UDC 004.056 **doi:** https://doi.org/10.20998/3083-6298.2025.03.11

Khazail Nuraddin oglu Rzayev[1], Mubariz Mahammadali oglu Ganbarov[1], Kamran Ali oglu Abilov[1], Halyna Sokol[2]

[1] Azerbaijan Technical University, Baku, Azerbaijan
[2] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

IMPLEMENTATION OF TWO-FACTOR AUTHENTICATION IN PARALLEL COMPUTING SYSTEMS

Abstract. Relevance of the research. The growing complexity of cyber threats and the widespread deployment of parallel computing architectures have significantly increased the demand for reliable authentication mechanisms capable of operating under high computational loads and distributed environments. This makes the enhancement of user account protection and cryptographic reliability in such systems particularly relevant. **The subject of the research** is two-factor and multi-factor authentication mechanisms and their application within parallel computing systems. **The purpose of the article** is to justify, design, and evaluate an improved two-factor authentication mechanism adapted for parallel computing systems to enhance their security and resilience to modern cyber threats. **Results.** The study examines various authentication methods used to ensure information protection, including evaluation criteria for biometric systems and existing multi-factor authentication practices in high-security environments such as banking, finance, public services, passport control, customs, and border security. A comparative analysis of different multi-factor authentication approaches is presented, highlighting their use cases, strengths, and limitations. Based on this analysis, a modified authentication model is proposed to improve the security level of user accounts. **Conclusions.** The results demonstrate that the proposed approach increases the cryptographic robustness and operational reliability of authentication processes in parallel computing systems. The conclusion emphasizes the practical value of the improved two-factor authentication mechanism and its potential application in critical infrastructures requiring a high level of information security.

Keywords: authentication, statistical biometrics, dynamic biometrics, two-factor authentication, biometric passport, multifactor authentication, parallel system, biometric identification.

Introduction

Problem relevance. The primary objective of this study is to investigate the challenges of two-factor authentication (2FA) and to improve methods for mitigating these issues. While technological advancements in the modern era have simplified many aspects of human life, they have also introduced new risks and security threats. Malicious actors and hackers often target information systems and databases to steal, misuse, or gain unauthorized access to user data. Consequently, both individual users and large organizations increasingly prioritize information security.

Historically, protecting user accounts relied solely on usernames and passwords. However, the emergence of high-value databases, cryptocurrencies, and parallel processing systems has demonstrated that this approach is no longer sufficiently secure. Despite the development of various cryptographic protection methods and algorithms, absolute protection against cyber threats cannot be guaranteed. In this context, two-factor authentication (2FA**)** has emerged as one of the most reliable security measures.

Literature review. One example of two-factor authentication is the operation of an ATM. To access its services, you must have a physical device (the card) and know secret information (the PIN). If the card is stolen, it cannot be used without the PIN – that's why it should not be written on the card. Using two factors makes security more secure.

In the digital environment, the principle is the same: to log in to an online account, you enter your username and password, but access is granted only after confirmation with a second factor – for example, a one-time code or fingerprint [2, 3].

To ensure the cryptographic strength of authenticators, two-factor protocols use pseudorandom number generation methods. Research shows that most authenticator creation methods in modern systems are vulnerable [1, 4]. Furthermore, advances in computer technology and social engineering methods allow for combined attacks, significantly increasing their effectiveness.

Experts in parallel and other computing systems continuously enhance information security measures, creating and implementing cryptographic algorithms. Nevertheless, these solutions do not always produce optimal results. The use of multiple algorithms across one or more independent systems transforms two-factor authentication into a robust solution for securing the system. This method combines two parallel verification mechanisms: a password (PIN or code) and an external device or software (token, SMS message, smartphone application, etc.). Two-factor authentication significantly complicates unauthorized access, as a malicious actor would need to compromise both independent authentication channels to gain entry.

Based on this, **the purpose of the article** is to substantiate, develop and evaluate an improved two-factor authentication mechanism adapted for parallel computing systems to increase their security and resilience to modern cyber threats.

1. Two-Factor Authentication (2FA) in parallel computing systems

Authentication is defined as the process of verifying a subject's identity, confirming that an individual or entity is indeed who they claim to be. For example, during travel by plane, train, or other transportation, a passenger must present an identification document (such as an ID card or passport) to a conductor. The conductor compares the information on the document with ticket details and grants access if the information matches. This verification process is referred to as authentication**,** whereas granting access is known as authorization**.** While authentication and authorization are related, they are distinct processes. Furthermore, authentication can involve two, three, or multiple factors, depending on the application domain and security requirements.

The main goal of 2FA is to ensure a high level of account security for users in parallel computing systems. This study focuses on securing data during parallel computations by implementing reliable, resilient, and robust two-factor authentication mechanisms.

In parallel computing systems, the authentication process typically relies on three types of factors (Fig. 1):

1. Knowledge factor: Something the user knows, such as a password, username, or PIN;

2. Possession factor: Something the user owns, such as a mobile phone, USB token, smart card, or digital signature device;

3. Inherence factor: Something inherent to the user, such as biometric data including fingerprints, iris patterns, facial features, hand geometry, voice, or body odor.

By combining these factors, 2FA significantly enhances the security of parallel computing systems, protecting user accounts from unauthorized access while maintaining system integrity.

Fig. 1. Biometric authentication forms

There are distinct differences between authentication and authorization. Authentication refers to the process of verifying the validity of the identity presented by a subject (individual), whereas authorization occurs after authentication and involves granting the subject access rights to specific resources within parallel computing systems. Table 1 presents the authentication methods used in parallel systems, along with their requirements, typical applications, and the corresponding levels of security they provide.

Two-Factor Authentication (2FA) in Parallel Computing Systems: Advantages, Limitations, and Challenges Based on the analysis of 2FA methods, despite their advantages and certain limitations, an increasing number of users today rely on two-factor authentication to securely protect the information they send and receive online. 2FA extends beyond the traditional username-password combination by adding an extra layer of security, requiring users to authenticate using a second or additional factor to gain access to their accounts or sensitive data.

While 2FA enhances information security in parallel computing systems, several challenges and limitations remain:

Table 1 – **Presents the authentication methods**

№	Methods	Requirement	Usage	Security	Usage
1.	*Multifactor mobile app*	Application on phone, internet access	Comfo-rtable	Maximum	Comfor-table
2.	*Biometric-based universal web authentica-tion*	Biometric sensor or external token, modern browser	Comfor-table	Higher	Comfor-table
3.	*Telegram Messenger*	Application on phone, internet access	Comfor-table	High	Comfor-table
4.	*One-time password Token*	External token	Depends on token	High	Depends on token
5.	*HMAC-based one-time password algorithm Token*	External token	Depends on token	High	Depends on token
6.	*Google authentica-tor*	Application on phone	Less comforta ble	High	Less comfort-table
7.	*SMS information or call*	Phone, tablet	Less comforta ble	Medium	Less comfort-table

1. Loss of the second factor: users may face difficulties if the second authentication element (e.g., mobile phone, token, or authenticator device) is lost. This includes inability to access codes sent via SMS or calls, unavailability of codes from authenticator apps (such as Google Authenticator or Authy), loss of physical security keys resulting in account lockouts, or lack of alternative recovery methods.

2. Latency and performance issues: in large-scale parallel systems, the additional verification process can slow down computations, as processing one-time passwords (OTPs) or other verification methods requires extra time.

3. Synchronization and centralization difficulties: coordinating authentication data among parallel servers and data centers can be complex. Inconsistent synchronization may lead to some users experiencing access problems.

4. Increased user burden: requiring a second factor for each login may slow work processes, frustrate users, and reduce overall user experience.

5. Security risks: codes transmitted via SMS or email can be intercepted; mobile authenticator app codes may become inaccessible; physical security keys (e.g.,

YubiKey) may be lost; and insufficient alternative recovery methods can prevent access.

6. Phishing and code interception: malicious actors may attempt to capture 2FA codes using fake accounts, phishing websites, or messages that mimic trusted platforms, leading to potential credential theft.

7. Financial and infrastructure costs: implementing 2FA requires additional hardware, software, applications, and IT resources.

8. Training requirements: some users may be reluctant or unwilling to adopt 2FA due to unfamiliarity.

9. User resistance: non-technical users often require extra training and support to use 2FA effectively.

Many of these challenges are associated with vulnerabilities in 2FA provider servers. If servers responsible for generating OTPs or authentication codes are compromised, attackers can gain unauthorized access to user data, posing serious threats to system integrity and availability. Malicious actors may also attempt to bypass 2FA mechanisms through various attack techniques.

Despite these challenges, two-factor authentication significantly improves the security and protection of information systems, websites, computing centers, servers, and applications against unauthorized access. Research indicates that 2FA represents one of the most advanced and promising directions for enhancing security in parallel computing environments [8].

In the presented study, the fundamentals, structure, key components, and algorithm of 2FA are described (Fig. 2). The 2FA method has gained increasing popularity in parallel systems and computing environments due to its ability to prevent result tampering, block unauthorized access, and provide more effective protection of user accounts. This approach not only reduces the risks of data corruption, deletion, and modification but also safeguards user accounts (such as social media and other online accounts) and personal information from theft and other malicious actions.

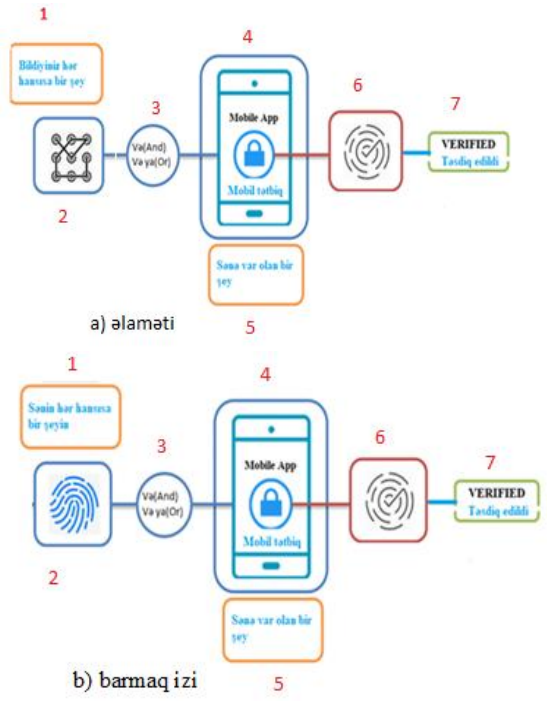

Fig. 2. Single-factor authentication: a) token b) fingerprint

Fig. 2 illustrates the overall structure of two-factor authentication. The design predominantly relies on logical AND and OR operations. Commonly referred to as two-step verification or two-factor authentication, 2FA is a security procedure in which a subject must present two distinct verification elements to authenticate their identity.

The identification factor refers to a category of credentials used to verify the identity of a subject (individual) or any entity requesting access to a system or resource. Each category of credentials is considered a factor. For example, usernames and passwords belong to the same factor type; therefore, using both together constitutes single-factor authentication (SFA), even though two elements are involved.

Fig. 2(a) presents a depiction of single-factor authentication based on any specific factor. The components are described as follows:

1. Trusted devices or credentials used by the subject, such as passwords, laptops, phones, or biometric tools;
2. Additional devices or biometric instruments used for authentication;
3. Logical combination of the elements mentioned above;
4. Identification device and the overall authentication process;
5. Characteristics of the identification based on the chosen factor;
6. Verification algorithm;
7. Confirmation of successful authentication.

Fig. 2(b) illustrates single-factor authentication specifically using fingerprint recognition. The components in this case include:

1. Any biometric element of the user considered for identification;
2. Trusted devices or credentials, such as passwords, phones, laptops, or other biometric tools used by the user for authentication;
3. Logical combination of these elements;
4. Identification device and the authentication process;
5. Characteristics of the identification based on the fingerprint factor;
6. Verification algorithm;
7. Confirmation of successful authentication;

These diagrams highlight the structured organization of single-factor authentication, showing how various identification elements, devices, and verification algorithms interact to securely authenticate a subject.

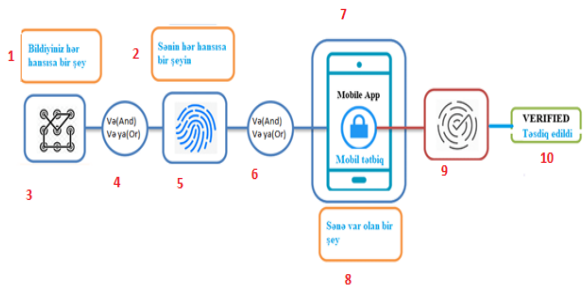

Fig. 3. Two-factor authentication

For the presented parallel computing systems, the overall structure of two-factor authentication (2FA), illustrated in Fig. 3, enables secure access both to system users and system resources. In 2FA methods, the first factor for users of parallel systems can be a password, while the second factor may involve biometric characteristics such as fingerprint, facial features, or vascular patterns of the hand.

By integrating this approach into the authentication process, the security level of parallel computing systems is significantly enhanced. This added layer of authentication makes it more difficult for malicious actors to access system devices, hardware, software tools, or active user accounts. If a cyberattacker obtains a user's primary authentication element (e.g., a password or PIN), access to the system is still denied unless the second factor is successfully verified.

Based on the above considerations, the algorithm of the 2FA mechanism in parallel computing systems can be outlined in several steps, as shown in Fig. 4**:**

Step 1: User login to the system. The authentication process begins with the user submitting a login request. At this stage, system participants enter their previously registered username or password to initiate access.

Step 2: Verification of initial authentication. If the user's initial login attempt is successful, the system proceeds to request the second authentication factor for the next stage of access.

Step 3: Factor validation. The user provides the second factor, which may include a one-time token or password generated by the authentication software, and this is processed as the second authentication element.

Step 4: Granting access. If both authentication factors are verified successfully, the user is granted access to the system. This process can occur almost instantaneously, often within a few seconds.

Step 5: Access denial and retry. If any of the conditions in the previous steps are not met, access to the system is restricted, and the user must repeat the authentication steps.

This structured 2FA process ensures that parallel computing systems remain secure against unauthorized access while maintaining efficient and reliable user authentication.

The main categories of authentication factors for accessing and managing parallel systems and applications are knowledge, ownership, inheritance, location, and behavior.

2. Mathematical model of a security mechanism for access confirmation based on 2FA

The security mechanism for confirming access to 2FA-based parallel systems can be described as a mathematical model. For this, the initial data are:

$$P_{auth}=P(F_1 \wedge F_2)=P(F_1)*P(F_2), \quad (1)$$

where U – the set of subjects (users); F_1 – the first factor (e.g., login credentials, PIN, password); F_2 – the second factor (e.g., OTP, mobile device, token, or biometric data); A – the authentication procedure (identification process verifying that the subject is genuinely the entity they claim to be, a critical stage in preventing unauthorized access); $P(F_i)$ – the probability of successfully compromising factor i, where $i = 1, \ldots, n$, and n is the total number of factors; P_{auth} – the probability of successful system authentication; P_{attack} – the probability of an attacker successfully authenticating.

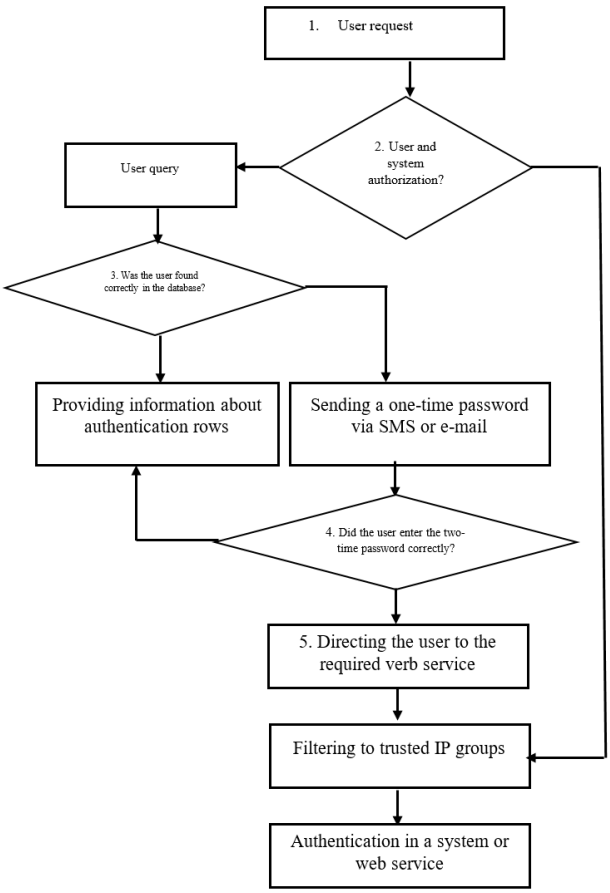

Fig. 4. Two-factor authentication algorithm for parallel systems

In a parallel system, authentication is considered successful only if the subject correctly presents both authentication factors. This condition can be logically expressed as: (1) Legitimate User Case. For a subject participating in a parallel computing system who possesses the correct credentials and presents both authentication factors correctly, the probability of successful authentication can be considered ideal, approximately equal to 1:

$$P_{auth} \approx 1. \quad (2)$$

This expression indicates that if the user correctly provides both F_1 and F_2, the likelihood of system access is nearly maximal.

Probability of Successful Attack. If an attacker attempts unauthorized access to the system and must guess or obtain both factors F_1 and F_2 then the probability of a successful attack corresponds to the joint probability of compromising both factors (3). In the simplest case – assuming the two factors are independent – this probability can be expressed as:

$P_{attack}=P(\textbf{compromise}F_1 \wedge \textbf{compromise}F_2)=P(F_1)*P(F_2)$, (3)

where $P(F_i)$ – the probability of successfully compromising (or obtaining) the *i-th* factor.

If the factors are not independent (for example, access to F_2 requires first compromising F_1, or attack methods are interdependent), the overall probability should be expressed using conditional probabilities (4):

$$P_{attack}=P(F_1)*P(F_1)|(F_2), \quad (4)$$

or equivalently,

$$P_{attack}=P(F_2)*P(F_2)|(F_1), \quad (5)$$

where $P(F_2|F_1))$ denotes the probability of compromising F_2 given that F_1 has already been compromised.

In general, for an *n*-factor multi-factor authentication system (assuming independence of factors), the probability of a successful attack is given by:

$$P_{attack} = \prod_{i=1}^{n} P(F_i). \quad (6)$$

For example, if:

we assume the probability of password cracking $P_{break}(F_1) = 10^{-5}$;

we assume the probability of OTP cracking $P_{break}(F_2) = 10^{-7}$.

Then: $P_{attack} = 10^{-5} \cdot 10^{-7} = 10^{-11}$.

This shows that using two factors for parallel systems increases security exponentially (Fig. 5).

Here:

Orange column: $P_{break}(F_1) = 1\times10^{-5}$.

Purple column: $P_{break}(F_2) = 1\times10^{-7}$.

Red column: $P_{attack} = 1\times10^{-12}$.

The graph shows the logarithmic (log10) scale of the probability values on the y-axis to make the differences more visible.

The y-axis shows numbers between −13 and −4, and each bar is located at its log10 probability value. This graph shows that the overall attack probability (Pattack) is much smaller than both $P_{break}(F_1)$ and $P_{break}(F_2)$.

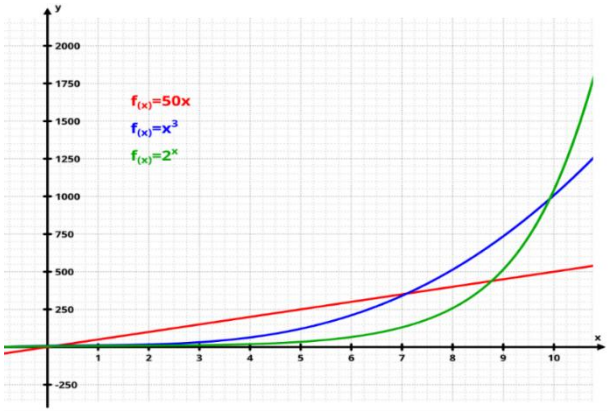

Fig. 5. Security indicator of using two factors in parallel systems

3. Calculation of cryptostrength (cryptodurability)

If the information entropy of each factor is measured in bits as H(Fi), then the overall security level is:

$$P_{attack}=H(F_1)+H(F_2) \quad (7)$$

Here for example:

Password entropy $H(F_1) = 22$ levels(bits).

If we assume OTP entropy $H(F_2) = 12$ levels, then the total security strength is: $H_{total} = 32$ levels.

In general, a formal classification for parallel systems (such as the IFA model) can be described as follows:

$$A(U,F_1,F_2)=\begin{cases}1, & if\ V(F_1)=true \wedge V(F_2)=true \\ 0\end{cases} \quad (8)$$

U includes either F_1 and F_2. Here $V(F_i)$ is the function for validating the given factor (e.g., an OTP server or password checker).

Fig. 6. Elements of information security

Thus, various technologies can be applied for the verification of authentication processes in parallel computing systems:

1. Email and SMS-Based Authentication – in this method, the user receives a one-time password (OTP) via their mobile phone or text message to access the system. The validity of this password is limited by time and typically consists of 4–8 digits. Most often, the OTP

contains 4 or 6 digits. If the user enters the code correctly within the specified time, access to the requested system or resource is granted.

2. Hardware Token Authentication – this type of authentication uses a physical device, such as a smart card or USB key. The device generates a dynamic, unique code that is valid only for a limited time frame and functions as a physical security key.

3. Software Token Authentication – software tokens generate one-time passwords based on time or specific events. The authentication software sends a verification code to the user's computer or mobile device. Similar to hardware tokens, these codes are dynamic, valid for a short period, and intended for one-time use only.

4. Push Notification Authentication – push notifications verify the user's identity by sending a secure alert directly to a trusted mobile application on the user's device. The message allows the user to approve or deny the login request with a single touch and contains details of the authentication attempt. Theoretically, this process confirms that the registered device is in the user's possession. Push notifications enhance account security by reducing potential attack risks. This 2FA method is considered highly reliable, but it requires a fast and continuously stable internet connection.

5. Biometric Authentication – a modern and secure method that verifies the user based on their biometric and biological characteristics, eliminating the need for a password. For example, iPhone and other mobile device users can authenticate via facial recognition, while other systems may use fingerprint scanning, iris recognition, or X-ray scanning technologies. Biometric 2FA is considered one of the most secure authentication methods. It is highly convenient for users, difficult to compromise, and effectively serves as a personal token. The use of biometric authentication on mobile or smart devices is illustrated in Fig. 5.

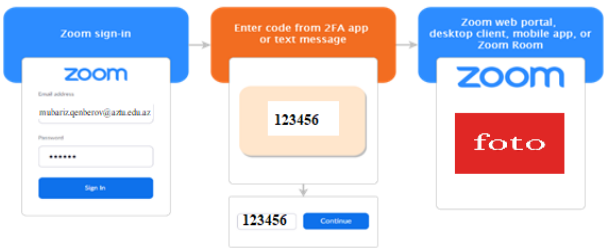

Fig. 7. Biometric authentication

Other biometric methods include hand geometry, retinal and iris scanning, voice recognition, and signature-based analysis. It has now become common for devices such as smartphones, tablets, and computers to integrate biometric technologies for digital authentication purposes.

To secure the 2FA authentication infrastructure, communications involving the transmission of 2FA codes or tokens can be protected using encryption protocols at the transport layer of the OSI model.

Research indicates that the most reliable type of two-factor authentication is hardware-based, particularly USB tokens. Unlike other methods, these separate devices are often connected to a computer and present cryptographic keys automatically in the form of a processor-enabled USB key [8].

Considering these factors, several combinations can be considered for establishing secure connections in parallel processing systems using 2FA:

password + SMS/push notification;
password + certificate;
fingerprint + one-time password (OTP);
PIN code + facial biometrics;
facial biometrics + fingerprint;
right-hand and left-hand fingerprints.

The implementation of 2FA in parallel computing systems is crucial to address potential problems in these environments [9]. The following measures are recommended:

storage of Backup Codes – backup codes should be kept in a secure location (on paper, in an encrypted file, or in a password manager). Most services (Microsoft, Google, GitHub, Facebook, etc.) generate backup codes when setting up 2FA. These codes can be printed and stored securely, added to a password manager (Password, Bitwarden), or saved in a personal encrypted file. They can be used to access accounts without the primary 2FA device;

addition of Alternative Verification Methods – additional phone numbers or backup email addresses should be assigned to enable account recovery;

installation of the Authenticator on Multiple Devices – applications like Authy allow codes to be synchronized in the cloud and transferred to other devices;

availability of Backup Physical Security Keys – a second physical security key should be kept as a backup. Alternative verification methods are required to restore accounts if the primary 2FA device is lost, such as: adding a backup phone number (e.g., a family member or a second device), specifying a backup email for account recovery, and installing authenticator apps on multiple devices (Authy allows cloud synchronization, unlike some apps such as Google Authenticator, which cannot transfer codes). Using multiple devices ensures alternative access to codes;

coordination with Operator and Service Support – if a phone number or authenticator device is lost or compromised (SIM swap attacks), timely contact with the mobile operator and service support team is essential to obtain a new SIM card and restore account access;

transition to Passkeys Technology [10].

Discussion of results

The study showed that the use of two-factor authentication (2FA) allows to increase the level of security of computing systems in which large volumes of data are processed. Analysis of authentication methods showed that identification based on a password does not solve security problems in modern infrastructures.

The assessment of authentication factors showed that to reduce the probability of unauthorized access, a combination of two independent categories is sufficient. This is confirmed by the conducted mathematical modelling. The joint use of individual factors exponentially reduces the probability of an attack. To ensure the integrity of the system, it is recommended to use multi-level protection mechanisms and multi-factor verification.

Despite the advantages of implementing 2FA, there are disadvantages associated with the loss and unavailability of the second authentication factor. This can lead to service interruption. In distributed environments, there are synchronization problems between authentication servers. To solve these problems, it is necessary to implement data duplication, redundancy and timely verification in the 2FA infrastructure.

The study showed that the choice of authentication mechanisms, resource availability and user awareness are important. The security strategy should include backup codes, recovery procedures and backup verification channels to minimize the risks associated with system failures.

Thus, the proposed modification of the 2FA approach allows to strengthen the security system of computing systems with an appropriate level of performance.

Conclusions

To avoid the aforementioned issues in parallel computing systems, a balanced authentication strategy should be implemented. In the future, two-factor authentication will move away from the classic "password + SMS" model and become more flexible, secure, and user-friendly with biometrics, blockchain, artificial intelligence, IoT and quantum technologies. This will lead to higher security standards in all technologies, from parallel computing systems to everyday mobile applications.

By employing adaptive authentication methods and security measures, these problems can be minimized within parallel computing environments. It should be noted that in certain services, if alternative verification methods are not preconfigured in the parallel systems, potential security incidents may make it impossible to restore user accounts in a timely manner. Further details on these approaches will be provided in our future publications.

REFERENCES

1. Slyman, M., O'Neil, S., Nicolae, G. H. and Van der Merwe, B. (2009), "An evaluation of hypothetical attacks against the PassWindow authentication method", *The PassWindow method*. URL: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.pdf
2. Shirvanian, M. and Agrawal, S. (2021), "2D-2FA: A New Dimension in Two-Factor Authentication", *arXiv preprint*, https://doi.org/10.48550/arXiv.2110.15872
3. Dvuxfaktornaya autentifikaciya pri udalennom dostupe (2006), *Infosecurity*, URL: http://itc.ua/articles/dvuhfaktornaya_autentifikaciya_pri_udalennom_dostupe_23166
4. Man In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication (2010), *Information week*, URL: http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495
5. ISO/IEC 19794-6 Information technology – Biometric data interchange formats (2012), URL: https://www.iso.org/standard/38750.html
6. Alrawili, R., AlQahtani, A. S. and Khan, M. Kh. (2024), "Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion", *Computers and Electrical Engineering,* Vol. 119, https://doi.org/10.1016/j.compeleceng.2024.109485
7. Ganmati, A., Afdel, K. and Koutti, L. (2025), "Deep Learning-Based Multi-Factor Authentication: A Survey of Biometric and Smart Card Integration Approaches", *Computer Science*, https://doi.org/10.48550/arXiv.2510.05163
8. AlOmari, W. and Abusaimeh, H. (2015), "Modified USB Security Token for User Authentication", *Computer and Information Science*, Vol. 8, No. 3, DOI:10.5539/cis.v8n3p51
9. Zhou, F. and Zhao, T. (2022), "A Survey on Biometrics Authentication", *arXiv:2212.08224*, https://doi.org/10.48550/arXiv.2212.08224
10. Evseev, S.P., Abdullaev, V.G., Agazade, Zh.F., Abbasova, V.S. (2016), "Usovershenstvovanie metoda dvuhfaktornoj autentifikacii na osnove ispol'zovanija modificirovannyh kripto-kodovyh shem", *Systemy obrobky informatsii,* № 9(146), URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=soi_2016_9_29

Received (Надійшла) 31.10.2025
Accepted for publication (Прийнята до друку) 14.11.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Рзаєв Хазаїл Нураддін огли – доктор технічних наук, професор, кафедра комп'ютерних технологій, Азербайджанський технічний університет, Баку, Азербайджанська Республіка;
Khazail Rzayev - Doctor of technical sciences, Professor, Department of Computer Technology, Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: xezail.rzayev@aztu.edu.az; ORCID Author ID: https://orcid.org/0000-0001-9272-4302;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57204042636.

Ганбаров Мубаріз Магаммадалі огли – старший викладач, кафедра комп'ютерних технологій, Азербайджанський технічний університет, Баку, Азербайджан;
Mubariz Qanbarov – Senior Lecturer, Department of Computer Technology, Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: mubariz.qenebrov@aztu.edu.az; ORCID Author ID: https://orcid.org/0009-0001-6119-3446.
Абілов Кямран Алі огли – старший викладач, кафедра комп'ютерних технологій, Азербайджанський технічний університет, Баку, Азербайджан;
Kamran Abilov – Senior Lecturer, Department of Computer Technology, Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: kamran.ebilov@aztu.edu.az; ORCID Author ID: https://orcid.org/0009-0009-2231-2471.
Сокол Галина Вікторівна – кандидат технічних наук, доцент кафедри систем інформації ім. В.О. Кравця, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Halyna Sokol – Candidate of Technical Sciences, Associate Professor of Information systems named after V. O. Kravtsia, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Halyna.Sokol@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0003-4847-518X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=55975966600.

РЕАЛІЗАЦІЯ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ В ПАРАЛЕЛЬНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Х. Н. Рзаєв, М. М. Ганбаров, К. А. Абілов, Г. В. Сокол

Анотація. Актуальність дослідження. Зростаюча складність кіберзагроз та широке розгортання архітектур паралельних обчислень значно підвищили попит на надійні механізми автентифікації, здатні працювати в умовах високих обчислювальних навантажень та розподілених середовищ. Це робить особливо актуальним підвищення захисту облікових записів користувачів та криптографічної надійності в таких системах. **Предметом дослідження** є механізми двофакторної та багатофакторної автентифікації та їх застосування в паралельних обчислювальних системах. **Метою статті** є обґрунтування, розробка та оцінка вдосконаленого механізму двофакторної автентифікації, адаптованого для паралельних обчислювальних систем, для підвищення їхньої безпеки та стійкості до сучасних кіберзагроз. **Результати.** У дослідженні розглядаються різні методи автентифікації, що використовуються для забезпечення захисту інформації, включаючи критерії оцінки біометричних систем та існуючі практики багатофакторної автентифікації в середовищах з високим рівнем безпеки, таких як банківська справа, фінанси, державні послуги, паспортний контроль, митниця та прикордонна безпека. Представлено порівняльний аналіз різних підходів до багатофакторної автентифікації, з висвітленням їх варіантів використання, сильних сторін та обмежень. На основі цього аналізу запропоновано модифіковану модель автентифікації для підвищення рівня безпеки облікових записів користувачів. **Висновки.** Результати демонструють, що запропонований підхід підвищує криптографічну стійкість та операційну надійність процесів автентифікації в паралельних обчислювальних системах. У висновку наголошується на практичній цінності вдосконаленого механізму двофакторної автентифікації та його потенційному застосуванні в критичних інфраструктурах, що потребують високого рівня інформаційної безпеки.

Ключові слова: автентифікація, статистична біометрія, динамічна біометрія, двофакторна автентифікація, біометричний паспорт, багатофакторна автентифікація, паралельна система, біометрична ідентифікація.