KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://karyailham.com.my/index.php/arca
2462-1927

Factors Affecting Users’ Quality of Experience (QoE) towards Graphical-based Authentication – A Systematic Literature Review

Juliana Mohamed[1,*], Mohd Farhan Mohd Fudzee[2], Noni Salzura Salim[3]

[1] Department of Information Technology, Centre for Diploma Studies (CeDS), Universiti Tun Hussein Onn Malaysia (UTHM), 84600 Pagoh, Johor, Malaysia
[2] Faculty of Computer Science and Information Technology (FSKTM), Universiti Tun Hussein Onn Malaysia (UTHM), 86400 Parit Raja, Batu Pahat, Johor, Malaysia
[3] Logistics Operation Distribution Centre, Telekom Malaysia (TM) Technology Sdn Bhd, Batu 10, 43200 Cheras, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 30 November 2025
Received in revised 14 January 2026
Accepted 15 January 2026
Available online 24 February 2026

Keywords:
Graphical-based authentication; Quality of Experience (QoE); usability; systematic literature review; PRISMA; authentication

ABSTRACT

Graphical-based authentication systems have emerged as promising alternatives to traditional text-based passwords since they enhance memorability and provide better protection against common cyber threats. Comprehensive research examining user perceptions when interacting with graphical-based authentication systems is limited. This paper conducts a systematic literature review (SLR) aimed at identifying the key factors influencing users' Quality of Experience (QoE) with graphical-based authentication. Following Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, the research analyzed 48 relevant studies published between 2010 and 2025 from reputable digital libraries. The results indicate that five key factors impacting QoE are usability, accessibility, memorability, visual design, and legibility. Furthermore, the review highlights an increasing need for authentication design that focuses on QoE, integrating subjective user preferences with objective usability metrics. The study concludes by offering insights into developing graphical-based authentication systems that adhere to user-centered principles, ultimately enhancing both security and user satisfaction.

1. Introduction

Authentication is central to digital security. Authentication refers to the process of effectively verifying an individual's or device's identification [1]. When using a bank card to make a purchase, we authenticate ourselves by having the card and knowing the Personal Identification Number (PIN) [2]. Since devices are used by so many people, authentication has become increasingly important. User authentication serves as the first line of defense against user impersonation, which is a serious security risk to any computer or device system [3]. The information needed to verify a user's identity can be divided into three categories: 1) knowledge-based, which includes PINs and passwords, 2)

[*] *Corresponding author.*
E-mail address: julianaju@uthm.edu.my

https://doi.org/10.37934/arca.42.1.7786

possession-based, which includes tokens and smart cards, and 3) inheritance-based, like biometrics, which use retinal scanning and fingerprints [2]. While alphanumeric passwords dominate, graphical-based authentication has gained attention for its potential to offer enhanced memorability and security.

Although traditional alphanumeric passwords have long been the most popular way to secure access to digital systems, issues with usability and memorability are raising doubts about their efficacy [4]. An alternative is the emergence of graphic-based authentication systems, which take advantage of the human brain's exceptional ability to interpret and remember visual information. Compared to text-based credentials, graphic-based authentication methods are more entertaining and frequently easier to remember because they incorporate visuals, patterns, drawings, or spatial memory into the authentication process [5]. Furthermore, graphic-based authentication is frequently praised for its resistance to prevalent threats like brute-force cracking and dictionary-based attacks [5]. Improved resistance to shoulder surfing is also demonstrated by certain implementations, particularly those that call for subtle or indirect graphical element selection. Because of these benefits, graphic-based authentication has become a desirable choice for improving user experience and security, especially in touchscreen and mobile settings [6].

User satisfaction and subjective experience are becoming increasingly important to the success of graphic-based authentication techniques, even if their technical robustness has been the main focus of research [5]. User-centered design (UCD) principles, which stress creating systems that are in line with users' demands, habits, and limits, are becoming more and more popular as a result of this. Quality of Experience (QoE) has become a complete and holistic metric within this paradigm, embracing usability, aesthetics, satisfaction, and real-world interaction situations [5]. QoE measures users' subjective impressions and emotional reactions during authentication activities, in contrast to typical usability metrics that only consider task efficiency or error rates. This is especially crucial for graphical-based schemes, where elements like environmental legibility, memorability, and visual design are critical [7,8]. For a variety of user demographics, including QoE into the design and assessment of graphic-based authentication systems guarantees that the authentication procedure is not only safe but also pleasurable, attainable, and long-lasting.

Although graphical-based authentication is becoming more popular, current research frequently prioritizes technical accuracy, algorithmic complexity, and security performance over the actual experience of the end-user [9]. Few studies attempt to assess more comprehensive experiential elements like cognitive load, ambient conditions, visual aesthetics, or long-term memorability, and those that do vary in their approach to usability [10]. A knowledge gap results from this incomplete assessment of how users really view and use graphical-based authentication systems in practical settings. Furthermore, the swift development of digital interfaces, particularly in mobile settings, necessitates a reexamination of authentication methods from a QoE perspective.

This systematic literature review (SLR) aims to fill this gap by thoroughly examining and compiling the main elements that affect user quality of experience (QoE) in graphical-based authentication systems. Following the principles of PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), this review offers a systematic summary of previous research, finds recurrent themes linked to quality of experience, and draws attention to important design factors and understudied aspects. In the end, this research attempts to direct the creation of authentication systems in the future that are not only safe and effective but also user-friendly, accessible, and emotionally fulfilling for a variety of user groups.

2. Literature Review

In the context of graphical-based authentication, however, nothing is known about the user's Quality of Experience (QoE), which is a comprehensive assessment of interaction. The various definitions of QoE that have been offered over the years somewhat reflect the fact that it remains at the intersection of multiple disciplines. QoE is defined as an application or service's overall acceptability as evaluated by the end-user [11]. These statements are accompanied by two statements that state that: 1) QoE comprises all end-to-end system effects, and 2) User expectations and context may determine overall acceptability [11]. Although it is evident that the ITU's definition emphasizes a service's acceptability, it ignores the user's actual experience. Furthermore, the intricate concepts of "user expectations" and "context" are not specified, and the potential impact of other human elements is disregarded.

QoE is a multidisciplinary concept that captures the general acceptability and satisfaction that a user has when engaging with a digital system, especially in dynamic or real-world settings. QoE goes beyond conventional usability measurements like task completion time, error rate, or efficiency in the context of Human-Computer Interaction (HCI) and User Experience (UX) studies [12]. QoE takes into account the emotional, environmental, and perceptual aspects that affect the user's subjective assessment of the system, whereas usability assesses how well a system helps users accomplish their objectives [13].

Although QoE has been used extensively in networked and multimedia applications (such as mobile apps and video streaming), its use in security systems, particularly graphical-based authentication, is becoming more apparent. QoE takes into account how users feel during the interaction, including whether they find the process interesting, cognitively manageable, aesthetically pleasing, and environmentally practical [13]. This is in contrast to usability, which can be objectively tested through performance challenges. Additionally, it takes into consideration contextual elements that are frequently disregarded in lab-based usability evaluations, such as screen glare, time constraints, and background distractions [14].

QoE becomes an important measure of practicality in graphical-based authentication systems, as users mainly depend on spatial patterns, visual memory, and interface aesthetics. Technically sound systems that are difficult to use in public, psychologically demanding, or visually occupied may not be trusted or adopted by users [5]. Therefore, approaching QoE from an HCI perspective facilitates a more sustainable and equitable authentication process by bridging the gap between technical security objectives and human-centered design principles [15].

There is still a large research gap that takes into account the subjective and contextual components of user experience, despite the fact that graphical-based authentication has been well studied in the fields of security algorithms and usability evaluation. While some previous studies stress usability by assessing task success rates, time to authenticate, and error frequency, many others concentrate on the technical performance of authentication schemes, such as computational efficiency, entropy levels, or resistance to brute-force attacks. These assessments, however, are frequently carried out in well regulated laboratory settings, which means they may not accurately represent the difficulties and limitations users encounter in actual settings [14].

In particular, little attention has been provided in authentication research to the environmental context, which includes elements like screen glare, lighting, mobility, and interactions in public spaces. These factors can have a big impact on how easily, safely, and effectively a user completes authentication tasks, particularly in situations when they are mobile or on the go. Subjective experiences like emotional fulfillment, perceived cognitive activity, and the authentication interface's aesthetics are also neglected [15]. These factors are included in QoE, which is becoming more widely acknowledged as a more comprehensive and user-centered paradigm for assessing the efficacy of systems.

The real experiences of end users and the design objectives of secure authentication systems get disconnected as a result of this neglect. Systems that are secure in principle run the danger of being rejected or poorly adopted in practice if they are not designed with user interaction with authentication interfaces in mind, taking into account varied contextual and emotional situations. Bridging this gap and guiding the creation of authentication solutions that are both technically sound and user-acceptable, hence requires a deeper examination of QoE aspects in graphical-based authentication research [16].

3. Research Objectives

By examining the quality of experience (QoE) elements documented in previous research, this systematic literature review aims to improve our understanding of how users interact with graphical-based authentication systems. As authentication techniques advance to become more interactive and graphic, it is more crucial than ever to look beyond performance measurements and consider the full user experience, which encompasses contextual, emotional, and cognitive aspects [17]. Through a methodical and thorough examination of the body of available literature, this review aims to close that gap.

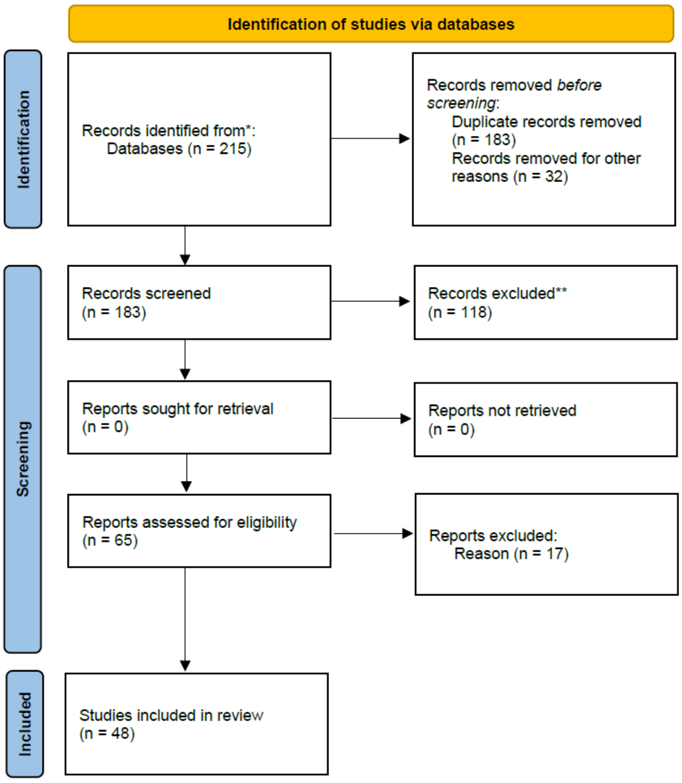
The research specifically aims to accomplish the following goals: 1) to identify and classify the primary factors that affect QoE in graphical authentication systems. In order to accomplish this, elements and aspects from empirical research, such as environmental legibility, cognitive load, visual design, usability, and memorability which must be extracted [19]. The study attempts to provide a taxonomy of QoE characteristics that are most discussed or ignored in literature by methodically arranging these factors, 2) to evaluate the degree to which user-centered criteria are incorporated into the assessment of graphical authentication systems in current studies. Numerous studies tend to ignore user subjective perceptions, such as perceived effort, emotional satisfaction, or comfort in various usage situations, in favor of concentrating primarily on objective usability outcomes or algorithmic strength [18]. Whether and how such experiential data is gathered, disseminated, and utilized to guide system design are assessed in this paper and 3) to highlight focus on crucial design implications, unrecognized problems, and potential avenues for further study in the creation of graphical authentication systems that are cognizant of QoE [20]. The review attempts to identify new issues by examining gaps and discrepancies in the literature. These include inadequate user segmentation (e.g., based on age, digital literacy, or accessibility needs), a lack of standard QoE evaluation frameworks, and a lack of real-world testing [21]. Future research and the creation of safe, context-aware, and user-centered authentication systems can both benefit from these ideas.

4. Methodology

In order to enhance the quality, transparency, and reproducibility of systematic reviews, this research study employs a set of evidence-based recommendations known as Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). The PRISMA framework makes sure the literature review adheres to a standardized, organized methodology. It is also appropriate for computer science and HCI research, particularly when examining trends, methodologies, or usability factors. It is frequently employed in the social and health sciences. PRISMA focuses on four key phases: 1. Identification, 2. Screening, 3. Eligibility and 4. Inclusion.

The research begins with the first step of identification by searching multiple digital databases (e.g., Scopus, IEEE Xplore, ACM, SpringerLink). This step recorded the number of records retrieved from each source. Some of the studies had duplicates removed before the screening process.

Fig. 1 illustrates the article selection process using the PRISMA 2020 flow diagram. A total of 215 records were identified through database searches. After removing duplicates and applying inclusion/exclusion criteria, 48 studies were included in the final review.


Identification of studies via databases
Identification
Records identified from*:
Databases (n = 215)
Records removed *before screening*:
Duplicate records removed (n = 183)
Records removed for other reasons (n = 32)
Screening
Records screened (n = 183)
Records excluded** (n = 118)
Reports sought for retrieval (n = 0)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 65)
Reports excluded:
Reason (n = 17)
Included
Studies included in review (n = 48)

*Consider, if feasible to do so, reporting the number of records identified from each database or register searched (rather than the total number across all databases/registers).

**If automation tools were used, indicate how many records were excluded by a human and how many were excluded by automation tools.

Fig. 1. PRISMA flow chart

Fig. 1 shows that there are about 183 records that have been duplicated. This number seems inconsistent, which likely reflects the total remaining after deduplication, rather than duplicating themselves. The records were removed for other reasons, discovered in 32 records. These may include papers not in English, irrelevant topics, or missing metadata.

In the second step of screening, the records were screened for about 183. After deduplication, the screening of 183 records by title and abstract was conducted to assess basic relevance. Records excluded 118. These were removed at this stage due to a lack of focus on graphical-based authentication, the absence of user experience elements, or non-peer-reviewed sources.

Moreover, the report was assessed for eligibility of 65, which retrieved the full text of 65 articles that passed the abstract screening. From this eligibility record, 17 reports were excluded. These full texts were removed for various reasons, such as focusing solely on algorithms, no empirical user evaluation, or lacking QoE-relevant data. There is no report sought/retrieved from this phase. This indicates that all potentially eligible reports were accessible online, and no additional retrieval was necessary.

The last step of Inclusion shows the studies included in the review of 48. These studies were analyzed to extract and categorize key QoE factors such as usability, memorability, visual design, cognitive load, and environmental legibility.

A thematic analysis method was used to determine the main Quality of Experience (QoE) elements that were covered in the included studies. One qualitative technique for finding, examining, and summarizing patterns or "themes" in data is thematic analysis. Through this procedure, this study was able to methodically identify and classify recurring components associated with the user experience in graphical-based authentication systems. Each publication was thoroughly examined to see if it addressed any areas of quality of experience (QoE), such as usability, memorability, visual design, cognitive effort, and environmental context, once the pool of 48 eligible papers was finalized.

Both deductive and inductive approaches were used to construct a coding framework. Informed by HCI and UX literature, including those found in ISO/IEC 9241-210 [16] and earlier QoE evaluation models in multimedia systems, deductive codes were developed based on predefined QoE parameters. Concurrently, inductive codes developed straight from the research itself, enabling the identification and inclusion of novel or surprising elements in the analysis, such as environmental legibility [22]. To increase reliability, two researchers independently coded each paper, and disagreements were settled by consensus and debate.

Five main themes emerged from the coded data: environmental legibility, cognitive load, visual design, usability, and memorability [23]. These themes were chosen because they were common and related to quality of experience (QoE), as evidenced by the qualitative and quantitative data from the reviewed research. The final themes were cross-referenced and verified against the study goals to make sure no important experiential component was missed.

3. Results and Analysis

The final synthesis includes 48 papers that satisfied the inclusion criteria out of the initial pool of 215 records found in major academic databases. These studies cover a wide range of research approaches, such as design case studies, survey-based user studies, usability testing, and experimental evaluations. The fact that most of the papers were released between 2014 and 2023 suggests that interest in graphical-based authentication systems and how they affect user experience has grown recently. Some research examined how users and current systems interacted in different scenarios, while others concentrated on creating innovative authentication mechanisms. The need for more thorough and consistent evaluation frameworks is highlighted by the fact that only a small percentage of publications explicitly measured Quality of Experience (QoE) as a formal notion. Table 1 summarizes the frequency and definition of five key QoE factors extracted through thematic analysis.

Table 1
QoE factors

QoE Factor	Frequency	Description
Usability	38	Ease of use, intuitiveness, and interaction flow
Memorability	34	Users' ability to recall graphical elements over time
Visual Design	29	Layout, color, clarity, and appeal of graphical interface
Cognitive Load	26	Mental effort required to perform authentication
Environmental Legibility	22	Impact of lighting, screen glare, and viewing angles in real-world scenarios

The most often discussed QoE element, usability, was found in 38 out of 48 investigations. Usefulness, system learnability, and overall interaction flow were the main criteria used by the majority of authors to evaluate usability. Task completion time, error rates, and evaluations of user satisfaction using Likert scales or System Usability Scale (SUS) scores were among the frequently employed metrics. Research has indicated that systems with user-friendly interfaces and low learning curves were more likely to be adopted by users and to achieve higher satisfaction ratings. Usability and interface simplicity were closely related; complicated navigation or crowded designs caused users to become confused and fail at their tasks. This highlights the significance of creating graphical-based authentication systems that are simple to use and require little effort from novice users.

There are thirty-four studies that found that memorability is essential to the long-term usage and efficacy of graphical-based authentication systems. Visual or spatial memory is frequently used in graphical-based authentication schemes, as contrast to text-based passwords, which depend on alphanumeric recall. Research has shown that graphical components that contain emotionally charged or significant content, such as landmarks or personal photos, significantly increase memory rates. But when consumers were subjected to a lot of cognitive strain or when the image space lacked uniqueness, memorability was frequently harmed. Some research used longitudinal assessments to measure recall over a period of days or weeks. The results showed that systems that used user-generated graphics or repetitive visual patterns were more memorable. Infrequently performed authentication procedures, such as logging into secure financial systems, require special consideration of this factor.

Users' opinions of a graphical-based authentication system are significantly influenced by visual design, according to 29 studies. This component includes clarity, color contrast, iconography, and spatial arrangement of graphical elements in addition to aesthetic appeal. According to studies, customers liked designs that were eye-catching but not too complicated. Cognitive confusion and lower usability scores resulted from inconsistent design patterns or inadequate contrast ratios. Furthermore, user engagement was guided by well-designed visual cues, which decreased errors and authentication time. The significance of contextual and culturally sensitive design was demonstrated by the generally higher ratings given to systems that included meaningful metaphors or imagery that was known to the user.

According to 26 studies, the idea of cognitive load refers to the amount of mental work needed to finish an authentication task. Overly complicated pictures, too many steps, or distractions in graphic-based authentication systems have been shown to raise cognitive load, especially for users with low levels of digital literacy. In addition to impairing usability, cognitive overload also has a detrimental effect on enjoyment and memorability. According to studies employing the NASA-TLX (Task Load Index) and post-task interviews, people felt that systems that required fine-grained remembering or attention-switching (such as choosing precise pixel locations) were cognitively taxing. The cognitive efficiency and usability of graphic-based authentication designs that facilitated chunking, progressive guidance, or iconic representations, on the other hand, were higher.

Environmental legibility is a less researched but more significant QoE element, as evidenced by 22 studies. This is a measure of a system's usability in real-world scenarios, including different light levels, screen reflections, device orientations, and even public interest. When authenticating while on the go, in bright outdoor settings, or when worried about shoulder surfing in public places, mobile users in particular encounter difficulties. Studies that replicated these circumstances discovered that precision-based input (such as dragging things), small icons, and low contrast graphics were far more difficult to utilize under uncontrolled settings. There is a need for further practical study in this field because environmental legibility is still underreported in the literature despite its influence on experience and security.

These five QoE dimensions' examination highlights how complex the user experience is in graphical-based authentication. Even if usability and memorability are the main factors in current evaluations, more comprehensive and balanced tests that incorporate visual design, cognitive ergonomics, and contextual legibility are desperately needed, especially as authentication interfaces become more widely used and mobile.

4. Discussions and Conclusion

A deeper comprehension of human-computer interaction (HCI) and cognitive psychology is shown in the prevalence of the five QoE elements that have been identified: usability, memorability, visual design, cognitive load, and environmental intelligibility. These elements are in line with fundamental concepts that describe how people view, engage with, and retain digital systems, such as Norman's Three Levels of Design (visceral, behavioral, and reflective). For instance, usability guarantees functionality and intuitive flow, which meets users' behavioral needs. The dual-coding theory, which highlights the human brain's superior capacity to retain visual information, lends credence to memorability. Cognitive load is related to the Cognitive Load Theory (CLT), which postulates that complicated or unfamiliar interfaces cause short-term memory to become overloaded, resulting in dissatisfaction and poor performance. Gestalt concepts, according to which users seek out logical, visually appealing patterns, are utilized in visual design. Environmental legibility, which acknowledges that user behavior is context-dependent and greatly influenced by surroundings, is the last concept that aligns with situated cognition. These theoretical connections support the importance of these elements in evaluating the actual user experience of graphical-based authentication.

Although graphical-based authentication research has traditionally placed a strong emphasis on usability, the results of this review reveal an imbalance in assessment procedures. The majority of research ignores more comprehensive experiential components in favor of performance-based usability indicators like task time, error rates, and perceived ease of use. Fewer studies examine contextual adaptation, perceived effort, or emotional satisfaction—all of which are essential for long-term user engagement. According to this inequity, graphical-based authentication systems are frequently designed for controlled environments rather than the unpredictability of real-world applications. For instance, memorability is occasionally assessed only right after use, ignoring its crucial function in long-term password recall. Furthermore, longitudinal studies that monitor changes in QoE over time or with repeated exposure are still uncommon. This emphasizes the necessity of moving away from discrete, brief usability tests and toward comprehensive, time-conscious, context-rich evaluations that closely resemble real-world user situations.

Among the five QoE dimensions identified, environmental legibility stands out as an emerging and underreported concern that is increasingly vital in today’s mobile-first landscape. Modern users frequently authenticate smartphones and tablets in dynamic, often public environments such as cafés, buses, or open offices. Under such conditions, external variables like screen glare, hand angle, lighting, and public visibility (shoulder surfing risk) dramatically affect the authentication experience. However, few studies rigorously simulate or measure these real-world variables, leading to a disconnect between lab-based evaluations and actual user needs. The neglect of environmental legibility poses significant implications—not only for QoE degradation but also for security vulnerabilities, as users may make hasty, unsafe choices to overcome visibility issues. This calls for a reframing of graphical-based authentication design, one that integrates environmental adaptability as a core usability criterion rather than a peripheral concern.

The results show a user-centric shift in authentication design, where experience metrics such as comfort, satisfaction, and ease of use are becoming critical. Most graphical-based authentication research prioritizes usability testing but lacks consistent frameworks for measuring QoE. Furthermore, environmental legibility is an emerging but underreported factor that directly impacts real-world performance and resistance to shoulder surfing.

This SLR highlights critical factors shaping the user's Quality of Experience in graphical-based authentication systems. As authentication continues to evolve, incorporating user preferences and real-world usability considerations will be vital. This review provides foundational insights for researchers and designers aiming to enhance both security and user satisfaction in future graphical-based authentication solutions.

Acknowledgement

The authors would like to thank the Center for Diploma Studies, Faculty of Computer Science and Information Technology, and Telekom Malaysia (TM) Technology Sdn Bhd for hardship and support in this research paper.

References

[1] Al Kabir, Mohammed Aziz, and Wael Elmedany. "An overview of the present and future of user authentication." In *2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pp. 10-17. IEEE, 2022. https://doi.org/10.1109/MENACOMM57252.2022.9998304

[2] Khan, Abdul Qadir. "Knowledge-based Systems for Cybersecurity in Internet of Things Environments." PhD diss., Sorbonne Université, 2024.

[3] Awan, Kamran Ahmad, Ikram Ud Din, Abeer Almogren, Neeraj Kumar, and Ahmad Almogren. "A taxonomy of multimedia-based graphical user authentication for green Internet of Things." *ACM Transactions on Internet Technology (TOIT)* 22, no. 2 (2021): 1-28. https://doi.org/10.1145/3433544

[4] Lapin, Kristina, and Manfredas Šiurkus. "Balancing usability and security of graphical passwords." In *Conference on Multimedia, Interaction, Design and Innovation*, pp. 153-160. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-031-11432-8_15

[5] Mohamed, Juliana. "Associating User's Preference and Satisfaction into Quality of Experience: A Shoulder-surfing Resistant Authentication Scheme by Visual Perception." *International Journal of Advanced Computer Science and Applications* (2022). https://doi.org/10.14569/IJACSA.2022.0131012

[6] Kamegne, Yvonne, Eric Owusu, and Joyram Chakraborty. "Usable Security: Cultural Impacts on Graphical Passwords Usability." In *Future of Information and Communication Conference*, pp. 10-20. Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-53960-2_2

[7] Laghari, Asif Ali, Xiaobo Zhang, Zaffar Ahmed Shaikh, Asiya Khan, Vania V. Estrela, and Saadat Izadi. "A review on quality of experience (QoE) in cloud computing." *Journal of Reliable Intelligent Environments* 10, no. 2 (2024): 107-121. https://doi.org/10.1007/s40860-023-00210-y

[8] Tangawar, Prajwal, Zeenat Shaikh, Dnyaneshwari Waghmare, Sakshi Randive, and Sujata Mali. "Survey paper on graphical password authentication system in terms of usability and security attribute." *Available at SSRN 4709737* (2024). https://doi.org/10.2139/ssrn.4709737

[9] Ologundudu, B. T., and B. A. Sakpere. "USABILITY STUDY ON TEXTUAL AND GRAPHICAL PASSWORDS." In *The Proceedings of the Nigerian Academy of Science*, vol. 14, no. 1, pp. 82-100. 2021. https://doi.org/10.1007/978-3-031-11432-8_15

[10] Kamegne, Yvonne, Eric Owusu, and Joyram Chakraborty. "Bridging the gap between usability and security: cultural adaptation of a graphical user authentication." In *International Conference on Human-Computer Interaction*, pp. 260-269. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-05028-2_17

[11] Yamazaki, Tatsuya. "Quality of experience (QoE) studies: Present state and future prospect." *IEICE Transactions on Communications* 104, no. 7 (2021): 716-724. https://doi.org/10.1587/transcom.2020CQI0003

[12] Kougioumtzidis, Georgios, Vladimir Poulkov, Zaharias D. Zaharis, and Pavlos I. Lazaridis. "A survey on multimedia services QoE assessment and machine learning-based prediction." *Ieee Access* 10 (2022): 19507-19538. https://doi.org/10.1109/ACCESS.2022.3149592

[13] Baraković, Sabina, Lea Skorin-Kapov, and Jasmina Baraković Husić. "The impact of QoE factors on the perception of constructs comprising information quality, usability, and aesthetics in mobile web browsing." *International*

Journal of Human–Computer Interaction 40, no. 22 (2024): 6996-7018. https://doi.org/10.1080/10447318.2023.2260982

[14] Mohamed, Juliana, Mohd Farhan Md Fudzee, and Muhamad Hanif Jofri. "Legibility Environment Factor for Shoulder-Surfing Resistant Authentication Scheme using Visual Perception of Graphical-based Authentication." *Journal of Advanced Research in Computing and Applications* 36, no. 1 (2024): 10-19. https://doi.org/10.37934/arca.36.1.1019

[15] Mohamed, Mona, Tobin Porterfield, and Joyram Chakraborty. "Cross-cultural effects on graphical password memorability and design." *Journal of Systems and Information Technology* 23, no. 1 (2021): 82-108. https://doi.org/10.1108/JSIT-06-2020-0105

[16] Mohamed, Juliana, Mohd Farhan Md Fudzee, Sofia Najwa Ramli, and Mohd Norasri Ismail. "Bridging Usability and Accessibility of User Authentication using Usable Accessed (UAce) for Online Payment Applications." *JOIV: International Journal on Informatics Visualization* 5, no. 4 (2021): 366-371. https://doi.org/10.30630/joiv.5.4.740

[17] Patil, Nikhil, Ganesh Bhutkar, Priyanshi Patil, Parth Pishte, and Apoorva Popalghat. "Graphical-based password authentication." In *International Conference on ICT for Sustainable Development*, pp. 411-419. Singapore: Springer Nature Singapore, 2023. https://doi.org/10.1007/978-981-99-6568-7_38

[18] Khedkar, Rutuja, Aditya Pawar, Krishna Dharmale, Nikhil Gaikwad, and Anushka Kangane. "A comprehensive survey of graphical passwords authentication systems that provides security." In *2024 International Conference on Expert Clouds and Applications (ICOECA)*, pp. 130-136. IEEE, 2024. https://doi.org/10.1109/ICOECA62351.2024.00036

[19] Mohamed, Mona, Joyram Chakraborty, and Sharma Pillutla. "Effects of culture on graphical password image selection and design." *Journal of Systems and Information Technology* 22, no. 1 (2020): 73-95. https://doi.org/10.1108/JSIT-08-2019-0157

[20] Naik, Sandhya Ramesh, Shettigar Sarvani Vasudeva, K. Shrilakshmi, and Vaishnavi Kothwal. "Advancements in user security: Enhancing usability with graphical password authentication." In *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, pp. 454-460. IEEE, 2024. https://doi.org/10.1109/IDCIoT59759.2024.10467993

[21] Fong, Jessica, and Ron Poet. "Creating graphical passwords on a mobile phone: graphical passwords on a mobile." In *13th International Conference on Security of Information and Networks*, pp. 1-6. 2020. https://doi.org/10.1145/3433174.3433608

[22] N. Li *et al.*, “Access control policy combining,” pp. 135–144, Jun. 2009. https://doi.org/10.1145/1542207.1542229

[23] Tangawar, Prajwal, Sakshi Randive, Zeenat Shaikh, and Dnyaneshwari Waghmare. "Graphical Password Authentication System In Terms of Usability and Security Attribute." *Available at SSRN 4804110* (2024). https://doi.org/10.2139/ssrn.4804110