furthermore, the integration of biometric authentication not only fortifies security measures but also enhances user experience by offering convenient access to digital services.

Biometric authentication operates on the principle of utilizing physical traits or behavioral patterns that are unique to each individual: such as fingerprints, facial characteristics, iris patterns, and behavioral attributes like typing rhythm or voice tone. Those characteristics serve as distinctive markers for identity verification.

Types of Biometric Authentication

Fingerprint Recognition: Among the most prevalent forms of biometric authentication is fingerprint recognition. It involves capturing and analyzing the unique patterns on an individual's fingertips. Widely used in smartphones, laptops, and access control systems, fingerprint scanners offer a reliable and convenient method of authentication.

Facial Recognition: Facial recognition technology employs algorithms to map and analyze various facial features, such as the distance between the eyes, the shape of the nose, and the contours of the face, to create a unique facial signature for each individual. This technology finds applications in device unlocking, surveillance systems, and airport security.

Iris Recognition: Iris recognition utilizes the intricate patterns in the colored part of the eye to verify identity. With its exceptional accuracy and resistance to falsification, iris recognition is employed in high-security environments such as border control checkpoints, secure facilities, and forensic investigations.

Voice Recognition: Voice recognition systems analyze an individual's vocal characteristics, including pitch, tone, cadence, and pronunciation, to create a unique voiceprint for authentication purposes. Used in call centers, virtual assistants, and automated telephone banking systems, voice recognition offers a hands-free method of authentication.

Application in Software

Biometric authentication has affected various aspects of software development, revolutionizing the way users interact with technology and access digital services. It offers the data protection on Mobiles devices by

implementing fingerprint scanners, facial recognition, and iris scanning. Similar purpose is being executed in Computer Security.

Biometric authentication is widely used in the financial sector to secure transactions conducted through mobile banking apps, online payment platforms, and cryptocurrency exchanges, safeguarding against identity theft and fraudulent activities. In healthcare, biometric authentication ensures secure access to electronic health records, medical devices, and healthcare management systems. Regarding enterprise sector, biometric authentication is integrated into enterprise software solutions for employee authentication, access control, time and attendance tracking, and secure document management, enhancing operational efficiency.

Advantages and disadvantages

Referring to the subject of biometric authentication, we cannot fail to mention advantages and disadvantages of this data protection tool. As for benefits – it offers a higher level of security compared to traditional authentication methods, as biometric characteristics are unique, difficult to replicate, and fundamentally tied to the individual. Biometric authentication eliminates the need for users to remember complex passwords or carry physical tokens. It makes user's experience more convenient. Additionally, this way of protection significantly reduces the risk of fraudulent activities such as identity theft, unauthorized access to sensitive information, and financial fraud by accurately verifying the identity of users.

Concerning disadvantages of biometric authentication, the cost of implementation should be mentioned. This requires investment in specialized hardware, software, infrastructure, and training programs. Admittedly, storing enormous personal data could lead to serious breaches of privacy, identity theft. What is more, biometric authentication systems may encounter accuracy and reliability issues due to factors such as variations in biometric characteristics over time, environmental conditions, and technological limitations, leading to false rejections or false acceptances.

Conclusion

In conclusion, biometric authentication stands at the forefront of software security, offering reliable protection and user convenience. Its widespread adoption across diverse sectors underscores its impact on digital identity management, access control, and transaction security. However, addressing challenges such as privacy concerns, cost considerations, and technological limitations is the obligation to ensure the continued evolution and widespread acceptance of biometric authentication as a cornerstone of modern cybersecurity practices. As technology continues to advance, biometric authentication is poised to play an increasingly integral role in shaping the future of secure and seamless digital interactions.