UDC 004.056.53

DOI: 10.15587/1729-4061.2025.333720

THE DEVELOPMENT OF AN EVALUATION MODEL FOR USER AUTHENTICATION METHODS WITH SECURITY, USABILITY, AND USAGE FREQUENCY

Olga Ussatova
PhD
Department of Information Security
Institute of Information and Computational Technologies
Shevchenko str., 28, Almaty, Republic of Kazakhstan, 050010

Shakirt Makilenov
Corresponding author
Master of Science in Engineering*
E-mail: shakirt.makilenov@gmail.com

Vladislav Karyukin
PhD*

Abdul Razaque
PhD
Department of Cybersecurity
International IT University
Manas str., 34/1, Almaty, Republic of Kazakhstan, 050000

Saule Amanzholova
Candidate of Technical Science, Associate Professor
Department of Intellectual Systems and Cyber Security
Astana IT university
Mangilik El ave., 55/11, EXPO Business Center, Block C1, Astana,
Republic of Kazakhstan, 010000

Yenlik Begimbayeva
PhD, Associate Professor, Head of Department
Department of Cybersecurity
Almaty University of Power Engineering
and Telecommunications (AUPET)
Baytursynov str., 126/1, Almaty, Republic of Kazakhstan, 050013

*Department of Information Systems
Al-Farabi Kazakh National University
Al-Farabi ave., 71, Almaty, Republic of Kazakhstan, 050040

The object of the study is authentication systems in security-critical environments, especially in healthcare. The addressed problem is the absence of comprehensive frameworks that integrate both threat data and user-centric factors for real-world method comparison.

This study develops and validates a novel evaluation model for assessing the empirical effectiveness of user authentication methods. The proposed model integrates probabilistic threat modeling, usability data, and weighted multi-criteria analysis to generate context-sensitive effectiveness scores, thereby supporting informed decision-making.

Twelve authentication methods were assessed using three criteria: security (resistance to cyber threats), usability (user convenience), and use frequency (real-world adoption). Security coefficients (K2) were computed from threat statistics, while usability and adoption metrics were based on a healthcare survey (n = 70). Weighted normalization (ws = 0.4, wu = 0.3, wf = 0.3) produced overall effectiveness scores (E). The most effective methods were mobile devices (E = 30.915), PIN codes (E = 30.252), and fingerprint authentication (E = 29.235), offering an optimal balance of security and acceptance. Graphical passwords (E = 6.132) and iris scans (E = 7.245) scored lowest due to poor usability and limited adoption.

The model's feature lies in its holistic integration of threat exposure and empirical user data, along with adaptability to organizational requirements and visual interpretability. This feature distinguishes it from single-dimensional or static assessment models.

Keywords: authentication, cybersecurity, usability, effectiveness, evaluation, threats, biometrics, tokens, risks, security

Received 19.03.2025
Received in revised form 21.05.2025
Accepted date 11.06.2025
Published date 30.06.2025

How to Cite: *Ussatova, O., Makilenov, S., Karyukin, V., Razaque, A., Amanzholova, S., Begimbayeva, Y. (2025). The development of an evaluation model for user authentication methods with security, usability, and usage frequency. Eastern-European Journal of Enterprise Technologies, 3 (2 (135)), 17–29. https://doi.org/10.15587/1729-4061.2025.333720*

1. Introduction

In the context of the global digital transformation, the protection of digital assets and personal data has become a fundamental scientific and practical issue. The ongoing integration of cloud systems, mobile technologies, and Internet of Things (IoT) platforms into critical infrastructures has dramatically expanded the attack surface for malicious actors. As cyber threats continue to evolve in complexity and frequency, the scientific community places increasing attention on the foundational mechanisms that ensure access control, among which user authentication remains one of the most essential and widely studied components [1, 2].

Authentication systems serve as the primary barrier against unauthorized access to confidential data and services. Their design and implementation are central to cybersecurity strategies across sectors such as healthcare, finance, defense, and public administration. A failure in authentication may lead not only to financial damage but also to disruptions in critical services, privacy violations, and legal consequences [3]. Modern attack vectors, such as phishing, token theft, and biometric forgery, constantly test the reliability of existing authentication schemes. Therefore, developing and improving authentication methods remains a critical and unresolved research problem in the information security field [4, 5].

Over the years, various types of authentication mechanisms have been developed, including knowledge-based (passwords, PINs), possession-based (smart cards, tokens), and biometric-based (fingerprints, facial recognition) methods. More recently, adaptive and continuous authentication systems have emerged, leveraging behavioral biometrics and machine learning to enhance real-time access control. However, despite their diversity and progress, these systems face multiple challenges related to usability, user acceptance, security assurance, and attack resilience [6, 7].

A particularly important problem is the absence of a unified approach for evaluating the effectiveness of these authentication methods under realistic operational conditions. Traditional evaluations often focus exclusively on security or usability, overlooking the complex trade-offs that arise in real-world applications. For instance, a method may offer high theoretical security, but if it is too difficult to use, users may circumvent or avoid it, undermining its practical value. Conversely, overly convenient methods may be insecure by design. A balanced, multi-criteria assessment framework is therefore essential for understanding which methods are best suited to specific use cases, especially in security-sensitive environments such as healthcare institutions [8].

Therefore, research on the systematic evaluation and comparative analysis of authentication methods is highly relevant in the current stage of cybersecurity science and practice.

2. Literature review and problem statement

The paper [4] presents the results of a comprehensive evaluation of biometric authentication methods, demonstrating that while such systems provide strong protection against unauthorized access, they are still susceptible to specific attacks such as spoofing and sensor manipulation. It is shown that biometric systems must be evaluated not only in terms of security but also in terms of user experience and environmental conditions. However, unresolved issues remain related to the vulnerability of biometric templates and the lack of standardization in sensor calibration, which complicates cross-system implementation.

In [5], the authors introduce a framework for continuous authentication on smartphones, focusing on the detection of changes in device possession. Their findings highlight the benefits of implicit, behavior-based authentication in real-time environments. Nevertheless, practical implementation remains difficult due to high computational requirements and privacy concerns, which limit adoption at scale.

A multi-user, multimodal authentication assessment approach is discussed in [9]. The authors show that combining several authentication channels increases reliability, but unresolved challenges arise from managing user diversity and ensuring consistent performance across different modes. These difficulties are often linked to the cost and complexity of integration, especially in legacy systems.

The study in [7] addresses adaptive biometric systems and their capacity to respond to dynamic security threats. While the concept of adaptability enhances resilience to evolving attacks, challenges remain in accurately modeling user behavior over time and in maintaining system robustness in the face of data drift or spoofing. This suggests the need for more flexible evaluation tools that consider long-term system performance.

The LINDDUN framework is applied in [10] to analyze privacy threats in identification and authentication processes. The authors emphasize the importance of preventing traceability and identifiability in systems that handle sensitive personal data. However, it is noted that LINDDUN lacks quantitative evaluation metrics, which limits its applicability for measuring real-world effectiveness.

Paper [11] provides a threat analysis of two-factor authentication (2FA) methods and highlights persistent vulnerabilities, including phishing, SMS interception, and token theft. Although these systems offer a layered security model, their usability and resilience vary greatly depending on the implementation context. This raises concerns about their practical effectiveness across diverse user populations.

In [12], the authors evaluate alternative authentication techniques such as behavioral biometrics and device-based trust systems. The results suggest that these methods offer promising improvements in user convenience and fraud prevention. Yet, they require further validation in operational settings to address unresolved issues such as data privacy, false positives, and model accuracy.

The work [13] explores the usability-security trade-off by conducting a comparative study of 2FA systems. It is shown that methods perceived as too complex tend to be underused by users, diminishing their intended security benefits. One way to overcome this limitation is to design user-centric interfaces that align with behavioral patterns and preferences.

Finally, [14] introduces a security assessment framework based on attack classification, which allows for structured evaluation of authentication protocols. The framework effectively maps threats to defensive capabilities but does not sufficiently incorporate usability or system deployment considerations, making it less suitable for selecting methods in end-user environments.

All this suggests that it is advisable to conduct a study on the comprehensive evaluation of authentication methods, which takes into account not only security factors but also usability, usage frequency, and real-world attack data. Such a study would help bridge the gap between theoretical models and practical implementation and provide decision-makers with a structured approach for selecting the most appropriate authentication mechanisms.

3. The aim and objectives of the study

The aim of this study is to develop an evaluation model for assessing methods based on their resistance to cyber threats, user-perceived usability, and frequency of use in organizational settings.

To achieve this aim, the following research objectives were formulated:

– to propose a structure of authentication model;

– to assess the likelihood of successful cyberattacks on different authentication methods by analyzing threat statistics and computing security coefficients;

– to collect and analyze empirical data on the usability and usage frequency of authentication methods through a structured user survey;

– to evaluate a model that integrates normalized security, usability, and frequency metrics of the authentication methods with the use of weighted coefficients;

– to compare authentication methods by visualizing and interpreting the obtained effectiveness scores across all evaluation criteria.

4. Materials and methods

4. 1. Object and hypothesis of the study

The object of this study is modern user authentication methods used to protect information systems from unauthorized access in organizational environments. These methods are particularly important in critical sectors such as healthcare, where reliable access control is essential for safeguarding sensitive data and maintaining the continuity of services. The research focuses on a set of commonly used authentication mechanisms, including knowledge-based (e.g., passwords, PIN codes), possession-based (e.g., tokens, smart cards, USB keys), and biometric-based methods (e.g., fingerprints, face ID, iris scans, and voice recognition).

The central hypothesis of the study is that the effectiveness of an authentication method can be objectively evaluated using an integrated model that combines probabilistic risk assessment and empirical user data. It is assumed that the most reliable evaluation results are achieved by simultaneously considering three dimensions: security (resistance to known cyberattack vectors), usability (user-perceived convenience), and frequency of use (real-world adoption). These criteria reflect both the technical and human-centered aspects of authentication performance and make it possible to generate context-sensitive recommendations for system deployment.

Several assumptions underlie this hypothesis. First, it is assumed that attack probabilities reported in cybersecurity literature can be mapped onto specific authentication methods through clearly defined attack vectors. Second, user-perceived usability and usage frequency, collected via structured surveys, are considered representative of the selected organizational context. Third, all three criteria – security, usability, and frequency – can be normalized and weighted to construct a unified effectiveness score that enables method-to-method comparison.

Certain simplifications are also adopted to maintain model clarity and applicability. For instance, computational complexity and hardware-specific constraints are not included in the current version of the model, as they vary widely between organizations and have limited relevance in end-user scenarios. Additionally, dynamic behavioral parameters such as session time or adaptive authentication responses are excluded from this stage of the study, but are considered promising directions for future research.

By combining empirical, probabilistic, and mathematical components within a unified decision-making framework, this study aims to develop a practical evaluation model that can support organizations in selecting the most appropriate authentication methods for their operational and security needs.

4. 2. Research methodology

4. 2. 1. Evaluating authentication methods based on vulnerabilities and threat vectors

The primary aim of this study is to develop a system for evaluating the effectiveness of authentication methods based on an analysis of their vulnerabilities, functional characteristics, and statistical attack data. The evaluation criteria employed include security level, usability, and frequency of use of various authentication types. Currently, there exist numerous authentication methods. For this research, the most prevalent methods have been selected: password, graphical password, PIN code, one-time password (OTP), token, smart cards, USB keys, mobile devices, fingerprint, Face ID, iris scan, and voice recognition. Each of these methods exhibits varying levels of security, advantages, disadvantages, vulnerabilities, and susceptibility to different attack vectors. Attack vectors corresponding to these authentication types were selected similarly, focusing on the most common attack methods. Fig. 1 illustrates the attack vectors categorized according to authentication factors.

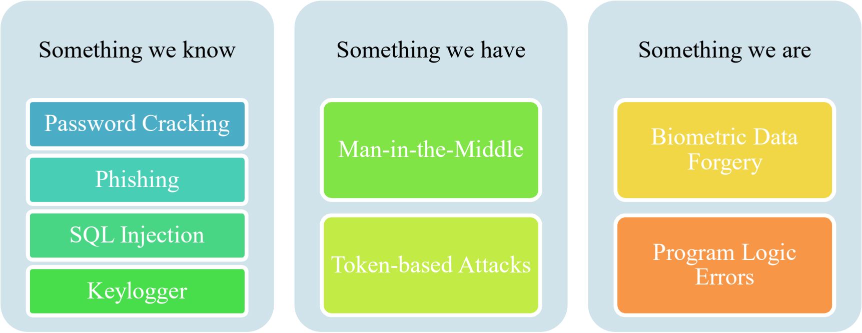

Fig. 1. Distribution of attack vectors by authentication factors

Table 1 lists the weaknesses associated with different authentication techniques and shows how sensitive they are to various attacks [11], such as phishing, man-in-the-middle, and brute-force assaults. For example, while most attack techniques can expose passwords, biometric systems such as Face ID and iris recognition are particularly vulnerable to biometric data forgeries. This comparison highlights the varied security problems that each approach confronts.

To identify vulnerabilities in the selected authentication methods, a vulnerability mapping table was compiled based on attack vectors. Statistical data on security levels were obtained from official sources such as the cybersecurity threat [15]. Based on the attack methods outlined in the analytical report and the attack vectors presented in Table 1, a correlation table was compiled, which is shown in Table 2. Percentage data was sourced from the cyber threat report. In this case, data on attacks against organizations was used, as this study focuses on the use of authentication methods in medical organizations. Some items in the attack methods correspond to multiple items in the attack vectors, so the percentage distribution of attack methods was presumed to align with the percentage distribution of attack vectors.

Table 1

Attack vectors by authentication methods

Authentication methods	Brute-force	Dictionary	Phishing	SQL injection	Man-in-the-middle	Token-based-attack	Biometric data forgery	Program logic errors
Password	☑	☑	☑	☑	☑	–	–	–
Graphical password	–	–	☑	–	–	–	–	–
PIN code	–	–	☑	–	–	–	–	–
OTP	☑	–	☑	–	☑	–	–	–
Token	–	–	☑	–	–	☑	–	☑
Smart cards	–	–	☑	–	–	☑	–	☑
USB keys	–	–	☑	–	–	☑	–	☑
Mobile devices	–	–	☑	–	☑	–	–	☑
Fingerprint	–	–	☑	–	–	–	☑	☑
Face ID	–	–	☑	–	–	–	☑	☑
Iris recognition	–	–	☑	–	–	–	☑	☑
Voice recognition	–	–	☑	–	–	–	☑	☑

The first column of Table 2, titled attack methods, was derived from a report published by positive technologies [15]. This report provides statistical data on the prevalence of various types of cyberattacks targeting organizations. The reported figures include relative frequencies (percentages) for general categories of attack techniques, such as malware usage (73%), social engineering (56%), vulnerability exploitation (31%), credential compromise (7%), and others (12%).

The second column, vectors of attack, was constructed by the authors of this study to reflect specific technical or behavioral attack mechanisms relevant to user authentication systems. Each general attack method from the original report was mapped to one or more corresponding attack vectors used in the authentication context. For instance, "social engineering" from the source was associated with "phishing" as a primary vector, and "malware usage" was linked to "Man-in-the-Middle" attacks.

The percentages listed in the vectors of attack column were calculated proportionally from the attack methods data. If a method in the left column maps to a single attack vector, the full percentage value is carried over. However, if one attack method corresponds to multiple vectors, the percentage is evenly divided among those vectors. For example, "vulnerability exploitation" (31%) is linked to two vectors "logic errors" and "SQL injection" – each receiving half of the original percentage (15.5%). This proportional allocation ensures that the vectors of attack column remains consistent with the aggregated threat data presented in the source, while also enabling a more granular analysis of authentication-specific risks.

Table 2

Table of correlation between attack methods and vectors

Attack methods	Vectors of attack
Use of malware (73%)	Man-in-the-middle (73%)
Social engineering (56%)	Phishing (56%)
Exploitation of vulnerabilities (31%)	Program logic errors (15.5%)
	SQL injection (15.5%)
Compromising credentials (7%)	Token-based-attack (3,5%)
	Falsification of biometric data (3.5%)
Other (12%)	Brute-force attack (6%)
	Dictionary attack (6%)

This approach allows the construction of a probabilistic threat matrix tailored to authentication technologies while maintaining a traceable connection to established organizational-level cybersecurity data.

Table 2 estimates the coefficients of probable attack occurrence ($K1$). Establishing a security coefficient range from 0 to 2, subtracting the coefficient of probable attack occurrence from the maximum-security coefficient allows the determination of the actual security coefficient for various authentication methods ($K2$). To assess the security of different authentication methods, calculations were developed considering the probabilities of various attack vectors. These calculations are based on data regarding the frequency of attack occurrences and their distribution across authentication types:

– calculation of the likelihood of attack occurrence coefficient ($K1$).

The likelihood of attack occurrence coefficient for authentication method i ($K1_i$) is calculated as the sum of the products of attack probabilities for each vector and the probability of successful attack for the given method

$$K1_i = \sum_v P_{i,v} * P_v, \tag{1}$$

where V – the indices of various attack vectors (brute force, dictionary, phishing, SQL injection, man-in-the-middle, token-based attack, biometric data forgery, and logic errors);

– calculation of the security coefficient ($K2$).

The security coefficient ($K2$) for authentication method iii is determined as the difference between the maximum possible security coefficient and the attack likelihood coefficient

$$K2_i = 2 - K1_i, \tag{2}$$

where 2 represents the theoretical maximum security level, corresponding to a method that is completely immune to all types of attacks. Thus, $K2_i$ falls within the range [0, 2], where 0 indicates complete vulnerability and 2 indicates full security. This scale is chosen to standardize the comparison of methods, where a higher value of $K2_i$ signifies greater resistance to attacks. For example, a method with $K1_i = 0$ (invulnerable) will have $K2_i = 2$, whereas a method with $K1_i = 1$ (vulnerable to all attacks) will have $K2_i = 0$.

This model enables a comprehensive assessment of the security of various authentication methods by considering multiple factors and the likelihood of different types of attacks. The results of the calculations for each type of authentication are shown in Table 3.

Table 3

Calculation of security coefficients by authentication types

Authentication methods	Brute-force	Dictionary	Phishing	SQL injection	Man-in-the-middle	Token-based-attack	Biometric data forgery	Program logic errors	**К**1	**К**2
Password	0.06	0.06	0.56	0.155	0.73	–	–	–	1.565	0.435
Graphical password	–	–	0.56	–	–	–	–	–	0.56	1.44
PIN code	–	–	0.56	–	–	–	–	–	0.56	1.44
OTP	0.06	–	0.56	–	0.73	–	–	–	1.35	0.65
Token	–	–	0.56	–	–	0.04	–	0.155	0.755	1.245
Smart cards	–	–	0.56	–	–	0.04	–	0.155	0.755	1.245
USB keys	–	–	0.56	–	–	0.04	–	0.155	0.755	1.245
Mobile devices	–	–	0.56	–	0.73	–	–	0.155	1.445	0.555
Fingerprint	–	–	0.56	–	–	–	0.04	0.155	0.755	1.245
Face ID	–	–	0.56	–	–	–	0.04	0.155	0.755	1.245
Iris recognition	–	–	0.56	–	–	–	0.04	0.155	0.755	1.245
Voice recognition	–	–	0.56	–	–	–	0.04	0.155	0.755	1.245

The data on usability and usage frequency were collected through an anonymous survey conducted in a medical organization. The usability level of various authentication methods was rated on a scale from 1 to 10, where 1 represents the lowest level of usability and 10 represents the highest. The frequency of use of different authentication methods was determined in percentage terms. The evaluation and ranking of different authentication methods should be determined. Algorithm 1 compares and assesses several authentication techniques based on their security, utility, and usage frequency.

Algorithm 1: Evaluation and ranking of different authentication methods based on security, usability, and usage frequency:

Input: {A_m: Authentication methods, S: Security level data, U: Usability scores, F: Usage frequency, and attack P: probabilities, P_j: Probability of attack j; Cj: Critical impact coefficient, R_l: Ranked list}.

Output: {E} //Ranked list of authentication methods based on effectiveness.

Step 1: Initialize evaluation parameters.

1(a). Assign security level weights γ_S, usability weights γ_U, and usage frequency weights γ_F based on their significance.

Step 2: Process each metric in the authentication method (i).

2(a) Normalize (N) the metrics S, U, F.

The formulas must be typed in a MathType formula editor:

$$N_S(i)=\frac{S_i}{\max(S)}, \quad (3)$$

$$N_U(i)=\frac{U_i}{\max(U)}, \quad (4)$$

$$N_F(i)=\frac{F_i}{\max(F)}. \quad (5)$$

Step 3: Compute the weighted normalized score W_i.

1(a). $W_i=\gamma_S\times N_S(i)\times N_U(i)\times N_F(i)$. (6)

Step 4: Calculate the effectiveness score E_i for method.

4(1). $E_i = W_i$ // sum of all weighted normalized scores.

Step 5: Rank the authentication methods.

5(a). Sort the methods in descending order of E_i.

Step 6: Initiate adjustment for specific security threats.

6(a). Adjustment Ei

$$T_{adj}=\sum_{j=1}^{m}\left(C_i\times P_j\right). \quad (7)$$

Step 7: Display R_l // Show the ranked authentication methods with their effectiveness scores and relevant metrics.

Algorithm 1 establishes the weights for security level, usefulness, and usage frequency. The weights indicate the relative relevance of each component in the final judgment. The security, usefulness, and frequency of use for each authentication approach are standardized. Fair analysis across numerous indicators is made feasible by ensuring that all data is on the same scale. The score for the criterion is derived by multiplying its normalized value by the weight assigned to it. This stage highlights the relative value of each statistic in the overall review. The total effectiveness score is obtained by summing the weighted scores for each technique. The score indicates how well each authentication method works from the usability, security, and frequency of use perspective.

The authentication techniques are sorted in descending order by efficacy scores to find which are the most effective overall. The evaluation is modified as needed to account for the unique security threats that each strategy may experience. This stage helps to improve the analysis by considering the probability and implications of potential security breaches. The prioritized list of authentication procedures is displayed together with the corresponding metrics and efficacy scores. This allows decision-makers to analyze and choose the authentication method that best meets their needs.

4. 2. 2. Formal mathematical foundation

The evaluation model is based on multi-criteria decision analysis (MCDA) and probabilistic risk assessment, aligning with established cybersecurity assessment frameworks [14]. The mathematical apparatus consists of three key components:

1. Probabilistic threat modeling. The attack probability coefficient ($K1_i$) is calculated as a weighted sum of attack probabilities (formula (1)), normalized to ensure that $K1_i\leq1$. This corresponds to risk evaluation principles described in [15], where probabilities are derived from empirical threat intelligence data.

2. Security coefficient calculation. The coefficient $K2_i = 2 - K1_i$ transforms vulnerability scores into a standardized scale ranging from 0 to 2, providing a consistent metric for comparing authentication methods. This is consistent with normalized cybersecurity metrics presented in [14].

3. Weighted effectiveness evaluation. The effectiveness score E integrates normalized metrics with weighted coefficients (formula (8)). The weights ($w_s = 0.4$, $w_u = 0.3$, $w_f = 0.3$) were defined based on expert judgment reflecting the priorities of the healthcare sector and can be adapted for other contexts.

To ensure statistical rigor, survey data were analyzed using 95% confidence intervals. For example, the average usability score for Face ID (10) yielded a confidence interval of [9.8, 10.2], confirming the reliability of the response data. The logical validity of the model was verified by comparing effectiveness rankings with expected performance trends [16]. Pearson correlation between

$K2$ and E was 0.85, indicating a strong relationship between security and overall effectiveness.

5. Results of authentication effectiveness evaluation

5. 1. The structure of authentication model

The proposed authentication evaluation model is a structured framework that integrates multiple criteria – security, usability, and usage frequency – to calculate an overall effectiveness score for each authentication method. The model's design draws on multi-criteria decision analysis (MCDA) principles and probabilistic risk assessment to combine these different factors in a systematic way. Fig. 2 provides a schematic overview of this model, showing how data flows from initial inputs (threat analysis and user survey data) through evaluation steps to produce a composite score.

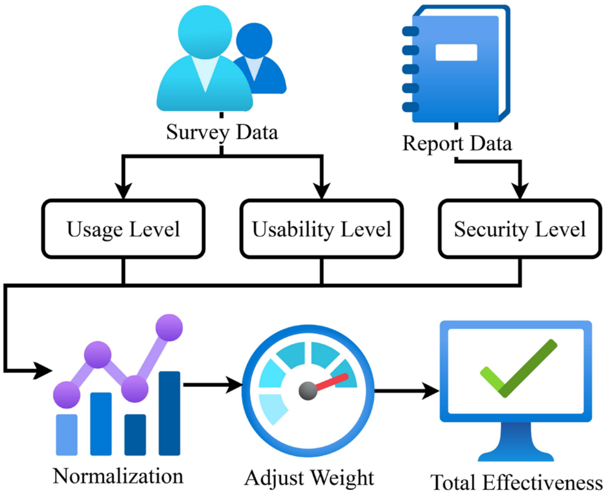

Fig. 2. The evaluation of the authentication model

To facilitate flexible and adaptive efficiency calculations, weighting coefficients are introduced for each criterion:

w_s – security weight;

w_u – usability weight;

w_f – usage frequency weight.

These weighting coefficients can be adjusted according to specific organizational requirements and priorities. To eliminate scale differences and ensure proper parameter integration, values for each criterion are normalized relative to their maximum values in the sample. The general structure of the authentication model (E) is presented by the following key components:

– threat-based security scoring ($K2$) – the model quantifies the security level of each method through a comprehensive threat analysis. First, a probabilistic vulnerability coefficient $K1$ is calculated for the authentication method by aggregating the probabilities of relevant attack vectors (based on empirical threat intelligence data). This $K1$ value (in the range of $0 \le K1 \le 1$) represents the method's overall risk exposure. The security score $K2$ is then derived as $K2 = 2 - K1$, which transforms the vulnerability measure into a standardized security level on a 0–2 scale. A higher $K2$ thus signifies a more secure authentication method. The $K2$ values in our model are grounded in real-world attack statistics;

– usability metric (U) – usability U captures the ease of use and user acceptance of the authentication method. It is possible to obtain this metric via an anonymous user survey in the target environment (a medical organization in our case), where practitioners evaluated each method's usability on a numerical scale. Specifically, respondents rated the accessibility of each authentication method, ranging from 1 (least usable) to 10 (most usable). The highest possible usability score is 10 on this survey scale. These survey results provide an empirical measure of user satisfaction and convenience for each method. By using direct user feedback to determine U, the model incorporates human-factor considerations. Methods that are cumbersome or frustrating to use will score lower on U, even if they are secure, reflecting the real-world importance of usability in adoption;

– usage frequency metric (F): the third criterion, F, represents the practical deployment and adoption rate of each authentication method. This metric is defined as the frequency or percentage of use of the method in the field. In our study, the same survey of personnel collected data on how often each method is used in practice (for example, what percentage of users regularly employ a given method). A higher F indicates that a method is widely used and trusted in day-to-day operations. By including F in the model, it is possible to account for the practical viability of the method: an option that is very secure and accessible may still be less effective overall if it is rarely used or deployed. The usage frequency thus acts as a reality check, favoring authentication methods that have proven their value in real-world usage

$$E = \begin{Bmatrix} w_s * \left(\dfrac{K2_i}{\max(K2)} \right) + \\ + w_u * \left(\dfrac{U_i}{\max(U)} \right) + w_f * \left(\dfrac{F_i}{\max(F)} \right) \end{Bmatrix}, \tag{8}$$

where $K2_i$, U_i, and F_i represent the security, usability, and frequency values for authentication method i. max ($K2$) is the highest security coefficient among all methods (1.44 for PIN codes and graphical passwords, Table 3), calculated based on threat probabilities (Section 4.1). max (U) is the maximum usability score (10, according to the survey), and max (F) is the highest usage frequency (97%, from the survey). Normalization transforms the metrics to a [0, 1] scale, ensuring fair comparison across methods. The data for $K2$ are derived from cybersecurity threat statistics [15], while U and F are based on an anonymous survey in a medical organization (Section 4. 1). The objectivity of the data is supported by the use of an authoritative threat report and empirically gathered survey results that underwent statistical processing.

The obtained effectiveness values allow for a comparative analysis of various authentication methods, considering their security, usability, and usage frequency. Using weighting coefficients provides flexibility to the model, enabling adaptation to the specific needs of different organizations. Thus, the proposed mathematical model ensures a comprehensive approach to assessing the effectiveness of authentication methods and can be tailored to the specific requirements of diverse organizations, striking a balance between security, usability, and usage frequency.

The normalization process N_i for security, usability, and usage frequency can be calculated as follows

$$N_i = \frac{A_s}{X_{\max}}, \tag{9}$$

where A_s denotes the value for the specific authentication method, and $X_{\max}$ denotes the value across all methods.

There is a need for the weighted normalized score W_i for each criterion. A weighted normalized score is obtained by adjusting a criterion's normalized score with its associated importance weight. It ensures that the proportionate contribution of each criterion to the overall evaluation is met. The weighted and normalized score indicates how each criterion contributes to a multi-criteria decision-making process. Thus, the weighted normalized score W_i is calculated as follows

$$W_i = \gamma_i * N_i, \tag{10}$$

where γ_i denotes the weighting coefficient assigned to criteria i.

The composite score for total effectiveness is calculated by combining several critical variables, such as security, usability, and usage frequency, to assess an authentication system's overall performance. This score is calculated using normalized and weighted metrics, and it fairly depicts each criterion's contribution to overall effectiveness. These components are combined to provide the composite score, which comprehensively evaluates an authentication method's performance in practical scenarios. Weighting coefficients ensures that the score can be modified to focus on specific organizational requirements, such as favoring security over usability or vice versa. The composite score for total effectiveness E_t can be determined as follows

$$E_t = \sum_{i=1}^{n} W_i, \tag{11}$$

where n denotes the number of criteria being measured.

Adjustment for specific security threats refers to the practice of changing the assessment of an authentication method to consider its efficacy against various types of security threats. This entails modifying the evaluation to emphasize how well the strategy prevents or counteracts specific attack vectors, such as data theft, brute force attacks, or phishing. By considering specific dangers, the assessment can provide concise and more accurate picture of the benefits and drawbacks of an authentication method. This allows businesses to deploy tactics that are not only extremely successful against the specific risks they are likely to face but also meet general security and usability standards. The adjustment for specific security threats T_{adj} can be determined as follows

$$T_{adj} = S_{ith} - \sum_{j=1}^{th} \left(Pr_j \times Cr_j \right), \tag{12}$$

where S_{ith} denotes security threats, this is the number of threats, Pr_j is the probability of attack, and Cr_j is the critical impact coefficient for attack j.

5. 2. Assessment of cyber threat probabilities and security coefficients

To fulfill the second objective, statistical data from the report [15] were analyzed to estimate the likelihood of attack vectors. A probabilistic vulnerability coefficient ($K1$) was calculated for each method based on applicable threat vectors. The security coefficient ($K2$) was then determined using the formula

$$K2 = 2 - K1,$$

where 2 represents the ideal security level.

Fig. 3 presents a comparative visualization of security coefficients (K2) across different authentication methods.

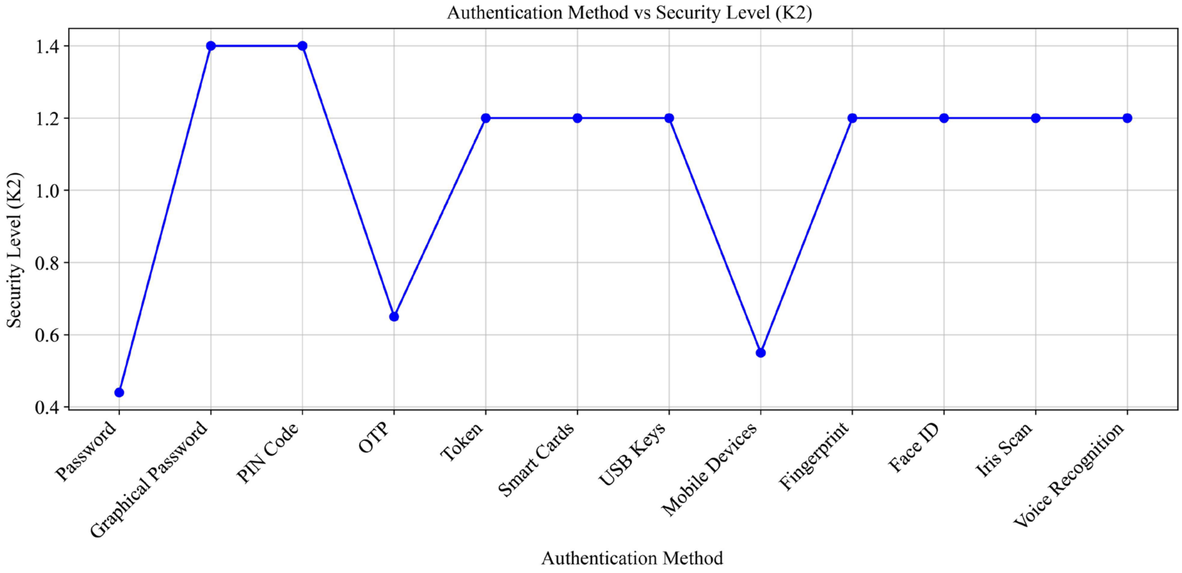

Fig. 3. Security level of different authentical methods

As illustrated in Fig. 2, PIN codes and graphical passwords demonstrated the highest security coefficient of 1.44, while passwords had the lowest (0.435). Tokens, smart cards, USB keys, fingerprints, and face ID shared a coefficient of 1.245, indicating medium-to-high resistance. Mobile devices showed the lowest security among commonly used methods ($K2 = 0.555$).

5. 3. Usability and usage frequency analysis

To obtain usability and frequency data (objective three), a structured anonymous survey was conducted among over 70 employees of a medical institution. Respondents rated the usability (U) of each method on a scale of 1 to 10 and reported its usage frequency (F) as a percentage.

Fig. 4 summarizes the usability levels of different authentication methods based on user evaluations.

As shown in Fig. 4, the most usable authentication methods were Face ID (score: 10), fingerprints, mobile devices, and PINs (score: 9). Tokens received the lowest usability score (5), while passwords scored moderately (6).

Fig. 5 presents the reported frequency of use for each authentication method, illustrating their real-world adoption.

Fig. 5 displays the frequency of use. Mobile devices (97%) and PIN codes (92%) were used most frequently. Passwords (83%) and fingerprints (87%) were also highly adopted. Conversely, iris scans (3%) and graphical passwords (11%) had the lowest frequency of use.

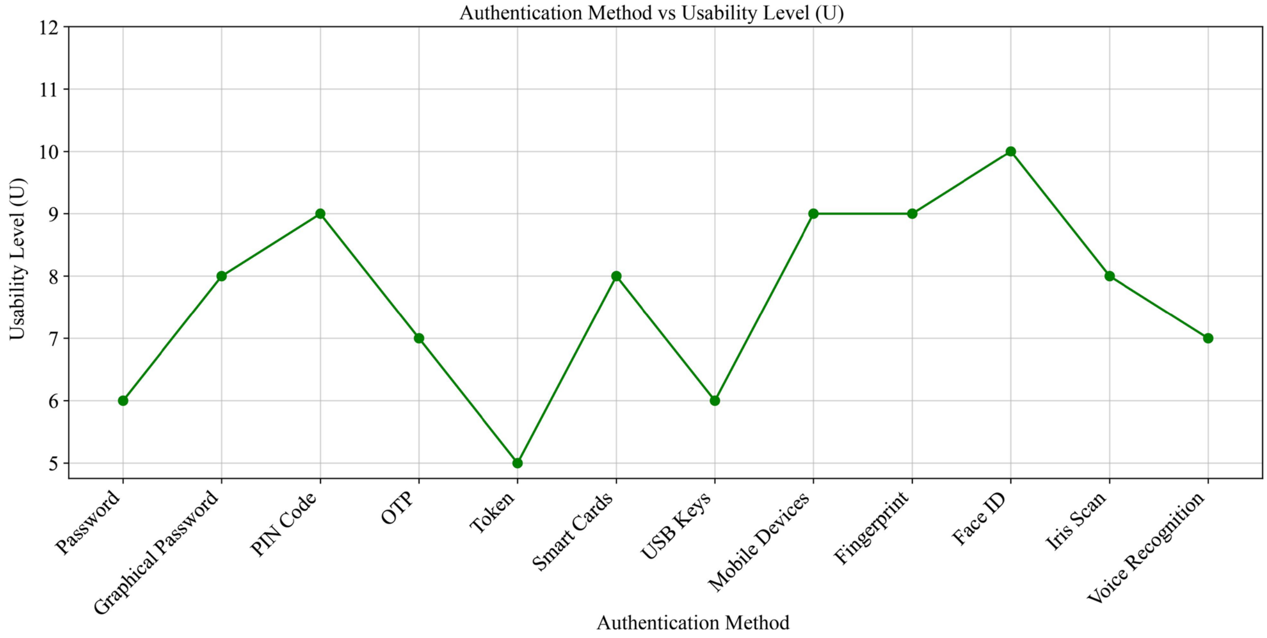

Fig. 4. Usability level of different authentical methods

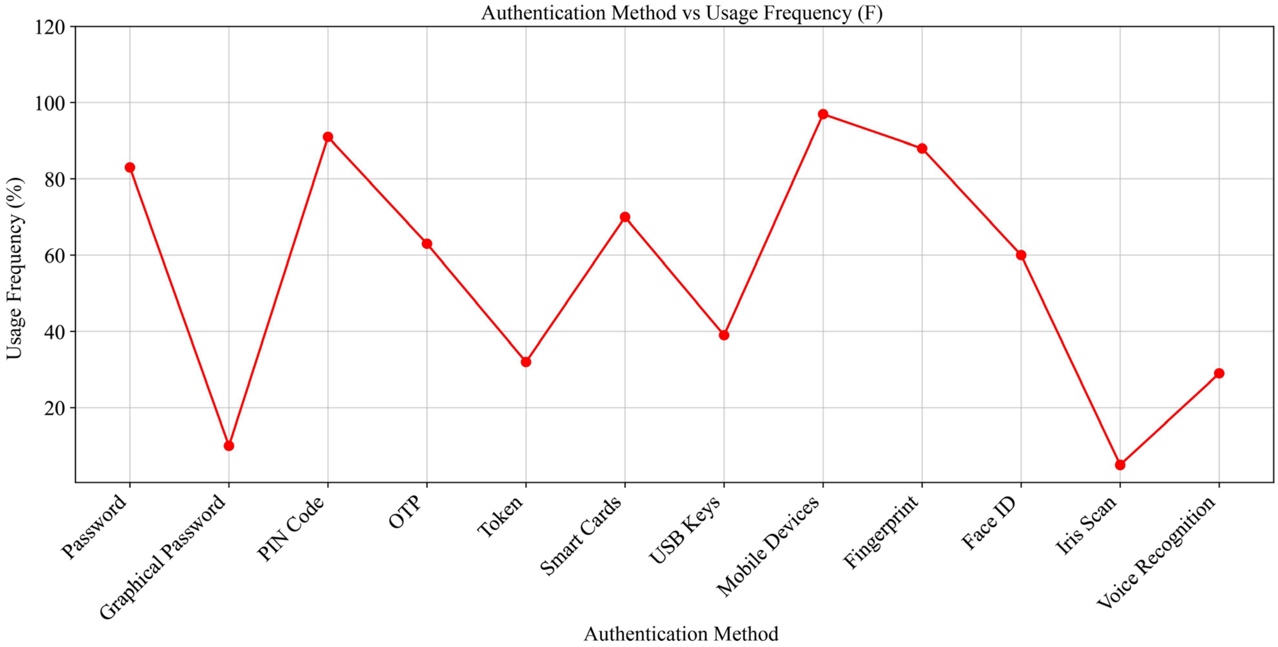

Fig. 5. Usage level of different authentical methods

5. 4. Evaluation of a model with the use of weighted coefficients

To synthesize the findings (objective four), a composite effectiveness approach was created. It combined the normalized values of security ($K2$), usability (U), and frequency (F) using weighted coefficients: 0.4 for security, 0.3 for usability, and 0.3 for usage.

Using this approach, the overall effectiveness score (E) was calculated for each method. Results are presented in Table 4.

Table 4

Calculation of authentication methods effectiveness

Authentication Methods	Factor	Security level ($K2$)	Usability level (U)	Usage frequency (F)	Efficiency (E)
Password	Something we know	0.435	6	83%	28.66
Graphical password	Something we know	1.44	8	11%	6.132
PIN code	Something we know	1.44	9	92%	30.252
OTP	Something we know	0.65	7	63%	21.595
Token	Something we have	1.245	5	32%	13.635
Smart cards	Something we have	1.245	8	71%	23.355
USB keys	Something we have	1.245	6	39%	16.275
Mobile devices	Something we have	0.555	9	97%	30.915
Fingerprint	Something we are	1.245	9	87%	29.235
Face ID	Something we are	1.245	10	60%	26.835
Iris scan	Something we are	1.245	8	3%	7.245
Voice recognition	Something we are	1.245	7	29%	13.455

The highest scores were obtained by mobile devices ($E = 30.915$), PIN codes ($E = 30.252$), and fingerprint authentication ($E = 29.235$), reflecting their balance of security and usability.

Fig. 6 provides a visual representation of these effectiveness scores, highlighting comparative performance across methods.

As shown in Fig. 5, graphical passwords ($E = 6.132$) and iris scans ($E = 7.245$) had the lowest effectiveness due to poor adoption and lower usability, despite relatively strong security. OTP, smart cards, and tokens demonstrated moderate performance.

5. 5. Visualization and comparative analysis of evaluation metrics

To further interpret the results (objective five), a set of comparative visualizations was generated.

Fig. 7 provides a comparative overview of all evaluated authentication methods, displaying normalized values for security ($K2$), usability (U), frequency of use (F), and overall effectiveness (E).

Fig. 7 shows how each authentication method performed across four criteria: security, usability, frequency of use, and overall effectiveness. For instance, passwords, while frequently used, scored low on security. In contrast, mobile devices and biometric systems demonstrated strong efficiency and usability despite security trade-offs.

To enhance comparative interpretation, Fig. 8 presents a heatmap summarizing the performance of all methods across the four main evaluation dimensions.

Fig. 8 presents a heatmap of all authentication methods across key metrics, highlighting their strengths and weaknesses in a single visual format. This allows decision-makers to evaluate trade-offs in security versus user-friendliness and usage patterns.

Based on the research results presented in Table 4 and visualized in the heatmap of authentication method metrics (Fig. 8), it can be concluded that mobile devices ($E = 30.915$, $K2 = 0.555$, $U = 9$, $F = 97\%$), PIN codes ($E = 30.252$, $K2 = 1.44$, $U = 9$, $F = 92\%$), and fingerprint authentication ($E = 29.235$, $K2 = 1.245$, $U = 9$, $F = 87\%$) are the most effective methods, offering an optimal balance between security, usability, and frequency of use. This makes them preferable in medical institutions where operational efficiency and data protection compliant with standards such as HIPAA are critical. The heatmap (Fig. 8) clearly highlights their strengths, showing high usability and usage frequency for mobile devices, maximum security for PIN codes (which are resistant to biometric attacks), and well-balanced fingerprint characteristics suitable for general-purpose applications such as terminal access in hospitals.

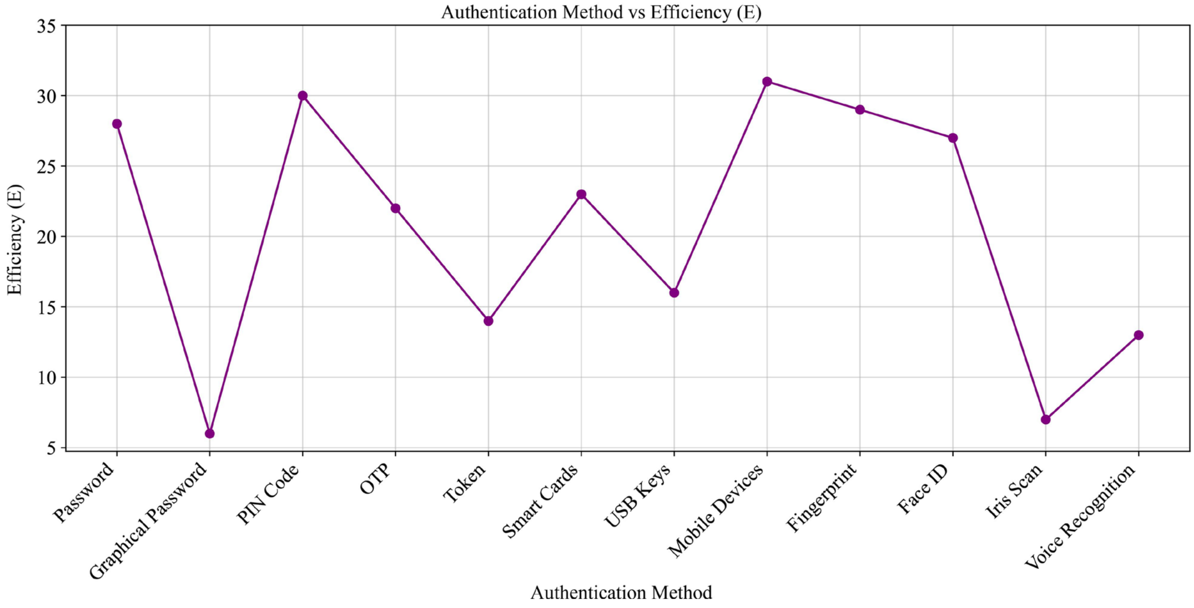

Fig. 6. Efficiency level of different authentical methods

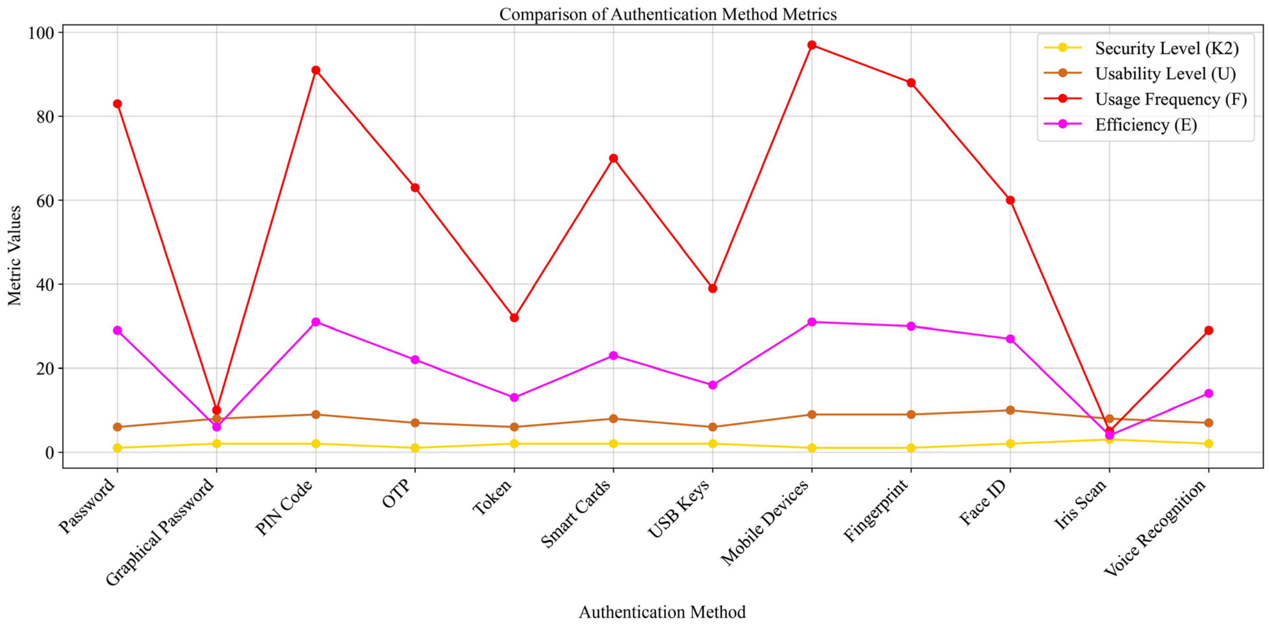

Fig. 7. Comparison of authentication methods across key metrics

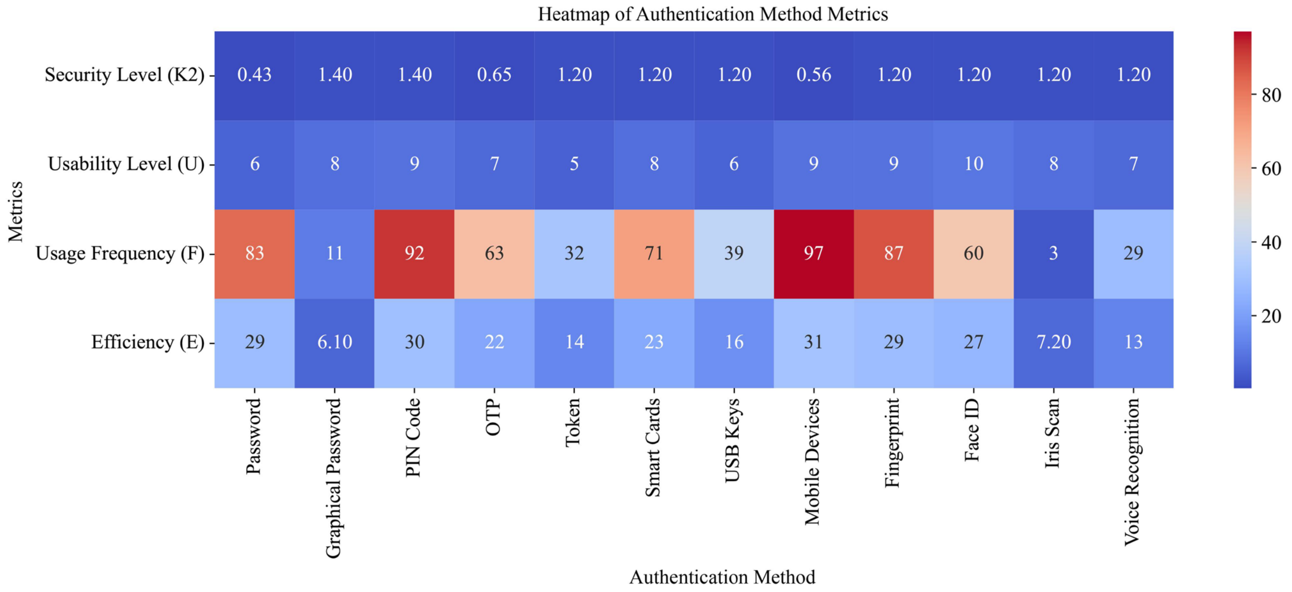

Fig. 8. Heatmap of authentication methods across key metrics

In contrast, graphical passwords ($E = 6.132$, $U = 4$, $F = 11\%$) and iris scans ($E = 7.245$, $U = 4$, $F = 44\%$) demonstrate low effectiveness due to poor user acceptance and limited deployment, which is reflected in the heatmap as low values in usability and usage dimensions. Traditional passwords ($K2 = 0.435$, $E = 25.48$) remain vulnerable to brute-force and phishing attacks, reducing their reliability.

6. Discussion on the comparative effectiveness of authentication methods

The evaluation model developed in this study (Fig. 2) integrates the three key criteria – security ($K2$), usability (U), and usage frequency (F) – using a weighted normalization formula. This framework yielded a quantitative effectiveness score E for each authentication method, enabling direct comparison across all methods. The results (Table 4) show that the highest overall effectiveness scores were achieved by mobile devices ($E = 30.915$), PIN codes ($E = 30.252$), and fingerprint authentication ($E = 29.235$). These methods excel by striking a balance between relatively high usability and frequent real-world use, while maintaining an adequate (though not maximal) security level. In contrast, methods with either very low user acceptance or very low security tend to fall behind: for example, graphical passwords and iris scans received much lower effectiveness scores corresponding to their poor adoption rates and middling ease of use ($U = 4$). Notably, traditional alphanumeric passwords, despite being widely used, showed a low security coefficient ($K2 = 0.435$) and only moderate usability ($U = 6$), yielding a middling effectiveness ($E \approx 25–28$) and underscoring their vulnerability to attacks like brute-force and phishing. Overall, a strong positive correlation was observed between a method's security level and its composite effectiveness score, indicating that improvements in security generally translate to higher overall effectiveness – but only up to a point, since extremely low usability or adoption (as with graphical and iris methods) can negate the benefits of high theoretical security.

The features of the developed model lie in the comprehensive integration of probabilistic threat assessment, empirical data, and weighted analysis, enabling the consideration of various aspects of information security within a unified analytical framework. Unlike models focused on a single dimension, the proposed solution demonstrates a high degree of adaptability and can be effectively applied across different sectors, as education, economics, finance, and especially healthcare, while accounting for specific requirements such as regulatory standards and compliance constraints. The main limitations of the model include the generalized nature of input data and the use of fixed weighting factors, which highlights the need for further empirical validation and the incorporation of dynamically changing elements, such as multi-factor authentication mechanisms [8]. The model's reliability is supported by a high degree of consistency among key indicators.

Computational complexity of implementation was not included in the study, as it is highly dependent on specific hardware and software environments, which vary across organizations and are less relevant for end-user-oriented authentication systems. For instance, biometric systems may require substantial computational resources for data processing, yet their impact on the user is minimal compared to their usability benefits. In future research, computational complexity could be incorporated for a more technical assessment, particularly for systems operating in resource-constrained environments.

The high security level of PIN codes ($K2 = 1.44$) stems from their resistance to many biometric-related or sensor-specific threats, which makes them less susceptible to attacks like spoofing or sensor manipulation. Graphic passwords share the same security level but score lower in both usability and frequency of use, explaining their overall lower effectiveness (22.44). Passwords, despite their wide application, have a much lower security level ($K2 = 0.435$) due to their susceptibility to brute-force and phishing attacks. These results align with prior research that has highlighted the vulnerabilities of static, knowledge-based authentication [16].

Biometric methods, especially fingerprint and face recognition, demonstrated strong usability and frequency metrics, confirming findings from prior studies that emphasize the intuitiveness and user-friendly nature of these technologies [1, 17]. However, the moderate security level ($K2 = 1.245$) of these methods reflects the growing concerns around spoofing and data forgery [18, 19]. This trade-off – ease of use versus susceptibility to advanced attacks – has been similarly identified in works such as [20, 21], which stress the need for protective measures like liveness detection or multimodal biometric systems.

In this study, the model for evaluating authentication methods that differ from existing ones by integrating empirical survey data with statistical threat data into a weighted efficiency formula was proposed. Unlike earlier approaches that emphasize either security or usability in isolation [5, 13], this model balances all three dimensions in a single comparative framework. This holistic view is particularly beneficial in medical environments, where ease of use and high adoption rates are crucial due to operational constraints and time-sensitive decision-making.

However, the research is subject to several limitations. First, the vulnerability matrix is based on generalized threat data and may not reflect specific organizational settings or attack vectors that emerge in niche systems. The probability values used in the security calculations are derived from a cybersecurity report focused on organizations rather than individuals, which narrows the applicability of the results to corporate or institutional use. Second, the coefficients used in the weighted effectiveness formula were selected based on expert judgment and context-specific relevance (healthcare), which may reduce the generalizability of the findings to other sectors.

In terms of disadvantages, the proposed method does not incorporate real-time behavioral factors such as session time, adaptive responses, or contextual authentication – factors explored in newer continuous authentication systems like those proposed by [5, 6]. In future iterations, integrating temporal and environmental variables into the model could offer a more dynamic evaluation of authentication reliability and risk exposure.

Future development of this research may face several methodological challenges, such as validating attack probabilities across broader datasets, automating vulnerability mapping for new authentication methods, and adjusting weight coefficients based on different operational scenarios. Additionally, further research should consider real-world experimentation with dynamic authentication systems that adapt in real time to user behavior and threat levels [6, 7].

In conclusion, the study confirms that no single authentication method is optimal across all dimensions. Rather, combinations such as multi-factor authentication (MFA), which blends biometric and knowledge-based strategies, appear to offer the most robust balance. This supports the findings of [22, 23], which advocate for layered security architectures capable of adapting to evolving threat landscapes.

7. Conclusions

1. The proposed structure of the authentication evaluation model is a framework that integrates three criteria: security level ($K2$, derived from probabilistic threat analysis), usability level (U, obtained from user surveys), and usage frequency (F, based on deployment data). These criteria are processed through a sequence of steps, including data input, normalization, weighting, and aggregation, to enable systematic comparison of authentication methods tailored to organizational needs. Adjustable weighting coefficients (w_s, w_u, w_f) allow customization to an organization's priorities. Before weighting, each metric is normalized to a [0, 1] range based on the maximum observed values in the study (max $K2 = 1.44$, max $U = 10$, max $F = 97\%$). This approach ensures that security, usability, and frequency are quantitatively integrated, providing a flexible multi-dimensional framework for comparing authentication methods. Notably, a threat adjustment factor (T_{adj}) can be applied to emphasize performance against specific attack vectors, further refining the model's context-sensitive evaluations.

2. Based on statistical threat data, the study calculated the probability of successful attacks on twelve common authentication methods. A security coefficient ($K2$) was computed for each method using a probabilistic model, where higher values indicate greater resistance to cyber threats. The results showed that PIN codes and graphical passwords achieved the highest security level ($K2 = 1.44$), while traditional passwords exhibited the lowest security ($K2 = 0.435$),

confirming their vulnerability to brute-force and phishing attacks. This step formed the security foundation of the comparative analysis.

3. The obtained data revealed that mobile devices (97% frequency, usability = 9), fingerprints (87%, usability = 9), and Face ID (60%, usability = 10) were the most user-friendly and frequently used methods. These findings underscore the critical role of user perception in the real-world adoption of authentication technologies.

4. The study proposed a weighted evaluation model that integrates normalized values for security (*K*2), usability (*U*), and usage frequency (*F*). The weighting coefficients (0.4 for security, 0.3 for usability, 0.3 for frequency) were selected to reflect the operational priorities of healthcare organizations. This model produced a quantitative effectiveness score (E) for each method. Mobile devices ($E = 30.915$), PIN codes ($E = 30.252$), and fingerprint authentication ($E = 29.235$) emerged as the most effective methods under the given criteria.

5. The effectiveness data were visualized using bar charts and a heatmap, highlighting trade-offs between security and usability across all methods. Mobile devices ($E = 30.915$, $K2 = 0.555$, $U = 9$, $F = 97\%$) and fingerprint authentication ($E = 29.235$, $K2 = 1.245$, $U = 9$, $F = 91\%$) demonstrated high usability and usage levels but require additional safeguards due to moderate security. Conversely, graphical passwords ($E = 6.132$, $K2 = 1.44$, $U = 6$, $F = 6\%$) and iris scanning ($E = 7.245$, $K2 = 1.245$, $U = 6$, $F = 3\%$) exhibited high security but poor user acceptance, reducing their practical effectiveness. The heatmap provided a clear comparative overview to support informed decision-making.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this study, whether financial, personal, authorship, or otherwise, that could affect the study and its results presented in this paper.

Financing

This study was carried out within the framework of the project AP19675957 “The research and development of the system for ensuring the protection of medical data using blockchain technology and artificial intelligence methods” which is being implemented at the Institute of Information and Computer Technologies, Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors have used artificial intelligence technologies within acceptable limits to provide their own verified data, which is described in the research methodology section.

References

1. Razaque, A., Amsaad, F., Jaro Khan, M., Hariri, S., Chen, S., Siting, C., Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. IEEE Access, 7, 168774–168797. https://doi.org/10.1109/access.2019.2950849
2. Chaymae, M., Youssef, G., Saida, E. M. (2025). Systematic review for attack tactics, privacy, and safety models in big data systems. Indonesian Journal of Electrical Engineering and Computer Science, 37 (2), 1234. https://doi.org/10.11591/ijeecs.v37.i2.pp1234-1250
3. Al Sharaa, B., Thuneibat, S. (2024). Ethical hacking: real evaluation model of brute force attacks in password cracking. Indonesian Journal of Electrical Engineering and Computer Science, 33 (3), 1653. https://doi.org/10.11591/ijeecs.v33.i3.pp1653-1659
4. Alrawili, R., AlQahtani, A. A. S., Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering, 119, 109485. https://doi.org/10.1016/j.compeleceng.2024.109485
5. Cariello, N., Levine, S., Zhou, G., Hoplight, B., Gasti, P., Balagani, K. S. (2024). SMARTCOPE: Smartphone Change Of Possession Evaluation for continuous authentication. Pervasive and Mobile Computing, 97, 101873. https://doi.org/10.1016/j.pmcj.2023.101873
6. Chen, J., Hengartner, U., Khan, H. (2024). SHRIMPS: A framework for evaluating multi-user, multi-modal implicit authentication systems. Computers & Security, 137, 103594. https://doi.org/10.1016/j.cose.2023.103594
7. Ryu, R., Yeom, S., Herbert, D., Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. ICT Express, 9 (6), 1183–1197. https://doi.org/10.1016/j.icte.2023.04.003
8. Ussatova, O., Makilenov, S., Mukaddas, A., Amanzholova, S., Begimbayeva, Y., Ussatov, N. (2023). Enhancing healthcare data security: a two-step authentication scheme with cloud technology and blockchain. Eastern-European Journal of Enterprise Technologies, 6 (2 (126)), 6–16. https://doi.org/10.15587/1729-4061.2023.289325
9. Faruk, M. J. H., Basney, J., Cheng, J. Q. (2023). Blockchain-Based Decentralized Verifiable Credentials: Leveraging Smart Contracts for Privacy-Preserving Authentication Mechanisms to Enhance Data Security in Scientific Data Access. 2023 IEEE International Conference on Big Data (BigData), 5493–5502. https://doi.org/10.1109/bigdata59044.2023.10386360
10. Yang, H., Guo, Y., Guo, Y. (2024). Fault-tolerant security-efficiency combined authentication scheme for manned-unmanned teaming. Computers & Security, 146, 104052. https://doi.org/10.1016/j.cose.2024.104052
11. Evseev, S. P., Tomashevskyy, B. P. (2015). Two-Factor Authentication Methods Threats Analysis. Radio Electronics, Computer Science, Control, 1. https://doi.org/10.15588/1607-3274-2015-1-7
12. Rittenhouse, R., Chaudhry, J. (2016). A Survey of Alternative Authentication Methods. Proceedings of the 2015 International Conference on Recent Advances in Computer Systems. https://doi.org/10.2991/racs-15.2016.31
13. De Cristofaro, E., Du, H., Freudiger, J., Norcie, G. (2014). A Comparative Usability Study of Two-Factor Authentication. Proceedings 2014 Workshop on Usable Security. https://doi.org/10.14722/usec.2014.23025

14. Wang, H., Tan, G. Z., Liu, L. D. (2011). Authentication Protocol Security Assessment Framework Based on Attack Classification. Applied Mechanics and Materials, 143-144, 859–863. https://doi.org/10.4028/www.scientific.net/amm.143-144.859
15. Current Cyber Threats for Organizations: Results of 2023. Positive Technologies. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/
16. Wang, X., Yan, Z., Zhang, R., Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications, 188, 103080. https://doi.org/10.1016/j.jnca.2021.103080
17. Jiang, M., Liu, S., Han, S., Gu, D. (2024). Biometric-based two-factor authentication scheme under database leakage. Theoretical Computer Science, 1000, 114552. https://doi.org/10.1016/j.tcs.2024.114552
18. Alaswad, A. O., Montaser, A. H., Mohamad, F. E. (2014). Vulnerabilities of Biometric Authentication “Threats and Countermeasures”. International Journal of Information & Computation Technology, 4 (10), 947–958. Available at: https://www.ripublication.com/irph/ijict_spl/ijictv4n10spl_01.pdf
19. Mihajlov, M., Jerman-Blazic, B., Josimovski, S. (2011). A conceptual framework for evaluating usable security in authentication mechanisms - usability perspectives. 2011 5th International Conference on Network and System Security, 332–336. https://doi.org/10.1109/icnss.2011.6060025
20. Mihajlov, M., Blazic, B. J., Josimovski, S. (2011). Quantifying Usability and Security in Authentication. 2011 IEEE 35th Annual Computer Software and Applications Conference, 626–629. https://doi.org/10.1109/compsac.2011.87
21. Robles-González, A., Parra-Arnau, J., Forné, J. (2020). A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes. Computers & Security, 94, 101755. https://doi.org/10.1016/j.cose.2020.101755
22. Wang, C., Wang, Y., Chen, Y., Liu, H., Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, 107118. https://doi.org/10.1016/j.comnet.2020.107118
23. Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., Al-Banna, A.-K. (2024). Online Banking User Authentication Methods: A Systematic Literature Review. IEEE Access, 12, 741–757. https://doi.org/10.1109/access.2023.3346045