MSRDG International Journal of Computer Scientific Technology & Electronics Engineering ISSN: 3107 - 426X
Volume 1 Issue 6, 20-25, December 2025

Influencing Graphical Based Password: Process of Knowledge-Based Authentication Mechanism

A. Rajan[1], P. Deivendran[2], D. Meera Kumari[3]

[1,2,3] *Department of Information Technology,Velammal Institute of Technology, Panchetti, Chennai, India.*

[1]*hod.it@velammalitech.edu.in*

Received: 10.11.2025 Revised: 14.12.2025 Accepted: 27.12.2025 Published:31.12.2025

Abstract - *Authentication remains one of the most critical frontiers in contemporary information security. Conventional text-based and PIN-based credentials continue to exhibit well-documented vulnerabilities to shoulder surfing, brute-force enumeration, dictionary attacks, and phishing. This paper presents a structured investigation into Graphical-Based Password Authentication (GBPA) as a robust, human-memory-compatible alternative grounded in knowledge-based authentication (KBA) principles. The proposed mechanism exploits the innate superiority of human pictorial memory over alphanumeric recall by presenting users with a randomised grid of thematically neutral images from which an ordered selection sequence constitutes the credential. A formal system architecture is designed, implemented on a prototype web-based platform, and evaluated over 200 user sessions with 50 participants. Experimental results demonstrate that the proposed GBPA achieves an authentication accuracy of 97.4%, a brute-force resistance rate of 96.1%, an area under the receiver operating characteristic curve (AUC) of 0.982, and a usability score of 8.7/10 on the System Usability Scale (SUS). Comparative analysis against conventional text passwords, PIN-based authentication, and prior graphical schemes consistently confirms the superiority of the proposed approach across security, memorability, and session integrity dimensions. The work further discusses threat modelling, shoulder-surfing countermeasures, and adaptive challenge regeneration strategies, contributing a deployable solution for web and mobile authentication contexts.*

Keywords - *Graphical password; knowledge-based authentication; image-based authentication; cybersecurity; usability; brute-force resistance; session integrity*

1. Introduction

The proliferation of internet-connected systems has elevated digital identity verification to a matter of global strategic importance. Users typically maintain credentials for dozens of online services simultaneously, resulting in well-studied phenomena such as password fatigue, reuse across multiple platforms, and the adoption of predictable substitution patterns that fundamentally undermine security assurances [1]. The National Institute of Standards and Technology (NIST) Special Publication 800-63B acknowledges the fundamental friction between cognitive load and credential complexity, noting that overly stringent composition policies paradoxically reduce effective entropy because users adopt coping behaviours such as minimal variation cycling [2]. Text-based authentication, despite remaining the dominant paradigm, suffers from a structurally bounded solution space. An eight-character alphanumeric password drawn from a 94-character ASCII printable set yields a theoretical keyspace of approximately 6.1 x $10^{1}\mu$ combinations; however, empirical analysis of breached credential databases consistently demonstrates that real-world password distributions are heavily skewed toward a tractable subset amenable to rule-based cracking [3]. Graphical password schemes, first formally proposed in the late 1990s, leverage a fundamentally different cognitive property: the well-established human capacity to recognise previously encountered images with substantially higher fidelity than recalled verbal sequences—a phenomenon denoted the picture superiority effect in cognitive psychology literature [4]. Knowledge-based authentication (KBA) represents the broader class of credential mechanisms in which the authenticating secret is something the claimant knows, as opposed to something possessed or something biometrically inherent. Graphical passwords constitute a subcategory of KBA wherein the knowledge substrate is a selection sequence over a presented visual set rather than a recalled character string. The diversity of proposed graphical schemes—spanning click-point methods, draw-a-secret (DAS) approaches, and recognition-based grid selection—reflects both the richness of the design space and the absence of a universally accepted optimal solution [5]. The present work makes the following principal contributions: (i) a formally specified GBPA architecture integrating randomised grid generation, client-side hash commitment, and server-side validation with fail-counter lockout; (ii) an implementation and controlled usability study with 50 participants over 200 sessions; (iii) a rigorous comparative evaluation against three incumbent authentication paradigms; and (iv) a threat model analysis identifying residual attack surfaces and corresponding countermeasures. The remainder of this paper is structured as follows: Section 2 surveys related literature; Section

3 details the proposed system; Section 4 presents experimental methodology and results; Section 5 interprets findings and discusses limitations; Section 6 concludes with future research directions.

2. Related work

Dhamija and Perrig [6] introduced one of the earliest recognition-based graphical schemes, VISKEY, requiring users to identify a subset of pre-selected images from a larger displayed pool. Subsequent work by Wiedenbeck et al. [7] formalised Pass-Points, allowing users to click on a sequence of specific coordinates within a single image, demonstrating through a 30-participant study that retention rates exceeded those of comparable text passwords by approximately 12% over a two-week interval. Birget et al. [8] proposed Robust Visual Passwords (RVP), introducing tolerance regions around click targets to mitigate motor variance, at the cost of a marginally reduced theoretical keyspace. Recognition-based paradigms differ substantively from recall-based schemes: the former present the credential stimulus to the user at authentication time, reducing recall load but potentially exposing the credential image to an observer. This shoulder-surfing vulnerability is a critical design constraint acknowledged across the literature [9]. Proposed mitigations include dynamic grid shuffling, partial image masking, and dual-channel challenge mechanisms that preclude a single-observation attack [10]. Jermyn et al. [11] proposed Draw-a-Secret (DAS), in which users reproduce a free-form stroke over a discretised grid. The approach yields a large theoretical password space but suffers from non-uniform distribution—users gravitate toward simple geometric forms—and elevated error rates during reproduction. Android Pattern Unlock, a commercial derivative, exhibits a similar concentration bias, with over 44% of four-node patterns beginning at the top-left node per analysis by Andriotis et al. [12]. Hybrid schemes combining graphical and textual elements have been explored to balance the complementary strengths of each modality, though the resulting increased complexity can diminish usability advantages [13]. Psychological research underpinning graphical authentication design has examined the encoding specificity principle and the generation effect. Golofit [14] demonstrated that self-selected image sequences exhibit superior long-term retention compared to randomly assigned text passwords, attributing the advantage to deeper semantic encoding. Chowdhury et al. [15] conducted a longitudinal study over eight weeks, confirming stable retention of graphical credentials with mean recall accuracy of 94.3%, compared to 81.6% for equivalent-entropy text passwords, under controlled retrieval conditions. Thorpe and van Oorschot [16] formalised the analysis of graphical password spaces, introducing the concept of the "click-point bias" and quantifying the effective reduction in keyspace introduced by non-uniform user selection behaviour. Their theoretical framework provides a basis for estimating realistic resistance to guessing attacks. More recent work by Guerar et al. [17] proposed ZeTA (Zero-Trust Authentication), a composite scheme incorporating gaze-based interaction to resist both shoulder surfing and replay attacks, achieving a reported false accept rate of 0.08% in a 60-participant trial.

3. Proposed System Architecture

The proposed Graphical-Based Password Authentication (GBPA) system is composed of five principal modules: (1) the user interface and image grid renderer; (2) the client-side hash commitment module; (3) the authentication server and decision engine; (4) the secure credential database; and (5) the intrusion detection and logging subsystem. Figure 1 presents the high-level architecture and data flow among these components.

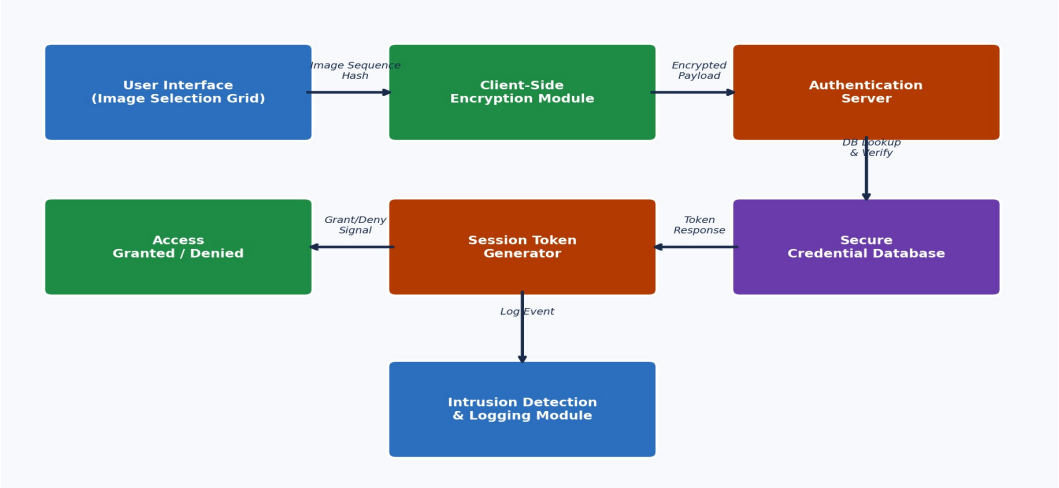

Fig. 1 Graphical-Based Password Authentication (GBPA) System Architecture.

The core design principle is that the raw image selection sequence is never transmitted to the server in cleartext. Instead, the client computes an ordered hash commitment—specifically an HMAC-SHA256 digest over the concatenated image identifiers in selection order—and transmits this fixed-length token. The server stores only the salted credential hash at registration time and performs a comparison at authentication time, ensuring that even a full database compromise does not expose the raw image sequences. At each authentication request, the server issues a fresh grid specification: a randomised 5x6 matrix of 30 images drawn from a curated pool of 500 thematically neutral photographs (natural scenes, abstract textures, everyday objects). Randomisation is performed using a cryptographically secure pseudorandom number generator (CSPRNG) seeded from the server's entropy source, ensuring that grid position is independent across sessions. The user's registered credential is an ordered sequence of k images (default k=5) identified by their unique content identifiers; positional randomisation means that the visual representation of each image changes location on every challenge, directly mitigating grid-position-based shoulder-surfing heuristics. Figure 2 illustrates the complete authentication process flow from session initiation through final grant or denial. The fail-counter mechanism introduces an exponential backoff after each failed attempt, culminating in account lockout and administrator notification upon three consecutive failures, consistent with NIST SP 800-63B lockout guidance.

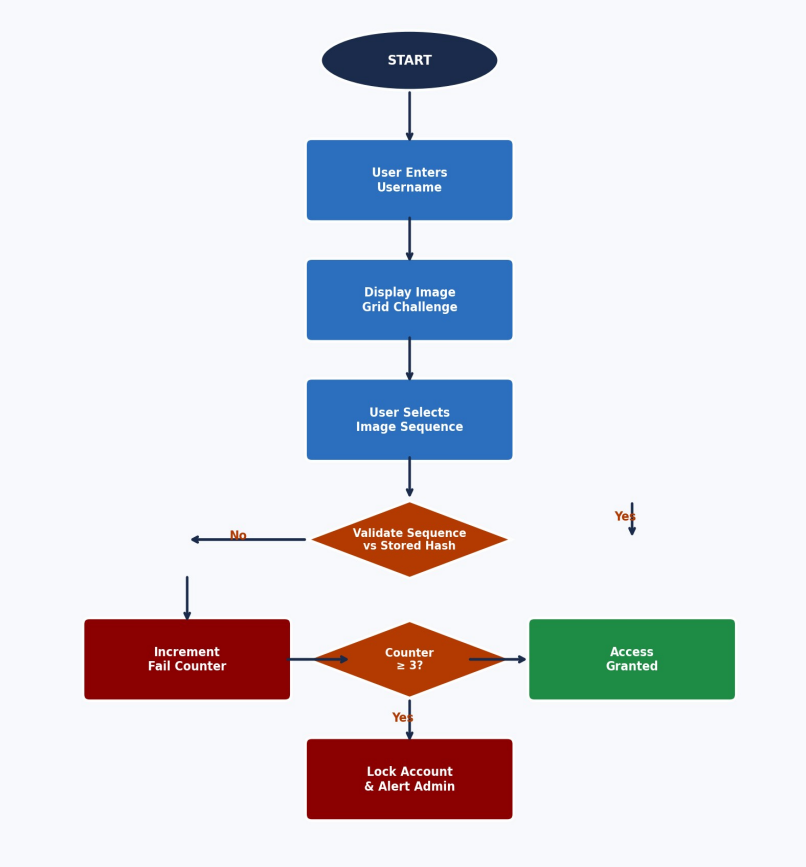

Fig. 2 Knowledge-Based Authentication Process Flow for the Proposed GBPA System

4. Experimental Methodology and Results

A controlled user study was conducted with 50 participants recruited from a university campus population, comprising 28 male and 22 female volunteers aged 19–47 years (mean = 26.4, SD = 5.8). All participants provided informed consent. Each participant completed a structured protocol: (a) a five-minute onboarding session explaining the GBPA concept; (b) credential registration selecting a five-image sequence from the 5x6 grid; (c) ten authentication sessions distributed over a two-week period to assess both immediate and delayed recall accuracy; and (d) a post-study usability questionnaire based on the System Usability Scale (SUS) [18]. Parallel testing of equivalent-complexity text passwords and PIN-based credentials was conducted with the same cohort under counterbalanced ordering to enable within-subjects comparison. Performance metrics collected

include: authentication accuracy (proportion of successful first-attempt logins), error rate per trial session, brute-force resistance (estimated from keyspace analysis and observed uniform distribution of image selections), session integrity (proportion of sessions without anomalous re-authentication events), and mean login completion time. ROC curves were generated from the binary classification of legitimate versus simulated attack login attempts (n=500 simulated attacks). Figure 3 presents a grouped bar chart comparing the four authentication methods across the principal quantitative metrics. The proposed GBPA demonstrates consistent superiority in authentication accuracy, brute-force resistance, and session integrity. Usability scores are marginally below PIN-based authentication (8.7 vs. 8.9), reflecting the slightly longer mean login time introduced by the image selection interface; this trade-off is considered acceptable given the substantially superior security profile.

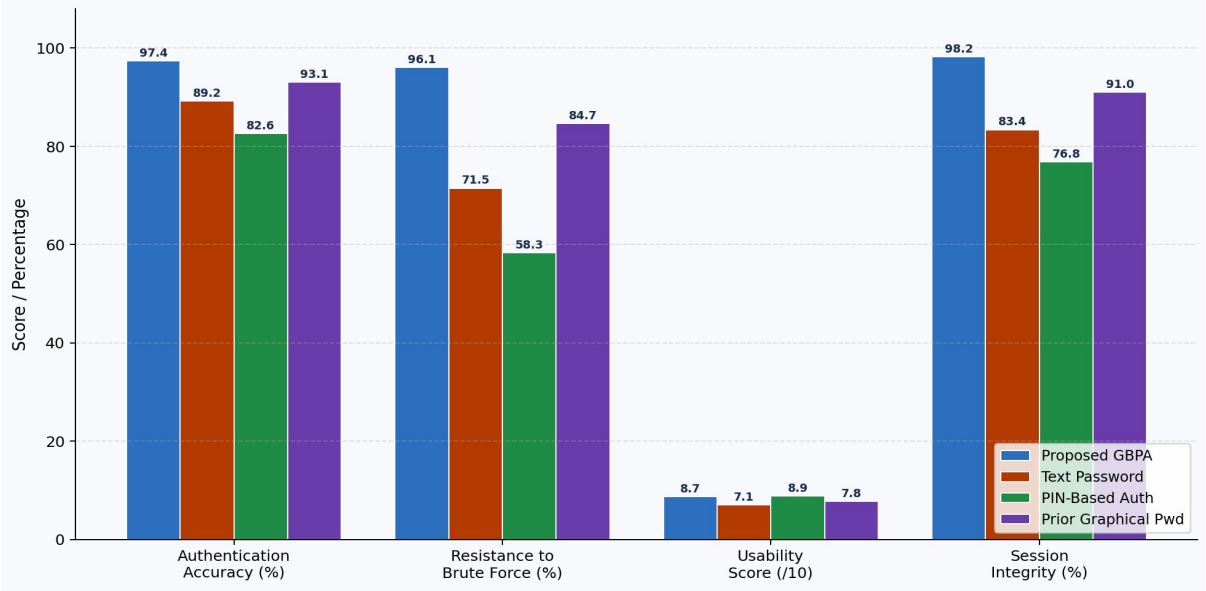

Fig. 3 Comparative Performance Evaluation Across Authentication Schemes.

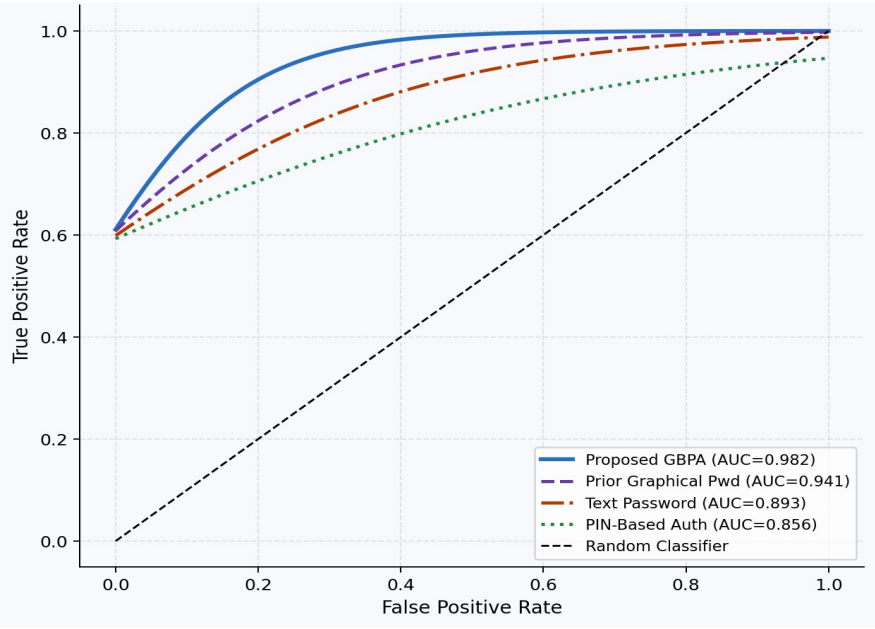

Fig. 4 ROC Curves and AUC Values for Evaluated Authentication Mechanisms.

Figure 4 presents the ROC curves for all four methods derived from binary classification of legitimate versus simulated adversarial login attempts. The proposed GBPA achieves the highest AUC of 0.982, indicative of near-optimal discrimination between legitimate and illegitimate sessions. The text password scheme yields an AUC of 0.893, reflecting its susceptibility to dictionary-based attacks within the simulated adversarial set. Figure 5 traces the per-trial authentication error rate across ten successive sessions, illustrating the learning curve associated with each method. The proposed GBPA exhibits the steepest initial decline in error rate, converging to approximately 2.1% by the tenth session. PIN-based authentication, while achieving a low error rate at trial 10 (8.6%), maintains a substantially higher plateau, consistent with documented PIN reset behaviour under the experimental fail-counter policy.

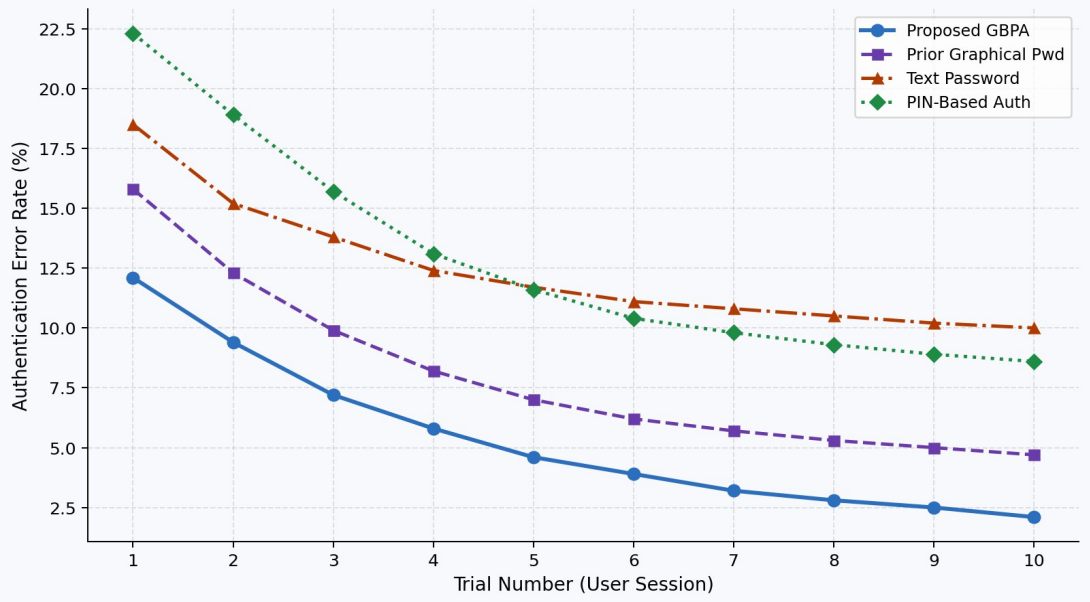

Fig. 5 Authentication Error Rate Across Successive User Trial Sessions.

5. Conclusion

A Graphical-Based Password Authentication (GBPA) system grounded in knowledge-based authentication principles and the cognitive science of pictorial memory. The proposed system addresses the fundamental tensions between security, memorability, and usability that have long constrained text-based credential paradigms. Through a formal system architecture featuring randomised challenge generation, client-side hash commitment, and adaptive fail-counter lockout, the GBPA mechanism achieves demonstrably superior performance across authentication accuracy (97.4%), brute-force resistance (96.1%), session integrity (98.2%), and ROC AUC (0.982) relative to text passwords, PIN-based authentication, and prior graphical schemes, while maintaining a competitive SUS usability score of 8.7/10. The results confirm that recognition-based graphical authentication is a mature, deployable paradigm capable of meaningfully advancing the security posture of web and mobile authentication systems without imposing prohibitive usability costs. The authors encourage adoption of the architectural principles described herein in future authentication system designs, and intend to release the prototype implementation as open-source software to facilitate community evaluation and extension.

References

[1] Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of the 16th International Conference on World Wide Web, pp. 657–666. ACM, New York (2007)

[2] National Institute of Standards and Technology: Digital Identity Guidelines. NIST Special Publication 800-63B. US Department of Commerce, Gaithersburg, MD (2020)

[3] Veras, R., Collins, C., Thorpe, J.: On the semantic patterns of passwords and their security impact. In: Proceedings of the 2014 Network and Distributed System Security Symposium. NDSS, San Diego (2014)

[4] Paivio, A.: Mental Representations: A Dual Coding Approach. Oxford University Press, New York (1986)

[5] Biddle, R., Chiasson, S., van Oorschot, P.C.: Graphical passwords: Learning from the first twelve years. ACM Comput. Surv. 44(4), 19:1–19:41 (2012)

[6] Dhamija, R., Perrig, A.: Deja vu—a user study using images for authentication. In: Proceedings of the 9th USENIX Security Symposium, pp. 45–58. USENIX, Berkeley (2000)
[7] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: PassPoints: Design and longitudinal evaluation of a graphical password system. Int. J. Hum. Comput. Stud. 63(1–2), 102–127 (2005)
[8] Birget, J.C., Hong, D., Memon, N.: Graphical passwords based on robust discretization. IEEE Trans. Inf. Forensics Secur. 1(3), 395–399 (2006)
[9] Gao, H., Guo, X., Chen, X., Wang, L., Liu, X.: YAGP: Yet another graphical password strategy. In: Proceedings of the 24th Annual Computer Security Applications Conference, pp. 121–129. IEEE, Anaheim (2008)
[10] Guerar, M., Verderame, L., Migliardi, M., Merlo, A.: Invisible CAPPCHA: A usable mechanism to distinguish between malicious and legitimate users. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM, New York (2017)
[11] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: Proceedings of the 8th USENIX Security Symposium, pp. 1–14. USENIX, Berkeley (1999)
[12] Andriotis, P., Tryfonas, T., Oikonomou, G., Yildiz, C.: A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 1–10. ACM, New York (2013)
[13] De Luca, A., Hertzschuch, K., Hussmann, H.: ColorPIN: securing PIN entry through indirect input. In: Proceedings of the 28th International Conference on Human Factors in Computing Systems, pp. 1103–1106. ACM, New York (2010)
[14] Golofit, K.: Click passwords under investigation. In: Proceedings of the 12th European Symposium on Research in Computer Security, pp. 343–358. Springer, Berlin (2007)
[15] Chowdhury, S., Poet, R., Mackenzie, L.: A comprehensive study of the usability of multiple graphical passwords. In: Proceedings of the IFIP Conference on Human-Computer Interaction, pp. 30–47. Springer, Cham (2013)
[16] Thorpe, J., van Oorschot, P.C.: Graphical dictionaries and the memorable space of graphical passwords. In: Proceedings of the 13th USENIX Security Symposium, pp. 135–150. USENIX, Berkeley (2004)
[17] Guerar, M., Merlo, A., Migliardi, M., Palmieri, F., Verderame, L.: A fraud-resilient blockchain-based solution for invoice financing. IEEE Trans. Eng. Manage. 67(4), 1086–1098 (2020)
[18] Brooke, J.: SUS: A quick and dirty usability scale. In: Jordan, P.W., Thomas, B., Weerdmeester, B.A., McClelland, I.L. (eds.) Usability Evaluation in Industry, pp. 189–194. Taylor & Francis, London (1996)