International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(23s) 2026 pp. 803-814
https://doi.org/10.70917/ijcisim-2026-5640
Article

An Intelligent Multi-Layer Biometric-Cryptographic Framework for Securing Ministerial Examination Questions

Ahmed Ramzi Rashid[1], Mustafa Dhiaa Al-Hassani[2]

[12] Department of Computer Science, College of Science.
[1] ORCID: 0000-0003-3674-0097
[2] ORCID: 0000-0003-0981-4177

Abstract: This paper seeks to deal with distinct challenges experienced by contemporary educational settings in safeguarding ministerial exam queries owing to technological innovations and augmented risks like the unlawful access and inner pressures. It analyses the insufficiency of single-layer safety structures for the protection of sensitive data across all stages of its lifecycle. To deal with these potential threats, the study recommends a smart, multi-staged security model that can fortify the protection of sensitive exam data.

The model is produced to achieve a cohesive structure that improves access control, data privacy, and accessibility. It supports the expansion of detection devices, using both observable and concealed imprints to thwart interfering efforts and enable the documentation of such offenders for possible trial. A pilot assessment confirmed this model across different set-ups, illuminating important enhancements in access control efficiency, device efficacy, and data security whereas maintaining a balance between operative load and system sensitivity.

Generally, the projected a detailed model to provide a scalable and dynamic security set-up that is suitable to protect some sensitive educational information and make it vital for domains that need strong security measures and continuing observation.

Keywords: Biometric verification, Context-aware security, Hybrid cryptography, Multi-layer security model, Watermark-inclined traceability.

1. INTRODUCTION

Defending sensitive data is crucial in the field of scientific research, predominantly the defense of governmental exam questions, considering its deep effect on the reliability of educational organizations and their results. Exam questions are considered highly sensitive content, as their disclosure undermines the credibility of an entire institution and erodes public trust in the education system. However, the use of electronic systems is a double-edged sword; while fast and accurate, they are also vulnerable to a range of cybersecurity risks, including unauthorized access, misuse of credentials, interception of data in transit, and manipulation attacks [1, 2].

Most electronic systems employ a traditional, single-layer protection system using passwords or single-layer encryption methods. While these mechanisms can maintain information confidentiality to a certain extent, they cannot address contextual authorization requirements, such as biometric identity verification, geographic and time-based restrictions, and device reliability checks [3]. While biometric authentication enhances access security for authorized users, it remains vulnerable to misuse if used without regulation, authorization, and ongoing monitoring [4].

All recent studies on this topic have focused on integrating multiple technologies to strengthen the protection of sensitive information systems. Some of the studies reviewed explored hybrid encryption systems, biometric authentication, and blockchain-enabled verification models [5, 6]. Most educational systems designed by researchers rely on biometric verification, distributed security models, and zero-trust access to limit unauthorized users [7, 8].

Copyright: © 2026 by the authors

Despite these efforts, most educational platforms employ isolated security mechanisms, relying on only a specific part of the security architecture, rather than developing a comprehensive framework.

One of the obstacles encountered is the lack of a comprehensive security system for managing, storing, transmitting, and protecting exam questions for comparison. Most prevailing efforts suffer from operative trials that are not sufficiently handled.

To address these issues, this study suggests a multi-staged intelligent model that is reliant on biometric dimensions and encryption to protect governmental exam questions. This security model includes hybrid encryption, biometric features, biometric verification, time barricades, geofencing, device verification processes, and tracking and observing devices that depend on on watermarks, all in a combined security setting.

This study seeks to contribute in the following ways:

- Introducing a multi-staged smart framework for safe storing and delivery of exam questions.

- Mixing biometric verification with hybrid encoded and relative authorization processes within a distinct bundle.

- Safeguarding the structure via a bundle that comprises geolocation, time barricades, and device security measures.

- Applying an combined equipment of observable and invisible imprints to confirm pursuing and numeral forensics analysis.

The other parts of this paper is prepared as follows:

This study is projected in the following way: section one is the research procedure to address security system to defend exam questions. Section Three highlights the system architecture on system plan, threat framework, background access control processes, and operative safety strata. Section Four deal with the basic parts of the security structure, which include biometric confirmation, background approval processes, hybrid encoding, observing, and key organization. Section Five contains a case study and reproduction that reports the defense of governmental exam content. Section Six highlights the biometric verification device and background confirmation measures. Section Seven assesses the operative presentation and retreat efficiency of the scheme. Section Eight also examines operative hazards and model placement restrictions. Lastly, Section Nine recognizes possible future investigation directions.

2. RESEARCH METHODOLOGY

The purpose of the planned model is to plan a secure, multi-staged operative approach to improve the guard of sensitive information and confirm its safety dissemination in high-risk educational domains. The planned model combines biometric verification structures with hybrid encoding and numerous admittance control devices, along with pursuing and observation to confirm reliable and perfect system operation.

The framework has three main operational inputs, beginning with the first: fingerprint templates used in the authentication process to verify biometric identity. The second input consists of access control factors such as geolocation details, time barriers, and device reliability, including MAC address details, CPU ID, storage device information, and motherboard ID, which are used together as a fundamental component to support contextual authorization processesThe third entry point includes the exam question file, which will be encrypted and transmitted securely, and secure decryption mechanisms. The proposed framework was developed and implemented using C#/.NET with SQL databases to securely store, manage, and monitor operational data. Data is secured during storage and transmission by integrating AES-GCM and ChaCha20-Poly1305 algorithms within a hybrid algorithm to protect the proposed tests.

To enhance the security of the proposed system, biometric authentication has been integrated as a verification mechanism to ensure the authorization process, rather than being a separate authentication mechanism. Security was further strengthened by the addition of geolocation technology using a NEO-6M GPS module and a SIM808 module

that works with GPS and GSM, operating on an Arduino-based programming interface, which is a prerequisite for decryption.

The proposed security system is designed to integrate several technologies with improvements at each layer to ensure effective risk reduction, such as unauthorized access, and to enhance monitoring, tracking, and accountability mechanisms after a breach.

3. SYSTEM ARCHITECTURE AND THREAT MODEL

3.1 System Architecture

The proposed security system architecture adopts a multi-layered design to protect and manage ministerial exam question data, ensuring secure storage, encryption, and transmission, as well as monitoring and tracking capabilities. The architecture integrates biometric authentication, hybrid encryption, and access control mechanisms based on factors such as device authentication, geolocation, and time zone restrictions.

The workflow mechanism begins with verifying the user's fingerprint to confirm their identity using fingerprint templates, and then using access control verification processes that include geolocation verification, time barrier verification, and verification of trusted devices. Then the content of the exam questions is secured using a hybrid encryption mechanism before the secure transmission and controlled decryption procedures begin.

In addition to all the above security measures, this system is enhanced with tracking mechanisms based on the use of watermarks and recording all movements within the system to ensure complete monitoring and provide digital forensic analysis to identify the breach if it occurs and who is responsible for it. Figure (1) shows the general structure and interaction between the basic security layers of the proposed security system.

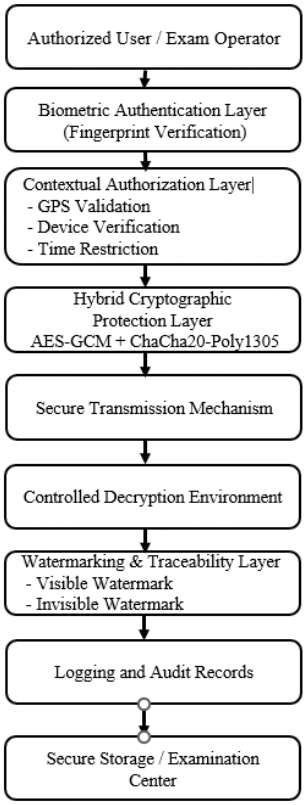

Figure 1. Overall architecture of the proposed multi-layer examination protection framework.

3.2 Data Protection During Transmission

The security foundation of the proposed system relies on a hybrid encryption mechanism to protect sensitive data during storage, transmission, and subsequent decryption. Encryption is achieved using a fully integrated hybrid algorithm based on two layers. The first layer utilizes AES-GCM and ChaCha20-Poly 1305. This hybrid algorithm is further enhanced by the design of the encryption and decryption key. The major component includes biometric fingerprint particulars and access control devices to produce an exclusive key, thus consolidating privacy and strong encoding.

In the process of distribution the encoding analysis the appropriate approval desires are met. These necessities comprise fingerprint confirmation to authorize uniqueness, attendance at the stated physical location, use of a principal device, and devotion to the stated timeframe. Failure to meet these requirements will result in the exam questions being decrypted under any circumstances.

After all operational security conditions are successfully met, decryption is performed. All system transactions and operations are meticulously documented to maintain a monitoring and tracking record capable of ensuring accountability in the event of a breach.

3.3 Security Design Rationale

The proposed security system design addresses weaknesses identified in previous systems, which relied on single-layer security mechanisms such as passwords or single-layer encryption. Once these are breached, the system is compromised, making it unsuitable for protecting sensitive data in a high-risk educational environment, particularly one responsible for evaluating a large number of students through final ministerial exams.

Therefore, the proposed security system adopts a coordinated, multi-layered security design. This design incorporates biometric verification, hybrid encryption, access control procedures, contextual authorization, and continuous monitoring throughout operation. All these layers combine to form a centralized, interdependent security system.

An additional layer relies on contextual authorization policies that authenticate devices, along with geolocation and time restrictions. Data decryption and system access are only permitted after all these conditions are met. This significantly reduces unauthorized access, even for users with valid credentials, as they must have a trusted device located at the designated location and time. A content tracking and monitoring mechanism has been added by reading the watermarks embedded in the content, whether visible or hidden, to identify the account holder responsible for leaking the content, as all movements within the system are documented and recorded.

3.4 Threat Model

The proposed security framework is designed to withstand threats to similar systems protecting sensitive data, including external threats and threats of misuse by authorized personnel that compromise the confidentiality and security of exam content and its secure distribution mechanisms .

Table 1. lists the main threats that the proposed security framework could face, along with the mitigation methods incorporated into the proposed system.

Table 1. Threat model and mitigation mechanisms

No.	Threat Scenario	Potential Risk	Mitigation Mechanism
1	Credential Theft	Unauthorized account access	Biometric verification + contextual authorization
2	Insider Misuse	Unauthorized examination disclosure	Time-bound access + audit logging
3	Unauthorized Device Usage	Access from untrusted systems	Device-binding validation
4	GPS Spoofing	Fake location authorization	Multi-factor contextual verification

5	Replay or Session Reuse	Repeated unauthorized access attempts	Session validation and temporal restrictions
6	Examination Leakage	Distribution of leaked content	Watermark traceability and forensic logging
7	Credential Sharing	Use of valid credentials by unauthorized individuals	Biometric authentication enforcement

What makes this system resilient to various threats is its reliance on multi-layered security rather than single-layered security. This is due to the multiple factors that underpin its protection mechanisms against threats such as unauthorized access to the system and instances of operational misuse.

Furthermore, the tracking, monitoring, and accountability mechanisms implemented through digital forensics enable the detection of suspicious access, support post-incident investigations, and pinpoint the source of any leaks.

3.5 Time Bound Security Layer

One layer of protection is a time barrier, which sets a specific disclosure period based on schedules determined by the entity responsible for managing the proposed security system. This barrier is designed to mitigate the risks arising from the early disclosure of exam content, which could lead to misuse of credentials, leakage of sensitive information, or unauthorized early access.

During the distribution of exam content, sensitive data is transmitted in a secure, encrypted packet as a hidden package, inaccessible even to authorized users, until the authorized release time. Some issues should be met, like fingerprint confirmation, the stated physical position, and the usage of a pre-approved device. If any of these situations are not met, the encoding procedure may be automatically forbidden.

4. MECHANISMS OF MULTI-STAGE SECURITY STRUCTURES

4.1 Verification and Authorization

The projected security structure depend on fingerprint verification to protect and confirm safety techniques, regulating unlawful admittance to protect content (questions). An amalgamation of issues is combined to improve scheme security by confirming prints along with background limitations such as reliable plans, time barriers, and geolocation to protect delicate information .

Traditional scrutiny schemes are dependent on single-layer, autonomous safety measures such as keywords or encoding, which cannot avert unlawful admittance or qualification leaks. This scheme overpowers these boundaries by planning some models that deal with numerous factors to confirm admittance is constrained to official users and averts misapplication of rights.

Further improving the scheme's consistency are the pursuing and observation of logs it uses. These logs record all forms of transactions in feature and document all encoding procedures with watermarks for traceability and responsibility in case of a gap.

4.2 Encryption Techniques

A hybrid encoding algorithm was planned for the projected safety model, to combine AES-GCM and ChaCha20-Poly 1305, to protect data storing and broadcast, as well as improve measured encoding. The reason for choosing this hybrid algorithm design was to improve encryption efficiency, overcome certain vulnerabilities, and protect data confidentiality during generation, storage, and transmission.

Instead of relying on fixed encryption standards, and to better secure data, a set of contextual inputs is used to generate a robust activation key. This key is based on a combination of factors, including a random component, biometric fingerprint, authenticated device identifiers, geographic location, and a specific time. The activation key generation process is represented as follows:

$$K_{final} = H(F_b \oplus D_{id} \oplus G_{loc} \oplus T_s) \quad \textbf{(1)}$$

Where:

- Kfinal The encryption final key generation.
- Fb Data extracted from fingerprint.
- Did Trusted device identifiers.
- Gloc Geographic location data.
- Ts Time access control values.

H Refers to the cryptographic hash function used to generate the final encryption key from a set of multiple contextual inputs.

Designing the security architecture in this way is to ensure that it does not rely on a single point of security, but rather on a set of contextual procedures to maintain documented encryption mechanisms to secure data at all stages it goes through, in order to improve the confidentiality of tests and reduce the risks that may be exposed to it.

4.3 Access Control Policies

The proposed security system relies on multiple control policies to regulate access to scanning and decryption processes, subject to access control according to the previously mentioned conditions. Access to data is only granted after all specified contextual security conditions are met simultaneously. These conditions include verification using biometric attributes, time barriers, geolocation, and the device used.

One of the challenges addressed was enhancing security mechanisms by multi-layering them while maintaining acceptable response speed and complexity. A set of operational conditions was implemented before access to protected data is granted.

One of the major security measures is the management of a log to confirm, audit, and record all sorts of transactions. This meaningfully decreases the dangers connected with credential misapplication or unlawful access efforts.

4.4 Monitoring and Auditing

Every system needs observing and reviewing records. The projected safety scheme has dealt this form to systematically, integrating devices for recording all scheme action and incessant observation and following to document the tracking procedure, confirm answerability, detect unlawful actions, and classify the offender of a breach. The event log archives every verification or confirmation process, efforts to admission exam content, encryption and decryption, account initiation and logout times, and scheme usage period. The scheme administrator can produce some files recording all action.

Additionally, to improve tracking, watermarks are supplemented to encoded files. These types of watermarks comprise information of each process. A digital forensics report is also accessible, given that exact details. The watermarks are planned to be resilient to cutting and compression, this makes them essential device to be tracking and classifying breaches. This differences with classical exam schemes, where the committer is frequently not recognized when a breach happens.

4.5 Security–Usability Balance

The projected safe system was planned with a very delicate balance between secrecy and security on the one hand. Thus, retrieving the scheme for approved workers is very modest and forthright, offered all the contextual circumstances are met. This removes the needless managerial difficulty essential in dispensing exam enquiries under classical examination schemes.

Applying biometric structures as the foundation for confirmation, verification, encoding, and decryption removes a number of processes that would be burdensome and monotonous. The user only enters their fingerprint, and the outstanding requirements are satisfied spontaneously and flawlessly. This confirms high privacy and consistency.

4.6 Dependence on Time and Geographical Location Factors

The projected system's safety is improved via context security which include time-inclined access control device and a geolocation-inclined access control device. The admittance control device fortifies access only at precise periods, restraining the period of the decryption procedure. This efficiently averts the leaky questions, a sensation that has happened recurrently in preceding years.

The geolocation safety layer confirms that the package can be decrypted through the system that can be obtained by approved persons at a specific time and place, thus justifying the risks of insider attacks and recommendation misuse.

4.7 Key Lifecycle Management

The planned safety scheme for defensive exam content through its lifecycle depend on on numerous issues, most prominently the use of unusual encoding keys based on special structured tenets. This ensures the confidentiality and security of exam content. The encryption keys are dynamically generated using several key factors that secure the proposed system. The key derives its information from a randomly generated fragment, along with biometric verification, geolocation, a trusted device identifier, and a specific time frame.

These temporarily generated operational encryption keys are used for encryption and decryption controlled by destructive contexts, without being stored permanently within the operating environment. This is to minimize the risks associated with the exposure of permanent keys and their unauthorized reuse.

Therefore, failure of any operational context security procedure will result in the failure of the associated decryption process. This approach to key management lifecycle management promotes controlled access to exams in high-risk educational environments.

4.8 Privacy and Biometric Data Protection

The projected safety scheme includes biometric data shield actions to lessen secrecy risks related with fingerprint-inclined verification devices. The key role of the biometric structures is to prove the uniqueness of the applicant and regulate whether they are an official user. Emphasis is placed on ensuring the confidentiality of this raw data, given its critical importance during the distribution of exam content..

Considering that insider threats are the most serious of all, biometric features are integrated into a comprehensive system to secure access to exam content and enhance its confidentiality.

Considering the potential challenges of biometric systems, including sensor reading variability and environmental authentication conditions, the system has been optimized to improve authentication and strengthen secure access procedures for exams.

4.9 Comparison with Traditional Exam Security

Due to the weaknesses identified in traditional examination systems, most notably their reliance on a single-layer security system such as standalone encryption, password protection, or fixed access control policies, in addition to the financial costs required for physically transmitting content and secondary problems affecting the entire country, such as internet shutdowns before and during exams to prevent the spread of leaked questions, the proposed security system addresses these issues. It deploys numerous stages of safety to reduce all possible issues essential in classical multiple examination formats.

To review, a evaluation is made between the safety approaches applied in classical examination programmes and the projected safety system, which is accessible in Table 3.

Table 2. Comparison of Security Measures in Traditional Examination Systems and the Proposed System.

No.	Security Feature	Traditional Systems	Proposed Framework
1	Authentication Method	Password-based access	Biometric + contextual authorization
2	Encryption Approach	Single-layer encryption	Hybrid cryptographic workflow
3	Access Control	Static authorization	Dynamic contextual authorization
4	Device Validation	Usually unsupported	Trusted device-aware validation
5	Examination Release	Manual or static scheduling	Time-bound controlled release
6	Traceability	Limited logging	Watermarking + forensic logging
7	Leakage Accountability	Weak or unavailable	Integrated monitoring and auditing

The above shows that all shortcomings identified in most classical analysis through the numerous security stages included into a single model for management governmental examinations. The measures implemented in the proposed system enhance contextual security, accountability, and traceability to confirm its functions even in high-risk instructive domains.

5. CASE STUDY: DEFENDING GOVERNMENTAL EXAM QUESTIONS USING INNOVATIVE TECHNOLOGIES MODELS

The assessment of a new system can be possible via a replication of the scheme to distribute and create a high-risk, educational domain. In this sense, the exam questions were encoded by the specific system administrator and disseminated from the principal server to approve sub-users using the projected safety set-up.

During this time, approved users had to achieve a kind of verification processes through fingerprints, confirm the reliable device, to authorize the location and then confirm the arrival period prior to the later decryption. It is also vital to confirm the arrival time before next decryption. The remaining packets are still left to go through usual processes and could only be decrypted after all required conditions were met.

Totaling traceability via watermarks and recording encryption, login, and decryption efforts confirms the structure to make it accountable, capable, and traceable digital forensics in the event of potential breach. Through unlawful operative scenarios, comprising ineffective biometric confirmation processes, use of an illegal method or geolocation, or efforts to access exam distinct content outside of selected time slots, the projected model spontaneously was rejected access.

In this regard, the projected security system can be combined through multiple stages within a unified safety protection domain that produced to improve security and the function of the perfect system that is operative and accountable and traceable.

6. Biometric Verification

The first amount in the projected security scheme is biometric confirmation through fingerprints to improve the identity confirmation during the access control and the decryption procedure.

The projected safety model may not function with relative fingerprints but the proposed template that was removed through the basic features but such biometric operating keys and verification.

This technique removes the necessity to propel part of a main parts of the receiver. The ordinary application of the application of the fingerprint that derived the organization ot the other contextual processes.

7. Results and Discussion

The projected security scheme was appraised within an operative setting that replicates genuine exam question delivery conditions. The focus was on numerous issues, mainly evaluating the consistency of biometric verification, the enactment of hybrid encoding, the processes used to regulate relative access, and the efficiency of mitigating these risks.

Table 3. The Assessment of biometric verification performance

No.	Metric	Value
1	Total Verification Attempts	200
2	Successful Matches	193
3	Failed Matches	7
4	FAR	1.5%
5	FRR	3.5%
6	Average Verification Time	1.2 sec.

The assessment outcomes for biometric confirmation prove steady presentation in operative distinctiveness acknowledgement, with satisfactory False Acceptance Rates (FAR) and False Rejection Rates (FRR) in skilful test domains. Incorporating biometric confirmation with other relative admittance control settings shows an important enhancement in operative access consistency and a considerable decrease in unlawful access.

Table 4. The Assessment of Encoding and Decryption presentation

No.	File Size	Encryption Time	Decryption Time
1	1 MB	0.41 sec.	0.36 sec.
2	5 MB	0.88 sec.	0.74 sec.
3	10 MB	1.47 sec.	1.31 sec.

The outcomes of the mixture of encryption assessment indicate that the hybrid safety measures prove satisfactory operative performance during both encoded and measured decryption. The timeframes for encoding, skimming, and decryption are still indicated to be secure and responsive, without unnecessary delay.

Table 5. Contextual access validation results

No.	Operational Scenario	Result
1	Authorized User + Authorized Device	Access Granted
2	Unauthorized Device	Access Denied
3	Invalid Geographic Location	Access Denied
4	Invalid Time Window	Access Denied
5	Invalid Fingerprint Verification	Access Denied

The above results show that contextual authorization has the ability to coordinate between multiple stages such as biometric verification, location identification, device authentication, and time barriers with a unified mechanism for controlling operational access.

Table 6. The Assessment of Threat Reduction

No.	Threat Scenario	Detection Result	Mitigation Outcome

1	Credential Sharing	Detected	Access Blocked
2	Unauthorized Device Access	Detected	Access Blocked
3	GPS Manipulation Attempt	Partially Detected	Context Validation Triggered
4	Session Replay Attempt	Detected	Session Rejected

The risk evaluation findings show projected model to resist unlawful access efforts. This is attained via numerous phases employed together to prevent such potential attacks. Furthermore, the addition of watermarks enhances tracking and accountability procedures in the event of a breach, and the provision of logs to document and record all system activity allows for holding the perpetrator accountable should a breach occur.

Additionally, the projected safety model considered the basic real-world biometric constraints with regards to the sensor superiority, ecological situations, and fingerprint response techniques. Other relative issues such as observing devices, time and location were also included to enhance the security of the system and other possible risks that may be provided by the entity.

8. Risk Scrutiny

Despite the projected security system's enhancements to the exam security via its contextual and operative measures of several practical constrains that occur in real-world instructive settings. These restrictions may include the consistency and accessibility of biometric sensors and their dimensions, as well as the obtainability of other essential elements for the effective execution of such a project.

Table 7. The proposed framework of operational risk analysis

No.	Risk Factor	Potential Impact	Mitigation Strategy
1	Biometric Sensor Failure	Authentication interruption	Multi-condition contextual validation
2	GPS Signal Manipulation	Incorrect location authorization	Context-aware authorization coordination
3	Hardware Dependency	Device compatibility limitations	Trusted device registration procedures
4	Network Instability	Delayed operational verification	Controlled offline operational handling
5	Credential Misuse	Unauthorized examination access	Biometric and contextual authorization enforcement

From the foregone, the data analysis indicates that the projected system may face in the process of the dissemination of the test content. Certainly, its procedure depend on profoundly on dependable biometric confirmation contextual and devices approval tools. Future enhancements could comprise sturdier anti-forgery devices, incorporation with a dispersed approval scheme by means of cloud computing, and the use of synthetic acumen to perceive and recognize irregularities, thus providing operative suppleness in large-scale instructive domains.

9. Conclusions and Future Work

This study offers a multi-staged operative security structure to safeguard the management, content, storage and encoding transmission of administrative exam questions in instructive domains, even high-risk ones. The system includes a detailed model that combines different processes of data encoding biometric and other operative background access control procedures such as time obstacles, device verification, geofencing, transaction logs and watermarking. This combined security domain affirms exam secrecy, strong publication administration, and operative answerability.

Despite these improvements, the scheme has the possibility for development and expansion in numerous areas. This comprises executing a deep learning-inclined fault detection algorithm and engaging forgery discovery devices. Additionally, the scheme can be made more dynamic and faster for management of secure investigation systems.

References

1. Belayadi, Y., Khababa, A., Attia, A., & Maza, S. (2022). An effective method based on bi-clustering and association rules for user activity analysis in location-based social network. *Ingénierie des Systèmes d'Information, 27*(6), 855–864.
2. Yusuf, A., & Abubakar, M. (2026). Development of a hybrid cryptographic security model combining lightweight PRESENT and RSA for resource-constrained devices. *Journal of Basics and Applied Sciences Research, 4*(1), 239–246.
3. Awwad, A. M. A. (2023). An adaptive context-aware authentication system on smartphones using machine learning. *Ingénierie des Systèmes d'Information, 27*(6), 903–915.
4. Ucheji, C. (2024). The future of zero-trust security architecture with AI automation. *International Journal of Research and Scientific Innovation (IJRSI), 13*(1), 700–713.
5. Abdulkareem, H., Baba, U. M., & Adamu, M. (2025). Biometric technology in security systems. *International Journal of Scientific Development and Research (IJSDR), 10*(4), b45–b60.
6. Yan, T., Chen, J., Zhang, X., & Hu, G. (2026). High-efficiency traceability mechanism for multimedia data in consumer Internet of Things combined with blockchain. *Multidisciplinary Digital Publishing Institute (MDPI), 26*(1), 74–96.
7. Gaata, M. T., & Al-Hassani, M. D. (2023). Underwater image copyright protection using robust watermarking technique. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 29*(2), 1148–1156.
8. Almalawi, A., Hassan, S., Fahad, A., & Khan, A. I. (2024). A hybrid cryptographic mechanism for secure data transmission in edge AI networks. *International Journal of Computational Intelligence Systems, 17*(1), 17–24.
9. Abdulkareem, R. (2024). Biometric systems: A comprehensive review. *Basra Journal of Science, 42*(1), 146–167.
10. Baleid, H. M., & Abdullah, M. F. (2026). Cybersecurity in higher education: A systematic review of threats, challenges, and mitigation strategies. *Journal of Science and Technology, 31*(1), 20–27.
11. Awwad, A. M. A. (2023). An adaptive context-aware authentication system on smartphones using machine learning. *International Journal of Safety and Security Engineering, 13*(5), 903–915.
12. Ulven, J. B., & Wangen, G. B. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 2–40.
13. Alzaidi, Z. S., Yassin, A. A., & Abduljabbar, Z. A. (2024). Main primitive and cryptography tools for authentication in VANET environment: Literature review. *Journal of Basrah Researches (Sciences), 50*(1), 222–249.
14. Mohammed, A., Salama, A., Shebka, N., & Ismail, A. (2025). Enhancing network access control using multi-modal biometric authentication framework. *Engineering, Technology & Applied Science Research, 15*(1), 20144–20150.
15. Al-Hassani, M. D., & Zuhair, J. B. (2018). An innovative data encryption technique through keys distributed over websites using linked-lists. In *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, Wasit–Kut, Iraq, March 14–15, 2018, id. 18.
16. Sylla, T., Chalouf, M. A., Krief, F., & Samaké, K. (2021). Context-aware security in the Internet of Things: A survey. *International Journal of Autonomous and Adaptive Communications Systems, 14*(3), 231–265.
17. Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control. *Alexandria Engineering Journal, 84*, 275–284.
18. Al-Fatlawi, K., Abd Zaid, M. M., Alyassri, L. S., & Albayati, O. M. (2025). Biometric authentication methods for strengthening access control in wallets and digital finance applications. Dubai, 2025.
19. Abdulla, Q. Z., & Al-Hassani, M. D. (2023). Robust password encryption technique with an extra security layer. *Iraqi Journal of Science, 64*(3), 1477–1486.
20. Xun, W., Du, X., Li, M., & Bao, X. (2023). Technology-enabled traceability and sustainable governance: An evolutionary game perspective on multi-stakeholder collaboration. *Sustainability, 17*(1), 1–30.
21. Ucheji, C. (2026). The future of zero-trust security architecture with AI automation. *International Journal of Research and Scientific Innovation (IJRSI), 13*(1), 700–713.
22. Elijah, B. T. (2023). Framework for enhancing security in computer-based examinations using a multimodal biometrics-supervision system. *Benin Journal of Advances in Computer Science, 8*(2), 29–39.
23. Abdulkareem, H., Baba, U. M., & Adamu, M. (2025). Biometric technology in security systems. *International Journal of Scientific Development and Research (IJSDR), 10*(4), b45–b50.
24. Abdulla, Q. Z., & Al-Hassani, M. D. (2023). Robust password encryption technique with an extra security layer. *Iraqi Journal of Science, 64*(3), 1477–1486.
25. Kakade, S., & Raut, U. (2026). Biometric authentication systems: Trends, challenges, and future prospects – A comprehensive review. *National Library of Medicine*.
26. Karamchand, G. (2022). Zero trust and AI: A synergistic approach to next-generation cyber threat mitigation. *World Journal of Advanced Research and Reviews, 24*(3), 3374–387.
27. Chinwe, L. C., & Ukachukwu, N. T. (2025). Secured examination management system using multi factor authentication. *International PeerReviewed Journal, 11*(6).

28. Tripathi, D. R., & Nishad, D. K. (2020). Biometric authentication systems: A survey. *Turkish Journal of Computer and Mathematics Education, 11*(3), 2878–2884.
29. Seshagiri, A. (2024). Multi-factor authentication based on biometric data. *American Research Journal of Computer Science and Information Technology, 7*(1), 42–46.
30. Mane, J. S., & Bhosale, S. (2023). Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics. *Revue d'Intelligence Artificielle, 37*(3), 709–718.
31. Abdulla, A. H., Mohamed, A. H., & Razali, S. (2020). A review on cybersecurity: Challenges & emerging threats. In *The 3rd International Conference on Networking, Information Systems & Security*, Morocco.
32. Ulven, J. B., & Wangen, G. B. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2).
33. Obasi, C., Ikharo, B., & Oisamoje, V. (2022). Security in distributed system: A review perspective. *International Journal of Latest Technology in Engineering Management & Applied Science, XI*(X), 49–55.
34. Sylla, T., Chalouf, M. A., Krief, F., & Samaké, K. (2021). Context-aware security in the Internet of Things: A survey. *International Journal of Autonomous and Adaptive Communications Systems, 14*(3), 231–265.
35. Khalaf, F. M., & Sagheer, A. M. (2025). A hybrid encryption model with blockchain integration for secure cloud data storage and retrieval. *Journal of Information Systems Engineering and Management, 10*(22), 169–179.
36. Mudavatu, V. K. N. (2025). Zero trust security architecture for legacy systems. *International Journal of Scientific Research in Computer Science Engineering and Information Technology, 11*(2), 2305–2313.
37. Bouhissi, H. E., & Yurko, P. (2025). Analysis of biometric access control systems. *Computer Systems and Information Technologies*, 87–96.
38. Chan, W., Gai, K., Yu, J., & Zhu, L. (2025). Blockchain-assisted self-sovereign identities on education: A survey. *MDPI, 3*(1), 1–37.