MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

2-SON 1(2)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O'ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG'ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali.
Chop etish tili: O'zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo'lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo'nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №2
Vol.1, Iss.2, 2023 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg'oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O'zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro'yxatdan o'tgan.

Tahririyat manzili:
151100, Farg'ona sh., Aeroport ko'chasi 17-uy, 201A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz
Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG'ONA - 2023 YIL

TAHRIR HAY’ATI

Jurnal quyidagi bazalarda indekslanadi:

OpenAIRE

zenodo

doi digital object identifier

Google Scholar

Crossref

DataCite FIND, ACCESS, AND REUSE DATA

iD ORCID Connecting Research and Researchers

DRJI Directory of Research Journals Indexing

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

THE USE OF BIOMETRIC AUTHENTICATION TECHNIQUES FOR SAFEGUARDING DATA IN COMPUTER SYSTEMS AGAINST UNAUTHORIZED ACCESS OR BREACHES

Mirzakarimov Baxtiyor Abdusalomovich,
teacher,
Fergana branch of the Tashkent University of
Information Technologies named after Muhammad al-Khorazmi

Xayitov Azizjon Mo’minjon o’g’li,
Assistant,
Department Of Intelligent Engineering Systems,
Fergana Polytechnic Institute, Fergana, Uzbekistan

Abstract: In today’s world, the focus of information security and cyber security is to minimize the risks associated with traditional password-based security solutions. Passwords have long been recognized as a weak link in security systems. Biometric authentication, on the other hand, offers a solution by linking personal identification with our physical features and behavioral patterns. With the increasing need for secure information exchange, there is a growing demand for implementing biometric authentication methods that utilize biological traits to safeguard computer systems.

Keywords: Biometric, biological biometric, biometric security, biometric authentication, biometric identification information systems, users of information systems.

Introduction. Biometric identification is gaining widespread popularity in personal and corporate security systems as a cutting-edge solution for protecting data. Despite the fact that each individual has a unique biological and behavioral identity, it may seem incredible that biometrics can accurately and effectively capture and authenticate these traits. However, biometric identification has the potential to be used as a standalone authentication method in many applications.

As a result of the increasing need for stronger security measures, biometric identification is becoming a popular choice for many organizations seeking to secure their data and systems. By utilizing unique physical and behavioral characteristics, such as fingerprints, facial recognition, and voice patterns, biometric identification provides a high level of security that cannot be replicated or easily compromised. Moreover, biometric identification is also convenient and easy to use, which makes it an attractive option for many users. Consequently, biometric identification has the potential to revolutionize the security landscape, providing a reliable and efficient way of authenticating individuals and protecting sensitive data.

Literature review and methodolgy. The study of existing research on the use of biometric authentication techniques to protect computer systems from unauthorized access or breaches. The approach or method used to investigate and analyze the effectiveness of biometric authentication techniques in securing data in computer systems.

In this article, we explore the basics of how to use biometric security to store information in cyber security. To implement these plans, we answer biometric questions: What does biometric mean? What is biometric data? What is a biometric scanner? What are the risks of biometric security? How can we make biometrics more secure?

Results. What is biometrics? Biometrics refers to biological measurements or physical characteristics that can be utilized to identify individuals. Fingerprint mapping, facial recognition, and retinal scanning are some of the most well-known forms of biometric technology. However, there are several other unique identifiers that researchers have identified, such as the shape of the ear, a person’s gait and posture, unique body odors, veins in the hands, and even facial wrinkles.

By utilizing these unique features, biometric technology offers an increased level of security

https://doi.org/10.5281/zenodo.7979123

https://journals.indexcopernicus.com/search/article?articleId=3609122

compared to traditional methods such as passwords or PINs. Since biometric identifiers are unique to each individual and cannot be easily replicated or forged, they provide a reliable and efficient way of authenticating individuals and protecting sensitive data. Moreover, the use of biometric technology is becoming more prevalent as it is also convenient and easy to use, making it an attractive option for many users.

Overall, biometric technology has the potential to revolutionize the security landscape by providing a reliable and secure way of identifying individuals and safeguarding sensitive data[1].

Three Types of Biometric Security: Biometric security can be broadly categorized into three types based on the type of biometric identifiers used for authentication: physiological, behavioral, and combination biometrics.

1. Physiological Biometrics: This type of biometric security utilizes unique physical characteristics of individuals for authentication. Examples include fingerprint recognition, iris scanning, facial recognition, hand geometry, and DNA analysis. These biometric identifiers are highly reliable and difficult to forge or replicate, providing a high level of security.

2. Behavioral Biometrics: This type of biometric security focuses on the unique behavioral patterns of individuals for authentication. Examples include keystroke dynamics, gait recognition, voice recognition, and signature verification. Behavioral biometrics are useful in situations where physiological biometrics are not practical or possible, such as remote authentication or continuous monitoring of user activity.

3. Combination Biometrics: This type of biometric security uses a combination of physiological and behavioral biometric identifiers for authentication. This approach provides an even higher level of security by combining the strengths of both types of biometric identifiers. For example, a system may require both fingerprint recognition and voice recognition for authentication.

Overall, the choice of biometric security type depends on the specific use case and requirements of the system. By leveraging the strengths of biometric authentication, organizations can enhance security and protect sensitive data from potential threats.

Biological biometrics are used at the genetic and molecular level. These may include characteristics such as your DNA or blood, which can be assessed through a sample of your body fluids[2]. Morphological biometrics include the structure of your body. More physical features such as eyes, fingerprints or the shape of your face can be mapped for use with security scanners. Behavioral biometrics are based on patterns that are unique to each individual. How you walk, talk, or even type on the keyboard can reveal your personality if these patterns are observed.

Biometric Security Jobs: The role of biometric identification in our everyday security is increasing. Physical characteristics are relatively fixed and individual - even with twins. Each person’s unique biometric identity can be used to replace or at least augment password systems for computers, phones, and access-restricted rooms and buildings. Once biometric data is captured and mapped, it is stored for comparison with subsequent access attempts. Often this data is encrypted and stored inside the device or on a remote server. In other words, biometric security means that your body is the "key" to unlock access[3].

Biometrics are mainly used because of two main advantages:

- Ease of use: Biometrics are always with you and cannot be lost or forgotten.
- Hard to steal or impersonate: Biometrics cannot be stolen like passwords or keys. While these systems aren’t perfect, they hold tons of promise for the future of cybersecurity[4].

Some overviews of biometric security:

- Voice recognition
- Fingerprint scan
- Recognize the face
- Recognition of Iris
- Heart rate sensors

In practice, biometric security has been effectively used in many fields. Complex biometric data is used to protect confidential documents and valuables. Citibank already uses voice recognition, and Britain’s Halifax Bank is testing heartbeat devices to verify customers’ identities. Ford is even considering installing biometric sensors in cars[5].

Biometric data is included in electronic passports around the world. In the United States, electronic passports contain a chip containing a digital photograph of a person’s face, fingerprint, or iris, as well as technology that prevents unauthorized data readers from reading the chip and erasing the data. As these security systems are developed, we are seeing the pros and cons in real time.

https://doi.org/10.5281/zenodo.7979123

https://journals.indexcopernicus.com/search/article?articleId=3609122

Biometrics - identification and privacy issues. Although biometric authentication is considered convenient, some privacy advocates are concerned that it poses a threat to personal privacy as it allows for easy collection of personal information without consent. One of the most common forms of biometric authentication is facial recognition, which is now widely used in Chinese cities for everyday transactions, and CCTV cameras in cities such as London, New York, Chicago, and Moscow are linked to facial recognition databases to help local police fight crime.

Furthermore, new technology is being developed, such as a camera at Carnegie Mellon University that can scan irises from a distance of up to 10 meters. Dubai Airport has also introduced a facial recognition system, where travelers passing through a tunnel in a virtual aquarium are photographed by 80 cameras. Similar systems are available at other airports around the world, including Helsinki, Amsterdam, Minneapolis-St. Paul, and Tampa.

The concern among privacy advocates is that all this personal data is stored in one place, increasing the fear of constant surveillance and potential misuse of data. As technology continues to advance, it is crucial for policymakers to strike a balance between the convenience of biometric authentication and the protection of individual privacy rights. [6].

Ways to protect biometric identification: To mitigate privacy and security risks, biometric systems need extra measures to ensure the protection of personal data. Multiple means of authentication such as life detection and encrypted matching coded patterns are often required to make unauthorized access challenging. Additional features such as age, gender, and height can also be incorporated into the biometric information to prevent hacking attempts. Biometric information can serve as a reliable substitute for usernames in a two-factor authentication strategy, increasing the security of personal data. [7].

As IoT devices continue to become more prevalent, the use of two-factor authentication is becoming increasingly important. This powerful combination of security measures provides an added layer of protection to prevent data breaches. Furthermore, employing a password manager to store traditional passwords can provide an additional level of security to safeguard sensitive information.

Conclusion. Biometric authentication is an increasingly popular method for verifying identity in cybersecurity systems. Combining physical and behavioral signatures with other authentication methods provides the most robust security available. Currently, this approach is more effective than relying solely on character-based passwords for verification. Biometric technology presents highly attractive security solutions due to its convenience and resistance to replication. Despite the risks associated with this technology, it offers significant benefits for cybersecurity. Furthermore, biometric systems are constantly evolving, which ensures that they will remain relevant and useful for years to come. As such, it is likely that biometric authentication will continue to be an important component of cybersecurity for the foreseeable future..

References:

1. Kayumov, A. (2023). THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE EDUCATIONAL PROCESS. Потомки Аль-Фаргани, 1(1), 35–38. извлечено от https://al-fargoniy.uz/index.php/journal/article/view/5

2. Olim, O., & Mokhichkehra, B. (2022). FEATURES OF MULTIPARTY SYSTEM IN UZBEKISTAN AND TURKEY: COMPARATIVE ANALYSIS. Web of Scientist: International Scientific Research Journal, 3(10), 1312-1321.

3. Ionin A. A. et al. Lasers on overtone transitions of carbon monoxide molecule //Laser Physics. – 2010. – Т. 20. – С. 144-186.

4. KONEV, Y., KOCHETOV, I., KURNOSOV, A., & MIRZAKARIMOV, B. (1994). CALCULATION OF CO LASER KINETICS WITH ALLOWANCE FOR MULTIPHOTON VV EXCHANGE. KVANTOVAYA ELEKTRONIKA, 21(2), 133-136.

5. R. Zulunov, R., & Soliev, B. (2023). IMPORTANCE OF PYTHON LANGUAGE IN DEVELOPMENT OF ARTIFICIAL INTELLIGENCE. Потомки Аль-Фаргани, 1(1), 7–12. извлечено от https://al-fargoniy.uz/index.php/journal/article/view/3.

6. Р. Зулунов, А.Тиллаволдиев. Использование технологий искусственного интеллекта в образовательном процессе. Periodica Journal of Modern Philosophy, Social Sciences and Humanities, 2022, v.12, Nov, p.137–142.

7. Musayev X.SH., Ermatova Z.Q., KOTLIN DASTURLASH TILIDA KORUTINLAR BILAN ISHLASHNI TALABALARGA O 'RGATISH

https://doi.org/10.5281/zenodo.7979123

https://journals.indexcopernicus.com/search/article?articleId=3609122

//Journal of Integrated Education and Research. – 2022. – Т. 1. – №. 6. – С. 119-125.

8. Ogli K. A. M. MODERN PROGRAMMING LANGUAGES: CLASSIFICATION AND CHARACTERIZATION //International Journal of Advance Scientific Research. – 2022. – Т. 2. – №. 11. – С. 108-111.

9. Azizjon Mo’minjon o’g X. et al. The Importance of Mathematical Game and Methods in the Formation of Mathematical Concepts in Primary Schools //Journal of Pedagogical Inventions and Practices. – 2022. – Т. 8. – С. 208-211.

10. Холматов А. А. У., Хайитов А. М. Ў. ИЗУЧИТЬ И ИЗУЧИТЬ СВОЙСТВА БАРИЯ И СТРОНЦИЯ-ТИТАНА, СИНТЕЗИРОВАННЫХ В БОЛЬШОЙ СОЛНЕЧНОЙ ПЕЧИ //Oriental renaissance: Innovative, educational, natural and social sciences. – 2021. – Т. 1. – №. 11. – С. 79-93.

11. Xolmatov A. A., Karimov J. X., Xayitov A. M. Effect of crystallizer catalyst on properties of glass-crystalline materials //EPRA International Journal of Research and Development (IJRD). – 2021. – С. 273-275.

12. Muminjonovich, K. A. (2023). SUN’YIY INELLEKTNI RIVOJLANTIRISHDA DASTURLASH TILLARINING RO ‘LI. Journal of new century innovations, 12(4), 159-161.

13. Асраев, М., Собир, Р., & Dadakhanov, M. (2023). ОСОБЕННОСТИ ОБРАБОТКИ И АНАЛИЗА ИЗОБРАЖЕНИЙ РУКОПИСНОГО ВВОДА. Потомки Аль-Фаргани, 1(1). извлечено от https://al-fargoniy.uz/index.php/journal/article/view/15

14. Musayev, X., & Soliev, B. (2023). PUBLIC, PROTECTED, PRIVATE MEMBERS IN PYTHON. Потомки Аль-Фаргани, 1(1), 43–46. извлечено от https://al-fargoniy.uz/index.php/journal/article/view/17

https://doi.org/10.5281/zenodo.7979123

https://journals.indexcopernicus.com/search/article?articleId=3609122