Chapter 1

Evaluation of Authentication Schemes in Online Exams within the Framework of Information Security: CIA Triad[1]

Canan Yazıcı[2]

Şemseddin Gündüz[3]

Abstract

With the widespread adoption of distance education, online examinations have become a central component of assessment and evaluation processes in higher education. However, ensuring exam security in online environments poses significant challenges, particularly with regard to authentication processes. In this context, authentication schemes used in online exams need to be examined in line with fundamental information security principles.

This book chapter examines authentication schemes used in online examinations within the framework of information security and evaluates them based on the CIA Triad (confidentiality, integrity, and availability). Knowledge-based, possession-based, and biometric authentication schemes are discussed in the context of online exams, focusing on their implications for exam security, user experience, and the protection of personal data. In addition, thematic evaluations based on the perspectives of instructors and university students are used to highlight how these authentication schemes influence the reliability of online examinations.

The evaluations indicate that relying on a single authentication scheme may be insufficient to ensure secure online examinations. Accordingly, the chapter suggests adopting context-aware and multi-factor authentication approaches that holistically address the dimensions of the CIA Triad, taking into account the nature and risk level of the exam. Accordingly, the chapter aims to contribute to both theoretical and practical discussions on online exam security.

[1] This study was derived from the thesis prepared by the first author under the supervision of the second author and was conducted in accordance with research and publication ethics.

[2] Avrasya University, cananyazici5561@gmail.com, ORCID: 0000-0002-7236-5864

[3] Necmettin Erbakan University, semsedding@gmail.com, ORCID: 0000-0003-1075-0043

https://doi.org/10.58830/ozgur.pub1137.c4676

1. Introduction

The impact of digitalization on education has led to profound transformations not only in teaching and learning processes but also in assessment and evaluation practices. With the widespread adoption of distance education models, online examinations have become one of the most frequently used assessment tools in higher education. While these examinations offer significant advantages such as flexibility and independence from physical location, they also introduce various challenges related to exam security and the reliability of assessment outcomes.

One of the most fundamental challenges of online examinations is verifying whether the individual accessing the exam is indeed the authorized examinee. In traditional face-to-face examinations, identity verification is typically ensured through physical supervision; however, in online environments, this process must be carried out through technical systems. This necessity positions authentication schemes as a central component of online exam security. Inadequate authentication methods may enable fraudulent activities that compromise exam integrity and reduce the reliability of assessment results.

Evaluating authentication schemes solely from a technical security perspective is insufficient. Factors such as user experience, the protection of personal data, and ease of access to systems must also be taken into consideration. In this context, the CIA Triad (Confidentiality, Integrity, and Availability), which is widely recognized in the field of information security, provides a theoretical framework that enables the multidimensional evaluation of authentication schemes used in online examinations (Cochran, 2024). This framework is also regarded as a fundamental reference in information security education and practice (Whitman & Mattord, 2022).

Accordingly, the aim of this chapter is to examine authentication schemes used in online examinations within the framework of information security and to evaluate these schemes based on the CIA Triad. To this end, different authentication approaches are analyzed in the context of online examinations, and their strengths and limitations are discussed with respect to confidentiality, integrity, and availability. In doing so, the chapter seeks to contribute to the development of more balanced and sustainable approaches to online exam security.

2. Conceptual Framework

2.1. Online Examinations and Information Security

Online examinations are widely used in higher education as an integral component of distance education practices. While these examinations provide significant opportunities for measuring and evaluating student performance, they also introduce security requirements that differ from those of traditional examination environments. In online settings where physical supervision is limited or entirely absent, the secure administration of examinations largely depends on digital systems and the security mechanisms they provide. Whitman and Mattord (2022) emphasize that security in digital assessment environments should not be limited to technical measures alone but should be addressed through a holistic approach encompassing processes, policies, and human factors. Similarly, Peltier (2016) highlights that the sustainability of information security largely depends on the definition and implementation of policies and procedures at the institutional level.

In the context of online examination systems, information security extends beyond the protection of exam questions to include the comprehensive safeguarding of student identity information, exam responses, and assessment results. In this regard, NIST (2020) recommends adopting a risk-based approach to security and privacy controls in information systems, while ISO/IEC 27001:2022 emphasizes the operation of information security management system (ISMS) processes through the plan–do–check–act cycle. Consequently, online exam security represents a complex structure involving multiple components such as technical infrastructure, access control, data management, and user behavior. The sustainability of this structure depends on the effective implementation of institutionally defined security policies and procedures (Peltier, 2016).

2.2. Security Issues in Online Examinations

One of the primary security challenges encountered in online examinations is impersonation and unauthorized access. Situations in which an individual other than the enrolled student takes the exam, identity credentials are shared, or external interference occurs during the examination process directly threaten the reliability of assessment and evaluation outcomes. Such practices hinder the accurate reflection of actual student performance and undermine the principle of academic integrity.

In addition, data security constitutes another major area of concern in online examinations. Risks such as the unauthorized acquisition of exam questions prior to the exam, the alteration of student responses during or after the examination, and the manipulation of assessment results pose serious threats to system integrity. Furthermore, technical failures, connectivity issues, and system outages may negatively affect students' access to examinations, thereby complicating the fair and equitable conduct of the assessment process.

These security challenges necessitate the design of online examination systems that are not only functional but also reliable and sustainable. In this context, information security principles provide a systematic framework for addressing security-related issues in online examinations. Managing these risks requires the selection and implementation of security controls based on a risk-oriented approach (NIST, 2020).

2.3. Information Security as a Theoretical Framework: The CIA Triad

With the widespread adoption of information systems, the security of data produced, stored, and transmitted in digital environments has become a critical requirement at both individual and institutional levels. All information systems—including computer networks, software systems, cloud computing infrastructures, and online services—are responsible for protecting the data they contain against unauthorized access, unauthorized modification, and service disruptions. With the increasing prevalence of online examination practices in particular, the reliability and integrity of systems used in assessment and evaluation processes have gained even greater importance. In this context, authentication schemes employed to access online examinations must be examined in accordance with fundamental information security principles. From this perspective, the CIA Triad provides a functional framework for classifying security objectives across different digital ecosystems, such as IoT-based applications (Al Reshan, 2024).

One of the most widely accepted theoretical approaches in the field of information security is the CIA Triad—Confidentiality, Integrity, and Availability—which emphasizes that an information system can only be considered secure when these three principles are ensured simultaneously and in a balanced manner. Sağıroğlu and Canbek (2009) underline that confidentiality, integrity, and availability should be addressed collectively when evaluating information security processes. Similarly, TÜBİTAK BİLGEM (2017) highlights the importance of jointly considering these principles within the scope of information security management. Whitman and Mattord (2022) also emphasize that these principles are not independent of one another but must be maintained in equilibrium. Accordingly, the CIA Triad represents not only a technical security model but also a comprehensive paradigm used for developing security policies, identifying risks, and designing protective measures (Chowdhury et al., 2023). The violation of any one of these fundamental principles directly undermines both data security and the overall trustworthiness of the system.

Authentication schemes used in online examination systems are directly associated with each component of the CIA Triad and exert distinct effects on each dimension. The confidentiality dimension involves protecting students' personal and biometric data against unauthorized access; the integrity dimension concerns safeguarding the accuracy and reliability of the examination process and results; and the availability dimension ensures that students can access examinations in a timely, uninterrupted, and reliable manner. The balance established by authentication schemes among these three dimensions is regarded as a determining factor in the reliability, fairness, and sustainability of online examinations.

In this section, the CIA Triad is adopted as a theoretical foundation for evaluating the effects of authentication schemes used in online examinations on information security. Accordingly, different authentication approaches are examined from a holistic perspective based on the dimensions of confidentiality, integrity, and availability. This framework serves as a fundamental reference point for assessing security objectives in online examination systems (Cochran, 2024).

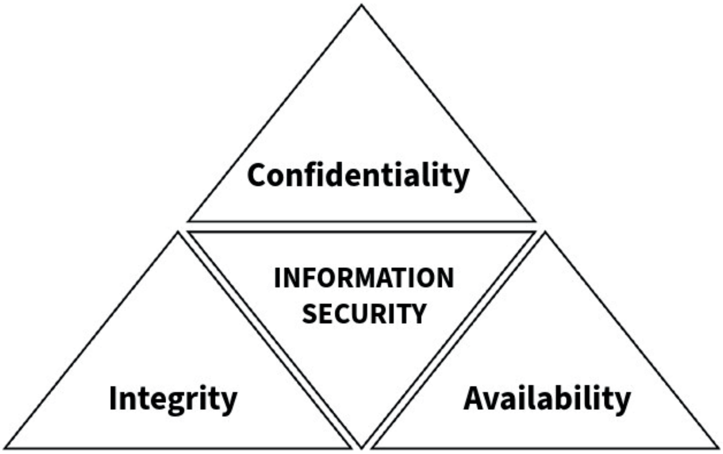

Figure 1. CIA Triad (Chopra & Chaudhary, 2020).

2.3.1. Confidentiality

Confidentiality is a fundamental principle of information security that ensures access to information is restricted exclusively to authorized individuals or systems (Özkan, 2016). This principle aims to protect sensitive information against risks such as unauthorized access, disclosure, or sharing. Violations of confidentiality may lead not only to the erosion of individual privacy but also to institutional reputation damage, legal sanctions, and the deterioration of trust relationships.

In the context of online examination systems, confidentiality encompasses the protection of students' personal information, identity data, examination questions, and exam responses from unauthorized access. Authentication schemes are regarded as the first line of defense in ensuring confidentiality. Failure to accurately verify whether a user accessing the system is indeed an authorized individual may result in violations of confidentiality and compromise overall exam security.

To safeguard confidentiality, mechanisms such as encryption and access control are widely employed (Stallings, 2023). However, particularly in cases involving the processing of user-specific data such as biometric information, confidentiality cannot be limited solely to restricting access. It must also be addressed through comprehensive policies governing the storage, processing, and secure disposal of personal data. Within this framework, confidentiality in online examination systems emerges as both a technical and an ethical responsibility.

2.3.2. Integrity

Integrity refers to the information security principle that ensures data is not altered, deleted, or manipulated by unauthorized parties (TÜBİTAK BİLGEM, 2017). This principle aims to preserve the accuracy, consistency, and reliability of information. Violations of data integrity directly undermine trust in system outputs and may lead to serious issues, particularly in assessment and evaluation processes.

In online examinations, integrity involves preventing the unauthorized acquisition of exam questions prior to the exam, protecting student responses from modification during or after the exam, and ensuring that assessment results are not manipulated. When authentication schemes are inadequate, situations such as impersonation or unauthorized intervention in the examination process become more likely. Such incidents pose direct threats to exam integrity and, consequently, to the validity of assessment outcomes.

Technical measures such as cryptographic hash functions, digital signatures, access authorization mechanisms, and logging systems are commonly used to ensure integrity (Stallings, 2023). In addition, multi-factor authentication approaches play a critical role in reducing risks related to impersonation and unauthorized access, thereby reinforcing the integrity principle. From this perspective, authentication is not merely a mechanism for controlling access but a core component that safeguards the reliability of the examination process.

2.3.3. Availability

Availability is an information security principle that ensures authorized users can access information and systems in a timely and uninterrupted manner whenever needed (ISO/IEC 27001:2022). Regardless of how secure a system may be, it cannot fulfill its intended function if authorized users are unable to access it. Therefore, availability constitutes a complementary dimension of information security alongside confidentiality and integrity.

In online examination systems, availability refers to students' ability to access the system smoothly throughout the exam period, the seamless operation of authentication processes without disrupting the exam flow, and the minimization of technical issues that could negatively affect exam performance. System outages, connectivity problems, or overly complex authentication procedures may weaken availability and adversely impact the overall examination experience.

To ensure availability, security solutions such as redundant systems, fault-tolerant infrastructures, and service continuity mechanisms are commonly implemented (ISO/IEC 27001:2022). However, excessively restrictive security measures may create tension between usability and security, potentially diminishing user experience. Consequently, the design of authentication schemes in online examination systems should adopt a balanced approach that carefully aligns security requirements with accessibility and ease of use.

3. Authentication Schemes in Online Examinations

The reliable administration of online examinations depends on the accurate and consistent verification of the identity of individuals accessing the exam. Accordingly, authentication schemes developed for this purpose have become one of the fundamental components of online examination systems. These schemes operate based on information known by the user, objects possessed by the user, or biometric characteristics, and they contribute to the conduct of the examination process in accordance with the principles of confidentiality, integrity, and availability.

In this section, authentication schemes commonly used in online examinations are classified and examined, and each type of scheme is evaluated within the context of online assessment.

3.1. Knowledge-Based Authentication Schemes

Knowledge-based authentication schemes rely on the verification of identity based on information that is assumed to be known only by the user. Common examples of this category include passwords, personal identification numbers (PINs), and one-time passwords (OTPs). In online examination systems, these schemes are frequently implemented in the form of system access through a username and password.

The primary advantages of knowledge-based authentication schemes lie in their ease of implementation and relatively low cost. From the users' perspective, such schemes require a comparatively low learning effort and do not necessitate additional hardware. However, these schemes exhibit several security vulnerabilities, as they may be shared, guessed, or compromised by malicious actors. In the context of online examinations, the sharing of authentication credentials or the compromise of passwords by third parties constitutes one of the main risks that directly threaten exam integrity. For these reasons, knowledge-based authentication schemes are generally considered insufficient to provide an adequate level of security for online examinations when used in isolation.

3.2. Possession-Based Authentication Schemes

Possession-based authentication schemes verify a user's identity based on a physical object that the user possesses. Examples of such schemes include smart cards, hardware tokens, and one-time verification codes sent to mobile devices. Two-factor authentication systems, which are commonly employed in online examinations, typically combine knowledge-based and possession-based schemes.

Compared to knowledge-based methods, possession-based authentication schemes offer a higher level of security. In particular, the transmission of one-time passwords via mobile devices reduces the likelihood of unauthorized access. However, these schemes may also introduce challenges when users are unable to access the required device. Situations such as the loss of a mobile device, depleted battery power, or technical malfunctions may hinder exam access and negatively affect availability. Therefore, possession-based authentication schemes in online examination systems should be designed in a manner that does not disrupt user experience or compromise the continuity of the examination process.

3.3. Biometric Authentication Schemes

Biometric authentication schemes verify user identity based on physical or behavioral characteristics. Methods such as fingerprint recognition, facial recognition, iris scanning, and voice recognition fall within this category. In online examinations, biometric schemes are regarded as a powerful tool for verifying whether the individual taking the exam is indeed the enrolled student.

The most significant advantage of biometric authentication schemes lies in their reliance on user-specific data that is difficult to replicate or forge. This characteristic substantially reduces the likelihood of fraudulent activities such as impersonation during the examination process. Nevertheless, the collection, storage, and processing of biometric data raise a range of ethical and legal concerns related to privacy, confidentiality, and the protection of personal data. Moreover, due to additional hardware requirements and the need for advanced technical infrastructure, biometric schemes may encounter challenges in ensuring uniform and seamless access for all users.

In this regard, the use of biometric authentication schemes in online examinations necessitates the adoption of a balanced approach that carefully weighs the security benefits they offer against requirements related to privacy protection and accessibility.

3.4. Comparative Evaluation of Authentication Schemes

Authentication schemes employed in online examinations differ in terms of the level of security they provide, user experience, and overall applicability. Knowledge-based schemes offer advantages in terms of accessibility and ease of use; however, they remain limited with respect to security. Possession-based schemes enhance security but may introduce technical and logistical challenges. Biometric schemes, while providing a robust level of security, require careful consideration due to concerns related to privacy, ethics, and data protection.

For these reasons, rather than relying on a single authentication scheme, the adoption of multi-factor authentication approaches tailored to the nature and risk level of the examination is recommended in online examination systems (Whitman & Mattord, 2022). Such integrated approaches not only strengthen exam security but also support a more balanced implementation aligned with fundamental information security principles.

Table 1. *Comparison of authentication schemes within the context of the CIA Triad*

Authentication Scheme	Confidentiality	Integrity	Availability
Knowledge-Based	Medium	Low	High
Possession-Based	Medium	Medium	Medium
Biometric	Low–Medium	High	Low–Medium
Multi-Factor Authentication	High	High	Medium

As presented in Table 1, authentication schemes differ considerably in terms of confidentiality, integrity, and availability within the CIA Triad framework. Knowledge-based authentication demonstrates high availability but relatively weaker integrity, whereas biometric authentication provides strong integrity assurances while introducing concerns related to confidentiality and accessibility. Overall, the comparison highlights that multi-factor authentication offers a more balanced approach by simultaneously strengthening multiple security dimensions, despite imposing moderate accessibility requirements.

4. Scope of the Study and Methodological Framework

The evaluations presented in this section are based on a qualitative research process aimed at exploring how authentication schemes used in online examinations are perceived within the context of information security and examining the types of impacts these schemes create across the dimensions of confidentiality, integrity, and availability. The methodological design of the study is structured within a qualitative research approach, which allows for an in-depth examination of a multidimensional and context-dependent phenomenon such as online examination security.

Within the scope of the research, the perspectives of two primary stakeholder groups who directly experience online examination practices were taken into consideration. These stakeholders consist of academic staff actively involved in distance education processes and university students participating in online examinations. The interactions of both groups with online examination systems play a decisive role in shaping their perceptions and expectations regarding authentication schemes (Hidayasari et al., 2025). Accordingly, the evaluations were conducted within a holistic framework that jointly considers the viewpoints of instructors and students.

Data were collected using the semi-structured interview technique, which enables participants to articulate their experiences, security perceptions, and potential concerns related to authentication schemes in their own words. Prior to the interviews, a brief informational session was conducted to establish a shared conceptual foundation among participants regarding the authentication schemes used in online examinations. This approach aimed to ensure that participants' evaluations were informed not only by individual experiences but also by a common analytical framework.

The collected data were thematically analysed using descriptive and content analysis techniques. During the analysis process, participants' views were examined within the framework of the core components of information security—confidentiality, integrity, and availability—and the effects of authentication schemes on these dimensions were interpreted through emergent themes. This approach allowed the findings to move beyond a purely descriptive level and to be interpreted in relation to the theoretical framework.

The methodological framework outlined in this section contributes to an understanding of the context and limitations within which the thematic evaluations presented in the subsequent sections are situated. In this way, readers are provided with the opportunity to assess the interpretations and conclusions regarding authentication schemes through the methodological foundation upon which the study is based.

5. Thematic Evaluation of the Findings

In this section, the findings obtained regarding authentication schemes used in online examinations are thematically evaluated within the framework of the core components of information security: confidentiality, integrity, and availability. The findings are derived from the experiences and perceptions of academic staff and university students and reveal the effects of authentication schemes on the security of online examinations. Rather than relying on quantitative measures, the evaluation focuses on shared themes and prominent viewpoints that emerged from participant narratives.

Table 2. Distribution of Participant Perspectives According to CIA Triad Themes

CIA Triad	Instructor Perspective	Student Perspective
Confidentiality	Biometric data perceived as risky	Concerns about data storage
Integrity	Impersonation as a major threat	Expectation of fair examinations
Availability	Technical disruptions as a problem	Complex authentication perceived as difficult

As shown in Table 2, instructors and students emphasize different concerns across the dimensions of the CIA Triad. While instructors primarily highlight risks related to biometric data and impersonation as threats to confidentiality and integrity, students focus more on data storage concerns and expectations of fairness in online examinations. In terms of availability, both groups draw attention to usability challenges, particularly those arising from technical disruptions and complex authentication procedures.

5.1. Findings Related to the Confidentiality Dimension

The findings related to the confidentiality dimension indicate that participants attach significant importance to the protection of personal information in online examinations. Both instructors and students emphasized that data used during the authentication process should be utilized solely for examination security purposes and should not be shared with third parties. In particular, evaluations of biometric authentication schemes reveal that although these systems are perceived as strong in terms of security, concerns regarding the storage and processing of biometric data are prominent.

Knowledge-based authentication schemes were considered preferable by some participants due to their reliance on less sensitive personal data. However, the shareable nature of such credentials was identified as a substantial risk that may lead to confidentiality breaches. Possession-based authentication schemes were perceived as offering a relatively balanced structure in terms of confidentiality; nevertheless, concerns regarding data security in mobile-device-based authentication processes were found to persist. Overall, these findings suggest that maintaining a delicate balance between authentication strength and personal data protection expectations is essential within the confidentiality dimension.

5.2. Findings Related to the Integrity Dimension

Findings related to the integrity dimension demonstrate that one of the primary expectations of participants in online examinations is the fair and reliable conduct of the examination process. Situations such as unauthorized individuals accessing the exam or impersonation—where one individual takes an exam on behalf of another—were identified as the most critical threats to exam integrity. In this context, authentication schemes were regarded as directly influencing the reliability of the assessment and evaluation process.

Biometric authentication schemes were perceived as the most robust methods in terms of maintaining integrity. Participants stated that techniques such as fingerprint recognition and facial recognition significantly reduce the likelihood of impersonation attempts. In contrast, the use of knowledge-based authentication schemes alone was considered insufficient to ensure exam integrity. A shared consensus emerged indicating that possession-based and multi-factor authentication approaches provide more reliable solutions for supporting the integrity of online examinations.

5.3. Findings Related to the Availability Dimension

Findings concerning the availability dimension highlight the critical relationship between security measures and user experience in online examinations. Participants emphasized that authentication processes should not prolong exam duration, cause technical disruptions, or impose excessive cognitive or operational burden on users. In this regard, knowledge-based authentication schemes were viewed as advantageous in terms of availability due to their ease of use and rapid access.

However, it was noted that certain biometric and possession-based schemes offering higher security levels may lead to accessibility challenges due to their technical infrastructure requirements. Factors such as internet connectivity, hardware compatibility, and device availability were identified as elements that could undermine the principle of equal access in online examinations. These findings indicate that accessibility must be considered a fundamental design criterion alongside security in the development of authentication schemes.

5.4. Overall Evaluation of the Findings

Overall, the findings reveal that participants' perceptions of authentication schemes reflect differing priorities across the dimensions of the CIA Triad. While biometric schemes were perceived as strong in terms of security and integrity, they also generated concerns related to confidentiality and availability. Conversely, knowledge-based schemes were regarded as advantageous in terms of accessibility but insufficient with respect to security and integrity. These results suggest that, rather than relying on a single authentication scheme, context-aware and multi-factor authentication approaches may offer more appropriate and balanced solutions for ensuring secure online examinations.

6. Discussion

The findings discussed in this section demonstrate that the CIA Triad—confidentiality, integrity, and availability—provides a functional and comprehensive framework for evaluating authentication schemes used in online examinations within the context of information security. The results indicate that the perceptions of instructors and university students regarding authentication schemes are shaped by the balance established among these three dimensions. This highlights the necessity of addressing online exam security not solely through technical safeguards, but also by incorporating user perceptions and experiences into the evaluation process.

Evaluations related to the confidentiality dimension are consistent with the privacy concerns frequently emphasized in the literature regarding biometric authentication systems. Previous studies have pointed out that although biometric data offer a high level of security, their irreversible nature may pose long-term risks for users. Similarly, the findings of the present study reveal that participants perceive biometric schemes as secure, yet express reservations regarding the storage and use of personal data. This indicates that confidentiality in online examinations should not be limited to access control mechanisms alone, but rather be addressed within a broader framework encompassing data management practices and ethical considerations.

Findings related to the integrity dimension support the view that authentication schemes play a decisive role in ensuring the reliability of online examinations. Issues such as impersonation and unauthorized access, which are widely identified in the literature as major challenges in online assessment environments, were also regarded by both instructors and students as primary threats to exam integrity in this study. In particular, the perceived effectiveness of biometric and multi-factor authentication approaches in mitigating such threats aligns with previous research. Nevertheless, it should be acknowledged that solutions focusing exclusively on enhancing security may negatively affect system sustainability if user experience is neglected.

With respect to availability, the findings point to a critical yet often overlooked aspect of online exam security that is closely linked to user experience. Participants' concerns regarding complex and multi-stage authentication processes potentially prolonging exam duration and adversely affecting performance correspond with the "security–usability trade-off" emphasized in the literature. The perceived advantage of knowledge-based authentication schemes in terms of accessibility helps explain their continued widespread use. However, if this advantage is not adequately balanced against their weaknesses in security and integrity, the overall reliability of online examinations may be compromised.

In this context, the discussion findings indicate that solutions relying on a single authentication scheme are insufficient for ensuring secure online examinations. When evaluated within the framework of the CIA Triad, it becomes evident that each authentication scheme exhibits strengths in certain dimensions while remaining limited in others. This underscores the importance of adopting context-aware and multi-factor authentication approaches in the design of online examination systems. Developing flexible and balanced authentication solutions that take into account the nature of the exam, the associated risk level, and the intended learning outcomes offers a more sustainable approach in line with fundamental information security principles.

7. Conclusion and Recommendations

In this chapter, authentication schemes used in online examinations were examined within the framework of information security, and the evaluations were conducted based on the CIA Triad (confidentiality, integrity, and availability). The review and thematic analyses demonstrate that online exam security cannot be ensured through single-dimensional technical solutions alone; rather, it represents a multidimensional structure that requires the integrated consideration of security, user experience, and ethical concerns.

The findings and discussions indicate that knowledge-based authentication schemes offer advantages in terms of availability; however, they exhibit significant limitations, particularly with respect to confidentiality and integrity. In contrast, biometric authentication schemes provide strong potential for preserving exam integrity and reducing fraudulent practices such as impersonation, yet they also give rise to user-centered concerns related to privacy and the protection of personal data. Possession-based and multi-factor authentication approaches, while capable of enhancing overall security levels, require careful design due to their technical infrastructure demands and potential implications for accessibility.

Within this context, it is recommended that the CIA Triad be adopted as a holistic guiding framework in the design of authentication processes for online examinations. Security measures that focus exclusively on ensuring exam integrity may negatively affect accessibility and user experience, thereby weakening system sustainability. Accordingly, the adoption of context-aware and multi-factor authentication solutions that can be adapted to the nature and risk level of the exam offers a more balanced approach to online exam security.

For practitioners and policymakers, the development of data management policies that prioritize user privacy is as critical as the implementation of technical security measures when determining authentication schemes for online examination systems. Universities and educational institutions should regard authentication processes not merely as technical requirements, but as integral components of the assessment and evaluation process, and should structure these processes in accordance with principles of transparency and user awareness.

In terms of future research, comparative studies examining the effects of authentication schemes across different disciplines and exam types would contribute to a more detailed understanding of how the CIA Triad is reflected in practice. Moreover, investigations into how users' privacy perceptions and security expectations evolve over time may facilitate the development of more inclusive and sustainable solutions for online examination security.

References

Al Reshan, M. S. (2024). IoT-based application of information security triad. *International Journal of Computer Science & Network Security*, 24, 85–92.

Chopra, A., & Chaudhary, M. (2020). *Implementing an information security management system*. Apress.

Chowdhury, M. M., Rifat, N., Ahsan, M., Latif, S., Gomes, R., & Rahman, M. S. (2023, May). ChatGPT: A threat against the CIA triad of cyber security. In *Proceedings of the 2023 IEEE International Conference on Electro Information Technology (eIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/eIT57321.2023.10187355

Cochran, K. A. (2024). The CIA triad: Safeguarding data in the digital realm. In *Cybersecurity essentials: Practical tools for today's digital defenders* (pp. 17–32). Apress.

Hidayasari, N., Kasmawi, K., Mansur, M., Husaini, M. I., & Nuranisa, P. (2025). Analysis of the application of CIA triad information security aspects in academic information systems. *ABEC Indonesia*, 562–567.

ISO/IEC. (2022). *ISO/IEC 27001:2022—Information security, cybersecurity and privacy protection: Information security management systems*. International Organization for Standardization.

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

Özkan, M., & Kara, A. (Eds.). (2016). *Bilgi güvenliği ve kriptoloji*. Nobel Akademik Yayıncılık.

Peltier, T. R. (2016). *Information security policies, procedures, and standards*. CRC Press.

Sağıroğlu, Ş., & Canbek, G. (2009). Bilgi güvenliği ve süreçleri. *Politeknik Dergisi*, 12(1), 21–30.

Stallings, W. (2023). *Cryptography and network security: Principles and practice* (9th ed.). Pearson.

TÜBİTAK BİLGEM. (2017). *Bilgi güvenliği ve bilgi güvenliği yönetim sistemi rehberi*. Ankara.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage.