

Comparative Review of Encryption, Authentication, Blockchain and Optical Approaches to Examination Security

Dishant Nitin Chaudhari^{#1}

Hitesh Nilesh Mahajan^{#2}

Sharvari Sandeep Gosavi^{#3}

Drushna Shantanu Sarode^{#4}

Prof.Kiran Borade^{#5}

¹²³⁴*Diploma Student, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India*

⁵*Lecturer, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India*

[¹dishant.chaudhari.work@gmail.com

²hiteshnm2008@gmail.com

³sharvarigosavi18@gmail.com]

Abstract— Examinations are high-stakes assessments, and their credibility depends on keeping questions confidential, verifying the identity of candidates, and protecting the integrity of examination results. This review compares three recent studies that address examination security from different perspectives. The first study uses a questionnaire survey and literature review to examine encryption and authentication practices in Jordanian universities. The second presents a blockchain and smart contract prototype designed to improve the security of online examinations. The third investigates an optical examination paper designed to reduce the possibility of lateral viewing during paperbased tests. These studies were selected by the author; therefore, this review represents a comparative analysis of a small set of studies rather than a systematic literature review. Each study was examined based on its security focus, methodology, evidence, reported findings, and limitations. The numerical results reported in the experimental study were also recalculated using the published values. Looking at the results as a whole, the findings indicate that the practices reported in the survey rely heavily on password-based authentication and the use of unencrypted question banks. The blockchain-based approach provides tamperevident storage of examination results, but it does not provide quantitative evaluation or address candidate impersonation. The optical examination paper reports statistically significant effects, although the study uses relatively small samples and contains some inconsistencies in its reported numerical results. The review identifies several important research gaps, including the lack of clear threat models, limited evaluation of cost and processing time, potential privacy concerns related to blockchain records, limited consideration of cheating assisted by generative artificial intelligence, and the absence of a common benchmark for comparing security solutions. Based on these findings, five possible research directions are suggested, along with a conceptual layered framework for improving examination security.

Keywords—examination security; online examination; encryption; biometric authentication; blockchain; smart contract; academic integrity; literature review

I. INTRODUCTION

Examinations are important for assessing learning and making decisions about student progression and certification. Their reliability depends on protecting examination questions, verifying candidate identities, securing results, and maintaining fair examination conditions. The shift to online examinations, especially during the COVID-19 pandemic, improved efficiency but also increased risks such as question leakage, cheating, fraud, and hacking [1]. Paper-based examinations also face security issues, including unauthorized viewing of nearby candidates' answer sheets [2].

Existing research uses different approaches to address these risks. Encryption and authentication protect examination content and candidate identities [1], while blockchain and smart contracts aim to prevent unauthorized changes to examination records [3]. Optical techniques have also been proposed to reduce the visibility of answer sheets to nearby candidates [2]. At the same time, these methods are usually evaluated separately, making it difficult to identify the weaknesses that remain after each method is applied.

The three studies reviewed here represent these different approaches. One survey of 30 universities in Jordan found widespread use of unencrypted question banks and password-based authentication [1]. Another developed an Ethereum-based smart contract for recording examination results [3]. A third study tested an optical examination paper with 60 undergraduate students to reduce unauthorized viewing [2]. Since the studies address different threats and use different methods and evidence, their security performance cannot be directly compared.

A comparative review is therefore needed to place the approaches in one frame, to check what the reported evidence can support, and to identify what none of them addresses. The review is deliberately narrow: it analyzes three studies selected by the author, and its conclusions are indicative rather than exhaustive. The contributions are:

- a taxonomy of the reviewed approaches by locus of protection (Fig. 2 and Table I);
- a structured comparison of objectives, methods, evidence and limitations (Table II);
- a recomputation of the test statistics reported in [2] from its published values and a re-plot of the survey counts in [1] (Table III and Fig. 3);
- a separation of gaps stated by the original authors from gaps derived by comparison (Table IV);
- five research directions and a conceptual layered framework (Table V and Fig. 4).

II. REVIEW SCOPE AND METHOD

The review includes three papers selected by the author: [1], [2], and [3]. No database search, screening process, or qualityscoring method was used; therefore, this work is a purposive comparative synthesis rather than a systematic review. The overall workflow is presented in Fig. 1.

For each of the three selected research papers, a detailed comparative analysis was conducted by examining the problem addressed, research objectives, methodology, tools and technologies used, data sources, reported results, strengths, limitations, and suggested future work. The main aim was to understand how each study approaches examination security, what type of protection it provides, and how effectively its proposed methods address the identified security challenges. The studies were compared based on their security focus, type and quality of evidence, research methods, and reported performance. Particular attention was given to encryption and authentication practices in universities [1], the effectiveness of optical examination paper in reducing unauthorized viewing [2], and the use of blockchain and smart contracts to improve the integrity and transparency of examination records [3]. Since the studies address different aspects of examination security and use different research methods, their findings were interpreted according to their respective objectives and evaluation conditions rather than treating them as directly equivalent approaches. Numerical results were compared only when the experimental conditions and available data were suitable for meaningful interpretation. Where sufficient information was available, statistical results were independently recalculated using open-source software to examine their consistency with the published values. These recalculations were based on the numerical information and assumptions provided in the original studies, and no unsupported comparisons were made when the available data were insufficient. The analysis also considered practical factors

such as examination content confidentiality, candidate identity verification, result integrity, prevention of visual cheating, implementation complexity, privacy, accessibility, and reliability of evaluation. In addition, attention was given to whether the proposed approaches were tested under realistic conditions and whether the reported evidence adequately supported the authors' conclusions. Systems and techniques discussed within study [1] were treated as findings reported by that study and were not independently analyzed as separate research papers. This approach helped maintain a clear distinction between primary research and information reported through the reviewed study. Throughout the paper, the phrase "reported by the authors" refers to findings, claims, or limitations explicitly stated in the original studies, whereas "comparative analysis suggests" indicates interpretations, observations, and research gaps identified through the comparison conducted in this review. Maintaining this distinction improves transparency, supports a more reliable interpretation of the available evidence, and helps identify areas where existing examination security approaches require further investigation and improvement.

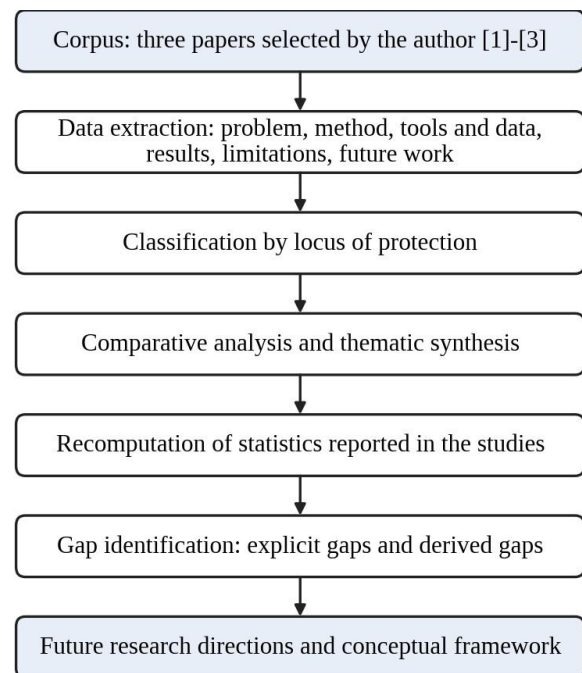


Fig. 1. Review workflow followed in this paper (original figure).

III. TAXONOMY AND SUMMARY OF THE REVIEWED STUDIES

The reviewed studies address four main protection areas (Fig. 2): examination content confidentiality, candidate identity, record integrity and auditability, and examination environment control. These areas correspond to the threats discussed in the

studies, including question leakage and fraud [1], record manipulation and transparency issues [3], and visual cheating [2]. Comparative analysis suggests that no study covers more than two protection areas, and none provides a clear threat model describing the possible capabilities of an attacker.

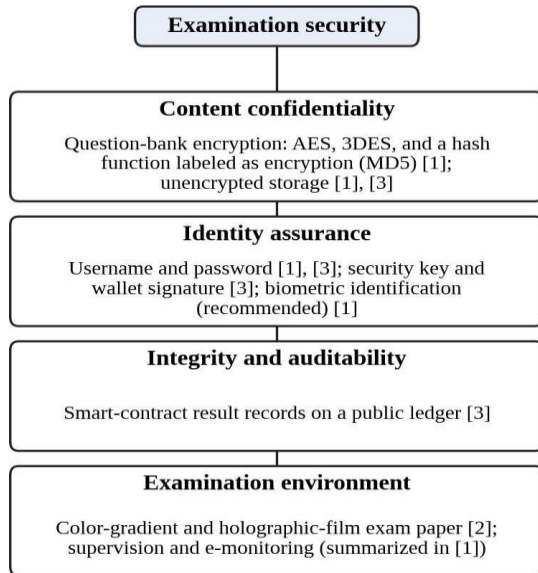


Fig. 2. Taxonomy of the examination security approaches in the reviewed studies, by locus of protection (original figure; sources in brackets).

Table I summarizes the studies. Study [1] is the only one that observes current practice, [2] is the only controlled experiment, and [3] is the only implementation that publishes source code. Their evidence is therefore of different kinds, which shapes the comparison in Section V.

TABLE I. SUMMARY OF THE REVIEWED STUDIES

Study	Objective	Method	Data and tools	Evaluation	Key findings
[1]	Assess encryption and authentication practice in online examination systems and recommend safeguards	Literature review (ten systems compared in a table) and questionnaire sent to all 30 public and private universities in Jordan	Questionnaire responses from 30 institutions; no software artifact	Counts and percentages (descriptive)	28 of 30 host the system inhouse; 10 of 30 encrypt the question bank; 28 of 30 use passwords only and 2 add biometrics
[2]	Reduce visual cheating in paper-based examinations while keeping the paper readable and comfortable	Randomized two-group experiment (30 and 30 undergraduates); observation checklist used by two observers; 16-item Likert questionnaire	Examination paper with color-gradient margins and holographic reflective film (FSC-certified 120 gsm stock) versus standard white paper	Independent-samples t-tests, chi-square tests, Cohen's d, Cronbach's alpha (0.87 overall)	Higher mean ratings in the experimental group on four variables; side-viewing attempts 4 versus 15; repeated peripheral observation 3 versus 12
[3]	Provide a tamper-evident, transparent online examination that needs no physical test center or invigilator	Prototype design and implementation, demonstrated in a simulated test session	Ethereum, Solidity, Remix IDE, MetaMask, web3.js, PHP, MySQL	None quantitative; interface screenshots and contract listing	Working prototype records student identifier, exam identifier, score, result hash and timestamp in a smart contract

IV. THEMATIC SYNTHESIS

A. Confidentiality of Examination Content

The survey in [1] shows that examination confidentiality is poorly protected in the sampled institutions. Of the 30 universities, 28 (93.3%) host their examination systems in-house, while only 10 (33.3%) encrypt their question banks and 20 (66.7%) keep them unencrypted [1] (Fig. 3). Among the institutions using encryption, AES is reported as the most common method, followed by MD5 and 3DES. Three respondents were also unaware of the encryption method being used [1].

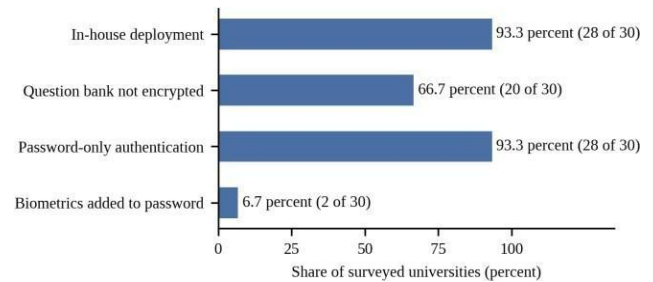


Fig. 3. Share of the 30 surveyed Jordanian universities reporting each practice (counts from [1], re-plotted by the author).

Fig. 4. The classification of MD5 as a question-bank encryption method should be treated with caution. MD5 is a one-way hash function, not a reversible encryption method, so it cannot protect content that must later be decrypted for use. Study [1] also describes MD5 as irreversible hashing and labels it as “MDF” in the survey figure. Comparative analysis suggests This means that either respondents were reporting passwordhashing practices or the survey category mixes hashing with encryption. Because of this, the actual proportion of institutions using effective question-bank encryption may be lower than one third.

The study records algorithm names but does not examine key management, encryption during transmission, or insider access. These factors are important for preventing leakage in systems hosted in-house. A similar gap appears in [3], which uses PHP

and MySQL for storing examination and user data without describing encryption. In [2], protection is limited to the examination environment during actual use.

B. Identity Assurance

Authentication in the surveyed institutions is mainly password-based: 28 of 30 use only usernames and passwords, while two (6.7%) combine passwords with biometrics [1]. The authors recommend biometric identification, but also note limitations such as sensitivity to lighting and expression in face recognition, background noise in voice recognition, and higher costs [1]. Since no false-acceptance or false-rejection rates are reported, the recommendation remains qualitative.

The prototype in [3] uses login credentials and security keys, with a MetaMask-signed transaction required during submission. At the same time, a signed transaction confirms control of a wallet rather than the identity of the student, and

implementation. Fourth, exam and user data are still stored in a centralized database, making the system hybrid rather than fully decentralized. Finally, [3] reports no gas cost, transaction latency, or throughput, which are important for assessing the feasibility of blockchain-based examinations.

The author acknowledges only that the approach demands technical knowledge and that the MetaMask wallet may be difficult for some users [3].

C. Prevention of In-Room Cheating

The optical paper in [2] is the only reviewed intervention tested through a randomized comparison. Sixty undergraduates were divided into two equal groups, with two observers recording side-viewing attempts. Participants rated readability, comfort, perceived security, and satisfaction on a five-point scale, with an overall Cronbach's alpha of 0.87. The experimental group scored higher on all four measures, including perceived

Study	Locus and approach	Sample or dataset	Reported performance	Strengths	Limitations
[1]	Content and identity; survey of current practice	30 universities in one country	Adoption shares only; no security performance measure	Coverage of the whole national sector as stated (30 of 30 institutions); observation of practice; comparison of ten prior systems	Instrument validation, respondent roles and response process not reported; MD5 counted as encryption; no key-management items; recommendations not tested
[2]	Environment; passive optical design for paperbased tests	60 undergraduates, 30 per group	Perceived security 4.68 versus 2.95 (five-point scale); sideviewing attempts 4 versus 15	Randomized allocation; control group; several measures; effect sizes reported	Small single-context sample; short-term; observers not blind; statistics not reproducible from published values (Table III); sustainability not measured; visual impairment excluded
[3]	Integrity and login; smartcontract result records	None; simulated session	None reported (no cost, latency or throughput)	Working code and interface; end-to-end flow shown; tamper-evident record concept	No evaluation; no access control in the listed contract; public score storage; wallet not bound to student; function name mismatch; centralized database retained

[3] does not explain how the wallet is linked to a registered candidate. Comparative analysis suggests that the prototype may still be vulnerable to impersonation, particularly because it removes the additional human verification provided by invigilators.

B. Integrity and Auditability

The design in [3] stores each exam submission in a smart contract, including the student ID, exam ID, score, result hash, and timestamp. Since deployed contracts cannot normally be changed, the authors argue that this provides transparency and tamper evidence. At the same time, several limitations reduce its practical value.

First, immutability starts only after submission, so it does not ensure that the score was calculated correctly or by an authorized person. Second, the contract code does not clearly restrict access to the record-writing function, while the public records mapping could expose all scores. Third, the client code calls `submitResult`, which is not present in the published contract, raising doubts about the completeness of the

security (4.68 vs. 2.95), and had fewer side-viewing attempts (4 vs. 15) [2]. These findings support the idea that the optical layer can reduce lateral viewing, although the study's design limits how widely the results can be generalized.

The treated paper is visibly different from standard paper, so observers could not be fully blinded to the condition; the single-blind procedure in [2] refers to participants' awareness of the study purpose. The study measured suspicious behavior rather than confirmed cheating, and no exam scores were reported. Perceived security was also self-reported by students using the treated paper, so it may partly reflect awareness of the treatment. Students with diagnosed visual impairments were excluded [2], leaving accessibility of the reflective gradient surface untested. Finally, the sustainability claims in [2] are

TABLE II. COMPARATIVE ANALYSIS OF THE REVIEWED STUDIES

shown through a proportional chart rather than measurements from the study, so they should be viewed as design intentions rather than demonstrated results.

V. COMPARATIVE AND QUANTITATIVE ANALYSIS

Table II compares the studies by approach, sample, reported performance, strengths, and limitations. All three highlight gaps in conventional examination controls. Studies [1] and [2] identify password-only access, invigilation, and surveillance as insufficient, while [3] presents reducing physical centers and invigilators as a cost advantage. At the same time, their approaches differ. Study [3] uses blockchain to reduce the need for invigilators, whereas [1] identifies impersonation and fraud

therefore cannot be directly applied to the digital settings of [1] and [3].

Looking at the results as a whole, the studies show a step-bystep progression. Plaintext question banks expose exam content [1], while encryption addresses storage but not key management. Password-only login provides weak identity protection, while biometrics improve verification but introduce cost and environmental limitations [1]. Blockchain improves result integrity [3] but does not solve identity binding, privacy, or cost issues. Similarly, the optical paper reduces in-room viewing [2]

TABLE III. STATISTICS REPORTED IN [2] COMPARED WITH VALUES RECOMPUTED IN THIS REVIEW

Quantity	Reported in [2]	Recomputed here	Comment
Perceived security, t and d	t = 5.12; d = 1.14	d = 3.53; t = 13.67	Means 4.68 and 2.95; single SD 0.49; n = 30 per group
Readability, t and d	t = 3.89; d = 0.82	d = 1.22; t = 4.74	Means 4.42 and 3.71; SD 0.58
Visual comfort, t	t = 3.11	t = 5.33	Means 4.36 and 3.52; SD 0.61
User satisfaction, t	t = 2.94	t = 6.61	Means 4.51 and 3.40; SD 0.65
p-values for the reported t (df = 58)	0.001; 0.003; below 0.001; 0.005	0.0003; 0.003; below 0.001; 0.005	Reported p for t = 3.89 is conservative
Side-viewing attempts, chisquare	8.34 (p = 0.004)	9.32 uncorrected (p = 0.0023); 7.70 with Yates correction (p = 0.0055); Fisher exact p = 0.0048	Counts 4 and 15, assumed to be participants out of 30 per group
Repeated peripheral observation, chi-square	7.92 (p = 0.005)	7.20 uncorrected (p = 0.0073); 5.69 with Yates correction (p = 0.0171); Fisher exact p = 0.0153	Counts 3 and 12, same assumption
Group means, Table 1 versus Fig. 3	Table 1 control: 3.71, 3.52, 2.95, 3.40; experimental: 4.42, 4.36, 4.68, 4.51	Fig. 3 (read from the chart) control: about 3.21, 2.87, 2.76, 3.05; experimental: about 4.42, 4.18, 4.61, 4.33	Order: readability, visual comfort, perceived security, satisfaction

a.

Recomputed by the author of this review with open-source numerical software. The published tables do not state whether the standard deviation is pooled, so the recomputed values are indicative.

as major online-exam threats and recommends stronger identity verification, which [3] does not provide. The optical paper in [2] addresses visual cheating in paper-based exams and

but does not address collusion or external assistance in digital exams. Thus, each approach addresses one security gap while leaving others unresolved.

ty, Table 1 of [2] implies a Cohen's d of 3.53 against 1.14 re-

Only [1] and [2] report numbers, and the numbers are not commensurable: [1] reports counts of institutions from a questionnaire (n = 30), [2] reports inferential statistics on 60 participants, and [3] reports no quantitative result. No accuracy, detection rate, latency, cost or false-rejection value is reported by any study, so a ranking by performance would be unjustified. The one quantitative comparison that can be made is internal, and Table III compares the statistics reported in [2] with values recomputed from its published means, standard deviation and counts.

Assuming 30 participants per group and that the single standard deviation column applies to both groups, the recom-

puted statistics and effect sizes are larger than the reported ones and cannot be reconciled with them; for perceived securiported. The control-group bars in Fig. 3 of [2] also differ from its Table 1. The chi-square values reported for observed behaviors differ modestly from those computed from the counts, and Fisher's exact test on the same counts still gives p below 0.05 (0.0048 and 0.0153), so the direction of that finding is robust while the reported statistics are not exactly reproducible. These discrepancies do not show that the intervention is ineffective. They show that the numerical record in [2] cannot be audited from the paper alone, and that the raw data should be shared.

on visual cheating, while factors such as lighting, seating, and reflections may affect the results. It also examined only shortterm effects and suggested improving the material with holographic layers. Study [3] acknowledges that its system requires knowledge of blockchain, smart contracts, and web development, while MetaMask may be difficult for some users. Study [1] reports that Jordanian institutions lack adequate security measures and procedural standards; however, the

VI. RESEARCH GAPS

A. Gaps Reported by the Authors

The authors of [2] note that the sample was small and limited to a specific higher-education setting. The study focused only

provided text does not include a section on its own limitations or future work.

B. Gaps Derived from the Comparison

The comparative analysis identifies eight additional gaps not clearly addressed by the original authors. (1) No study defines

report instrument validation, respondent roles, or the response process. (3) Cost, latency, and scalability are not evaluated. (4) Privacy and data protection are also overlooked, despite [3] storing records on a public ledger and [1] recommending biometric identification. Blockchain-based exams do not address identity binding.

(5) None considers generative AI-assisted answering as a threat; [1] discusses AI only for proctoring. (7) Accessibility and fairness are overlooked: [2] excludes

TABLE IV. RESEARCH GAP ANALYSIS

Existing approach	Limitation	Evidence	Type	Research gap	Potential solution
Unencrypted or loosely specified question banks [1]	Encryption reported by one third of institutions; MD5 counted as encryption; key management not surveyed	10 of 30 encrypt; survey figure and comparison table of [1]	Derived	Whether reported encryption actually prevents leakage is unknown	Authenticated encryption with audited key management; follow-up survey with a validated instrument
Password-only authentication [1], [3]	Knowledge-based login is weak against impersonation; alternatives not quantified	28 of 30 in [1]; login design of [3]	Explicit in [1]; derived for [3]	No identity-bound authentication with reported error rates and cost	Biometric or multi-factor login evaluated with false acceptance and rejection rates

a specific adversary, making it difficult to assess protection against threats such as database insiders, impersonating candidates, or outside assistance. (2) The evidence is limited or difficult to verify: [3] provides no measurements, [2] has a small sample and numerical inconsistencies, and [1] does not

visually impaired candidates, while [1] does not assess lighting effects across groups. (8) There is no common benchmark or reporting standard, and no study provides data or code for reproducibility. Table IV links these gaps to evidence and possible solutions.

Existing approach	Limitation	Evidence	Type	Research gap	Potential solution
Blockchain result storage [3]	Integrity only after submission; no access control in listing; public scores; no cost data	Text and code listing of [3]	Derived	Privacy, identity binding and scalability unmeasured	Hash-anchored records, access-controlled contract, test-network benchmarking
Optical examination paper [2]	Small single-context sample; short-term; inconsistent statistics; observers not blind	Limitations stated in [2]; Table III	Explicit and derived	No replication, blinded outcome assessment or accessibility testing	Multi-site randomized trial with blinded video coding and open data
Sustainability claim of [2]	Percentages in the impact chart not derived from reported measurements	Fig. 5 of [2]	Derived	No measured life cycle assessment	Life cycle assessment of material, energy and reprinting
All approaches [1]–[3]	No threat model, no common metrics, no treatment of generative AI assistance	Absence in the three texts	Derived	No cross-layer evaluation	Threat-model-driven benchmark for digital and paper-based settings

VII. FUTURE RESEARCH DIRECTIONS

Five directions follow from the gaps in Table IV and are summarized in Table V. They are described as underexplored opportunities; their novelty has not been checked against the wider literature, which a three-study review cannot cover. Methodological improvements common to all five are explicit threat models, preregistered protocols, blinded outcome assessment where the intervention is visible, standardized reporting of error rates, cost and latency, and open data and code.

TABLE V. FUTURE RESEARCH DIRECTIONS

Direction	Gap and evidence	Proposed method	Data and evaluation	Expected contribution
1. Threat-model-driven benchmark for examination security	No adversary definition or shared metrics across [1]–[3]	Define adversary classes (insider, impersonator, colluder, Allassisted candidate); build scenario suites for digital and paper-based settings	Simulated sessions with red-team attacks; attack success rate, detection rate, false rejection, latency, cost	Comparable evidence across protection layers
2. Privacy-preserving ledger anchoring with identity binding	Public scores, unrestricted writing in the listing, wallet not bound to student [3]	Store salted hash commitments only; role-restricted contract; credential-bound wallets	Test-network deployment with synthetic records; gas cost, confirmation time, throughput; access-control attack tests	Feasible and privacy-aware tamper evidence
3. Biometric and multifactor authentication with reported error rates and fairness	Password-only login at 28 of 30 institutions; cost and sensitivity to lighting named but not quantified [1]	Face or fingerprint verification with liveness detection plus a second factor; template protection	Public biometric benchmarks and a consented pilot; false acceptance and rejection by lighting and subgroup; usability and cost	Quantified trade-off for institutions
4. Auditable encrypted question banks with key management	20 of 30 unencrypted; algorithm named but key handling not surveyed [1]	Authenticated encryption with envelope keys, role-based access and access logging; validated multi-institution questionnaire	Overhead and leak-simulation tests; reported response rate and respondent roles	Evidence on whether encryption prevents inhouse leakage
5. Replicated, blinded evaluation of passive optical papers with life cycle assessment	Small sample, inconsistent statistics, unmeasured sustainability [2]	Multi-site randomized trial; independent blinded video coders; accessibility testing; open data	Larger samples with confidence intervals; copying measured where permitted; measured material and energy use	Reliable effect size and verified sustainability claims

Fig. 4 combines the directions in a conceptual framework. A threat model fixes the adversaries; four control layers (content, identity, integrity, environment) are chosen against it; an evaluation stage measures security, usability, fairness, privacy, cost and sustainability; and an evidence stage requires blinded replication, open data and a shared benchmark. The framework is a synthesis of the gaps identified above and has not been validated.

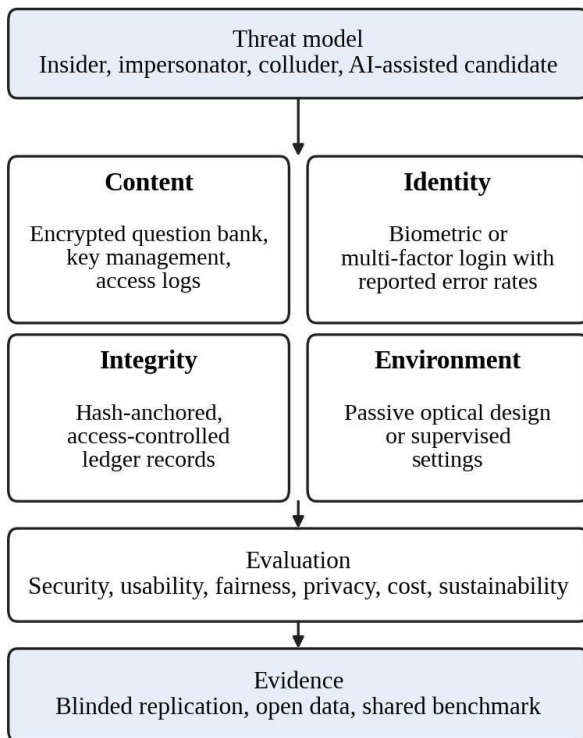


Fig. 5. Conceptual framework derived from the research gaps (original figure; not validated).

VIII. DISCUSSION

Taken together, the three studies show that practical examination security still lags behind available safeguards. Each proposed solution mainly addresses one security layer, while the supporting evidence is often weaker than the claims made. Study [1] is the only one that examines actual institutional practice and finds that most institutions manage their own infrastructure but still leave question banks unencrypted and depend mainly on passwords. This indicates an implementation gap as well as a research gap, since some surveyed institutions were already using AES [1].

The most promising approach depends on the evaluation criterion. For deployability, question-bank encryption is the most immediately applicable measure, although [1] does not

examine key management. For experimental evidence, the optical paper [2] is the only study using randomization and a control group, despite inconsistencies in its reported statistics. Blockchain records [3] show potential for improving result integrity, but the prototype does not yet demonstrate all its claimed benefits because of access-control, privacy, and cost concerns. Biometric authentication [1] may help address impersonation, but its effectiveness remains unquantified.

The results differ because the studies evaluate different security layers and outcomes, ranging from institutional practices and observed behavior to perceived security and prototype functionality. Their settings also vary, from a national survey to a classroom experiment and a technical prototype. Key adoption barriers include cost and technical expertise [1], wallet usability [3], environmental limitations of biometrics [1], lack of procedural standards [1], and unmeasured sustainability benefits [2].

This review has several limitations. It covers only three studies selected by the author and does not use a systematic search. The recomputation in Table III is based on stated assumptions, while values from the figures in [2] were estimated from published charts. Also, studies summarized within [1] were not independently examined. Because of this, the findings should be considered indicative rather than conclusive.

IX. CONCLUSION

This review compared three studies that protect examinations at different layers: encryption and authentication practices in Jordanian universities [1], a smart-contract prototype for online examinations [3], and an optical examination paper for paper-based tests [2]. The evidence is limited and uneven. The survey describes existing practices but not security outcomes, the prototype reports no quantitative measurements, and the experiment reports significant effects whose statistics cannot be reproduced from the published values.

The synthesis indicates that major practical weaknesses include unencrypted question banks and password-only authentication. Blockchain records can provide tamper evidence after submission but still require access control, privacy protection, and cost evaluation. Similarly, the optical paper is a promising but narrow control that requires further testing under blinded conditions. The authors identify gaps related to sample size, technical expertise, and threat scope, while this review also identifies missing threat models, identity binding, privacy analysis, cost and latency data, accessibility, generative-AI-assisted cheating, and common benchmarks.

Five directions are proposed: threat-model-based benchmarking, privacy-preserving ledger anchoring with identity binding, biometric and multi-factor authentication with reported error rates, auditable encrypted question banks, and replicated optical-paper trials with life-cycle assessment. Since the review covers only three studies, these conclusions are indicative, and a systematic search is needed to determine whether these gaps remain across the wider literature.

REFERENCES

- [1] A. M. Al-Ghonmein, Y. Alemami, K. G. Al-Moghrabi, and S. Atiewi, "Enhancing online exam security: encryption and authentication in Jordanian and international universities," *International Journal of Electrical and Computer Engineering*, vol. 15, no. 1, pp. 719–727, Feb. 2025, doi: 10.11591/ijece.v15i1.pp719-727.
- [2] B. M. Fouda, M. M. Ali, S. Abdelhalim, and N. Elgammal, "A sustainable smart exam paper design for enhancing examination confidentiality using visual security solutions," *Acta Innovations*, no. 61, pp. 264–284, 2026.
- [3] R. K. Giri, "Secured online exam using blockchain technology," *Anusandhanvallari*, vol. 2025, no. 1s, pp. 100–110, Jan. 2025.