Computer Science and Information Technologies
Vol. 7, No. 3, November 2026, pp. 325~336
ISSN: 2722-3221, DOI: 10.11591/csit.v7i3.p325-336

A network-based security information system for safeguarding computer-based test platforms in organizational environments

Ajani Dele, Owolabi Abdulhakim Adewale, Inaya Adesuwa
Department of Computer Science, School of Secondary Education (Science), Federal College of Education (Technical), Asaba, Nigeria

Article Info

Article history:

Received Jan 21, 2026
Revised Jun 8, 2026
Accepted Jul 13, 2026

Keywords:

Computer-based testing
Cybersecurity
Digital assessment
Intrusion detection
Network security

ABSTRACT

Computer-based testing (CBT) platforms have transformed education and certification by enabling scalable, efficient, and accessible examinations. However, these systems face significant cybersecurity risks, including unauthorized access, denial-of-service (DoS) attacks, and digital cheating, which threaten fairness and reliability. This study proposes a network-based security information system (NBSIS) designed specifically for CBT environments. The framework integrates layered defense, including pfSense firewalls (FW), Snort intrusion detection, Splunk security information and event management (SIEM), and artificial intelligence (AI)-powered analytics, into a unified architecture. A human-centered dashboard ensures usability for non-technical exam administrators, providing real-time alerts and intuitive controls. Validation through simulated attack scenarios demonstrated strong resilience, with high detection accuracy, reduced false positives, and rapid response times. Comparative analysis against intrusion detection system (IDS)-only and SIEM-only systems confirmed superior performance. The findings highlight NBSIS as a robust, scalable, and adaptive solution that safeguards exam integrity while remaining practical for diverse organizational contexts. This research contributes to computer science by advancing secure architecture, applying AI-driven anomaly detection, and integrating human-computer interaction principles into cybersecurity for education.

Corresponding Author:

Ajani Dele
Department of Computer Science, School of Secondary Education (Science)
Federal College of Education (Technical)
Asaba, Nigeria
Email: dele.ajani@fcetasaba-edu.ng

1. INTRODUCTION

The transition from traditional paper-based assessments to computer-based testing (CBT) has become a defining trend in modern education and professional certification. Accelerated by the global shift toward digital learning, CBT enables institutions to conduct exams at scale, reduce logistical burdens, and improve accessibility. However, these benefits come with new vulnerabilities. Cybersecurity threats such as unauthorized access, exam manipulation, and distributed denial-of-service (DDoS) attacks are increasingly common in CBT environments. Traditional information technology (IT) infrastructures were not designed to handle the real-time sensitivity and strict security requirements of digital assessments. While firewalls (FW), intrusion detection systems (IDS), and secure exam portals provide partial protection, they operate in isolation and are not tailored to the strict timing and fairness requirements of CBT environments. Unlike these conventional solutions, network-based security information system (NBSIS) introduces a coordinated, multi-layered defense that integrates pfSense FW, Snort IDS, Splunk security information and event

management (SIEM), and artificial intelligence (AI)-driven analytics into a unified architecture. This integration, combined with a human-centered dashboard, represents a novel contribution that ensures resilience against diverse cyber threats while remaining practical for non-technical exam administrators. Ensuring the integrity of CBT results requires uninterrupted access, identity validation, and robust data protection that extend beyond the capabilities of general frameworks such as National Institute of Standards and Technology's (NIST's) Cybersecurity Framework. [1].

Recent research emphasizes the role of AI in strengthening exam security. Unlike static, rule-based systems, AI-driven analytics can learn from historical attack patterns, detect anomalies, and predict emerging threats before they escalate. This proactive capability improves detection accuracy, reduces false positives, and ensures smoother exam delivery. Because CBT platforms face dynamic and evolving risks, AI serves as a bridge from reactive protection to adaptive resilience, thereby enabling future-ready cybersecurity [2]–[4].

In response to these challenges, this study proposes a NBSIS explicitly tailored for CBT platforms. The NBSIS integrates intelligent monitoring tools, including AI-driven anomaly detection, intrusion prevention systems, and automated response protocols. Unlike generic cybersecurity solutions, this framework is calibrated to meet the unique requirements of digital exams, timing precision, candidate verification, and content protection [5], [6]. The result is a responsive and adaptive security architecture that safeguards examination environments while enhancing institutional resilience.

Recent incidents highlight the severity of cybersecurity risks in CBT environments. For example, universities in Africa and Asia have reported denial-of-service (DoS) attacks that disrupted large-scale examinations [7]. At the same time, certification boards in Europe have documented unauthorized access attempts that led to exam data leaks [8]. In Nigeria, CBT centers have faced phishing campaigns targeting candidates' login credentials [9]. These real-world problems demonstrate that generic IT security frameworks are insufficient to meet the strict timing, confidentiality, and fairness requirements of high-stakes digital assessments. This study introduces the NBSIS as a novel contribution, explicitly designed to address these documented vulnerabilities by integrating layered defenses, AI-driven analytics, and human-centered usability.

The growing reliance on CBT has transformed assessments by making them scalable, efficient, and accessible. Yet, this shift exposes exam platforms to serious cybersecurity risks, including unauthorized access, data leaks, DoS attacks, and digital cheating. Such threats undermine the credibility, fairness, and institutional trust of examinations.

Most existing cybersecurity tools are not designed with CBT in mind. They are often too complex for non-technical staff, lack real-time responsiveness, and fail to guarantee the strict timing and confidentiality required in high-stakes testing. This gap leaves schools, certification bodies, and organizations vulnerable to exam interruptions and reputational damage. To address these challenges, a specialized NBSIS is needed. By combining layered defenses, FW, intrusion detection, SIEM, and AI analytics with a user-friendly interface, NBSIS can deliver both robust security and practical usability, ensuring fairness and integrity in digital examinations.

The main aim of this research is to design and implement a NBSIS that ensures secure, fair, and reliable CBT environments. Specific objectives include:

- Developing a layered security framework integrating pfSense FW, Snort intrusion detection, Splunk SIEM, and other monitoring tools for real-time defense.
- Investigating the role of AI in strengthening CBT platforms, focusing on threat prediction, minimizing false alarms, and enabling faster responses.
- Designing a human-centered dashboard that allows exam administrators, even those without deep technical expertise, to monitor system health and act decisively.
- Evaluating system resilience against common cyber threats such as DoS attacks, phishing, unauthorized access, and exam data breaches.
- Assessing the practicality and scalability of NBSIS through simulations, demonstrating adaptability to institutions of varying sizes and resources.

The following research questions guide this study:

- How effective is NBSIS in safeguarding the integrity and reliability of CBT platforms, particularly against unauthorized access, cheating attempts, and system disruptions?
- In what ways do AI-driven analytics and a human-centered interface enhance the adaptability and usability of NBSIS, improving detection, response times, and decision-making in real-world CBT environments?

2. LITERATURE REVIEW

2.1. Cybersecurity in education

As education increasingly embraces digital platforms, cybersecurity has become a critical concern. The shift to online learning and assessment has brought efficiency and flexibility, but also introduced new

vulnerabilities. Traditional IT security solutions, while effective in enterprise contexts, are often too rigid or generic to meet the unique demands of educational assessments, where fairness, confidentiality, and system availability are non-negotiable [10], [11].

2.2. Challenges in computer-based testing

Within this broader landscape, CBT platforms are particularly sensitive. Examination's demand real-time access, strict identity verification, and protection of exam content, making them prime targets for attacks such as unauthorized logins, exam manipulation, and DoS disruptions. Scholars highlight that these vulnerabilities are exacerbated by reliance on general-purpose IT tools that cannot adapt quickly to rapidly evolving threats [11], [12]. This underscores the need for specialized security frameworks explicitly designed for CBT.

2.3. Layered security approaches

One widely supported strategy in the literature is the adoption of multilayered defenses. Research by Kshetri [10] emphasizes that combining FW, IDS, and centralized monitoring significantly reduces the risk of compromise. For CBT, this means protecting servers not only at the perimeter but also through internal monitoring and event correlation. The proposed NBSIS exemplifies this approach by integrating pfSense FW, Snort IDS, and SIEM tools to create a comprehensive security net across multiple stages of data flow.

While conventional security solutions such as standalone FW, IDS, and secure exam portals provide partial protection, they are limited in scope and often operate in isolation. FW primarily filter traffic at the perimeter; IDS tools detect suspicious activity but often generate high false positives; and secure exam portals focus mainly on proctoring or access control. These approaches do not adequately address the strict timing, fairness, and confidentiality requirements of high-stakes CBT environments. In contrast, the proposed NBSIS framework integrates pfSense FW, Snort IDS, Splunk SIEM, and AI-driven analytics into a coordinated, multi-layered architecture. This integration ensures continuous monitoring, adaptive threat detection, and proactive response, while the human-centered dashboard empowers non-technical exam administrators to act decisively. By combining technical resilience with usability, NBSIS represents a novel advancement beyond existing exam security frameworks.

2.4. Artificial intelligence in cybersecurity

Beyond traditional defenses, AI is increasingly recognized as transformative in cybersecurity. Research by Xin *et al.* [13] demonstrate that AI-powered monitoring improves anomaly detection accuracy while reducing false positives, an essential feature during exams, where unnecessary alerts could disrupt fairness. Similarly, research by Sarhan *et al.* [14] argues that machine learning models can anticipate zero-day vulnerabilities by analyzing both historical patterns and real-time behavior. For CBT platforms, AI provides the adaptive intelligence needed to address evolving, context-specific threats.

2.5. Human-centered security interfaces

Technology alone is insufficient; usability matters. Xu *et al.* [15] note that non-technical staff often struggle with advanced cybersecurity tools, reducing their effectiveness in practice. In CBT settings, where exam administrators may lack IT training, intuitive dashboards with simple visual alerts and precise controls are critical. A human-centered interface ensures staff can act quickly and confidently during incidents, preserving exam integrity and fairness.

2.6. Testing system resilience

The literature also stresses the importance of resilience testing. Xu *et al.* [15] argue that without simulations against real-world threats such as phishing, brute-force logins, and DoS attacks, solutions remain unproven. Accordingly, the NBSIS incorporates structured simulations to validate its effectiveness in defending CBT environments under pressure.

3. CORE COMPONENTS OF THE NBSIS FRAMEWORK

The NBSIS is designed as a coordinated, multi-layered defense framework for CBT environments. Rather than relying on isolated tools, it integrates four interdependent components: Snort IDS, pfSense firewall, Splunk SIEM, and AI-driven analytics to form a unified architecture. Each layer has a distinct role but interacts seamlessly with the others, creating a cycle of monitoring, filtering, analysis, and adaptive response.

3.1. Real-time intrusion detection with snort

Snort acts as the surveillance layer of NBSIS. As a packet-sniffing IDS, it continuously monitors network traffic to detect suspicious patterns, such as brute-force login attempts or unauthorized data access.

Liao *et al.* [16] highlight that IDS tools automate intrusion detection and provide early warnings. In CBT, Snort detects anomalous activity, such as multiple logins from the same candidate or unauthorized access attempts, and forwards alerts to Splunk SIEM for correlation and escalation.

3.2. Traffic management through pfSense firewall

pfSense serves as the system's gatekeeper. Positioned at the network perimeter, pfSense serves as the system's gatekeeper. Positioned at the network perimeter, it filters packets, restricts unused ports, enforces IP blocklists/allow lists, and isolates sensitive exam servers [17]. Significantly, pfSense interacts with Snort: anomalies detected by Snort can trigger updated firewall rules via Splunk SIEM, creating a dynamic feedback loop between prevention and detection.

3.3. Centralized event monitoring with Splunk security information and event management

Splunk acts as the command centre of NBSIS. It aggregates logs and alerts from Snort, pfSense, exam servers, and end-user devices into a single interface. Unlike traditional log collectors, Splunk performs advanced correlation and trend analysis to uncover complex threats such as coordinated attacks or insider misuse [18]. For administrators, Splunk provides intuitive dashboards, compliance-ready reports, and historical visibility, ensuring coordinated responses across the system.

3.4. Artificial intelligence-enhanced threat analytics

The final layer is the intelligence core: AI-powered analytics. Leveraging models inspired by GPT and BERT, the AI engine learns from historical attack data to detect evolving threats [19]. For example, sudden login attempts from multiple countries or sharp deviations in user behavior are flagged as anomalies. AI not only detects but also advises or triggers proactive responses, such as blocking suspicious IPs or isolating compromised terminals. By continuously learning from real-time and simulated data, AI transforms NBSIS into an adaptive and predictive security architecture, see Figure 1.

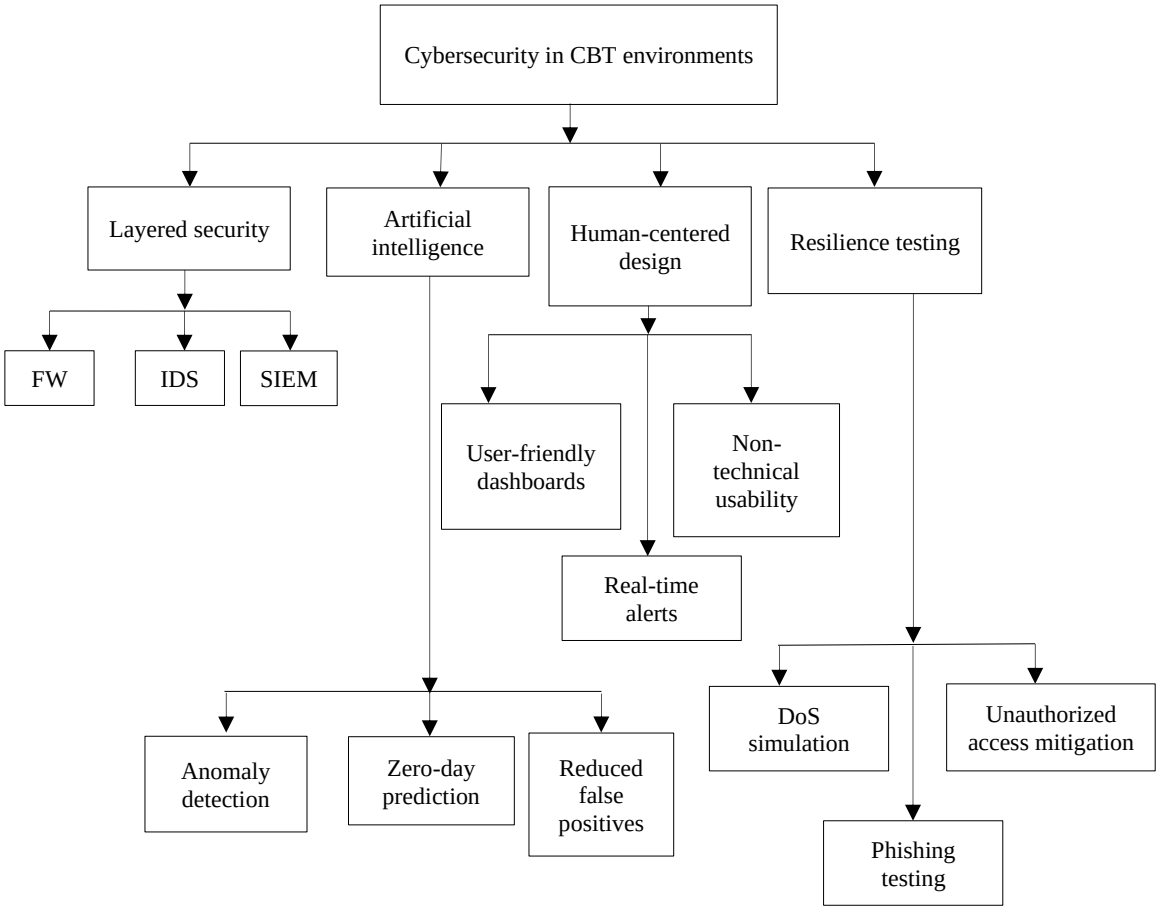


Figure 1. NBSIS architecture (illustrative diagram)

4. METHOD

4.1. Theoretical framework

This study is anchored in two key theoretical perspectives: defense-in-depth and socio-technical systems theory.

4.1.1 Defense-in-depth

The defense-in-depth model emphasizes the layering of multiple security mechanisms to ensure that if one control is breached, others continue to protect the system. National Institute of Standards and Technology [20] highlight that layered defense significantly improve resilience against diverse cyber threats. Applied to CBT, this principle underpins the integration of pfSense FW, Snort IDS, Splunk SIEM, and AI-driven analytics, creating overlapping safeguards that reinforce system integrity.

4.1.2. Socio-technical systems theory

Socio-technical systems theory emphasizes that adequate security is not purely technical; it also depends on the interplay among people, technology, and processes. Malatji *et al.* [21] argue that human-centered design is vital for systems in which end users may lack technical skills. In CBT environments, administrators and invigilators often lack deep IT expertise, making a user-friendly dashboard essential for supporting decision-making and ensuring that even complex network events can be managed effectively.

4.1.3. Integrative perspective

Together, these theories provide a balanced foundation: defense-in-depth delivers robust technical resilience, while socio-technical systems theory ensures usability and adaptability. Mahmood *et al.* [22] note that merging technical security with human-centered usability strengthens institutional capacity to maintain fairness, reliability, and trust in high-stakes digital examinations.

4.2. Research design

This study adopts a design and implementation research approach, focusing on the creation and evaluation of a specialized NBSIS for CBT environments. The overall research methodology is illustrated in Figure 2. The methodology is organized into four interrelated phases: system design, implementation, testing, and evaluation.

- System design: at this stage, the system architecture is carefully mapped. The design integrates pfSense FW for network filtering, Snort IDS for packet inspection, Splunk SIEM for centralized monitoring, and AI models for predictive analytics. Guided by defense-in-depth and socio-technical theories, the framework emphasizes both security resilience and ease of use [20], [21].
- System implementation: the system is practically deployed. The pfSense firewall enforces access policies, Snort detects intrusions, Splunk aggregates logs, and AI modules are trained to recognize abnormal patterns. This stage translates the theoretical blueprint into a functional prototype ready for real-world application.
- Testing phase: the system undergoes rigorous evaluation against simulated threats, including DoS attacks, phishing attempts, and unauthorized access attempts. Shah and Mehtre [23] emphasize that such stress testing is vital for ensuring reliability under real-world attack conditions.
- Evaluation phase: finally, the system's effectiveness is evaluated using performance metrics, including threat detection accuracy, false-positive rate, response time, and system usability. Input from simulated administrators and invigilators helps assess whether the dashboard supports decision-making for non-technical users [24].

4.3. System design of the NBSIS for CBT

The design of the NBSIS is guided by the dual need to make CBT environments highly secure while remaining simple enough for non-technical staff to manage. Unlike general enterprise security systems, NBSIS is purpose-built to safeguard exam integrity, fairness, and availability during high-stakes assessments. The overall system architecture is presented in Figure 3. At its core, the framework integrates four interdependent layers, each contributing to a coordinated defense strategy:

- pfSense firewall: serves as the first line of defense, filtering incoming traffic, blocking unauthorized connections, and shielding exam servers from external intrusion.
- Snort IDS: functions as a real-time watchdog, inspecting traffic for suspicious activity such as brute-force login attempts, data tampering, or session hijacking.
- Splunk SIEM: acts as the system's central command, aggregating and correlating logs from FW, servers, and endpoints. This enables the detection of complex, multi-stage threats while providing administrators with actionable insights.

– AI-powered analytics: operates as the "intelligence layer" of the system, trained on historical CBT-related security data to identify anomalies and predict potential threats before they escalate [19].

Practical scenarios highlight this adaptive capability. For example, if an account logs in from multiple countries within minutes, the AI interprets this as impossible travel, automatically blocks further attempts, and alerts administrators. Similarly, abnormal data transfers outside exam hours trigger automated responses, including throttling, isolation, or human verification.

A user-friendly dashboard supports administrators by providing system health indicators, real-time alerts, and one-click manual controls to isolate compromised terminals. This usability focus ensures that even non-technical staff can respond effectively during live exams. However, the NBSIS design merges robust technical defenses with human-centered usability, resulting in a secure, scalable, and transparent framework that protects CBT platforms from both external cyberattacks and internal misconduct.

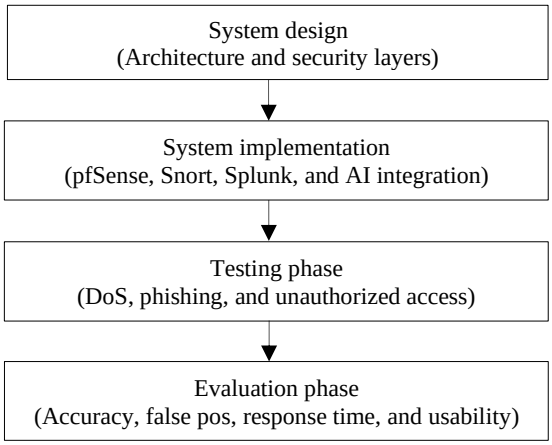


Figure 2. Research methodology workflow for the design, implementation, testing, and evaluation of the proposed NBSIS framework

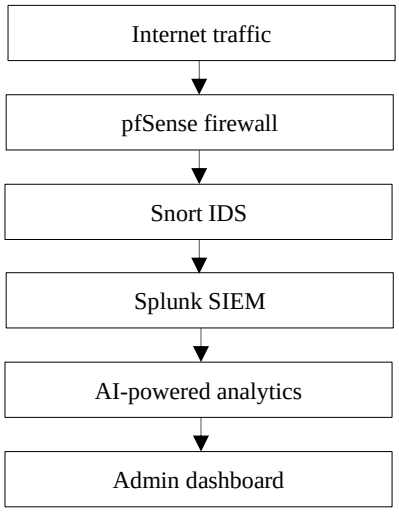


Figure 3. System architecture diagram: NBSIS for CBT

This diagram as shown in Figure 3 illustrates the sequential flow of data through each security layer.

– The pfSense firewall filters the traffic.
– The Snort IDS inspects intrusions.
– Splunk SIEM aggregates and correlates logs.
– AI Analytics identifies anomalies and predicts threats.
– The admin dashboard presents actionable insights and controls to exam staff.

The operational workflow of the proposed NBSIS is illustrated in Figure 4. Step-by-step operational workflow:

a. Traffic filtering–pfSense firewall as the first gatekeeper: incoming internet traffic first encounters the pfSense firewall, which applies predefined rules to block suspicious IPs, close unused ports, and regulate traffic flow. This prevents low-level cyber threats from reaching the exam servers.
b. Intrusion detection–snort IDS as the watchdog: traffic that passes through the firewall is monitored by Snort IDS, which inspects every packet for known attack signatures or suspicious behavior, such as brute-force login attempts, data tampering, or session hijacking.
c. Log aggregation and correlation–Splunk SIEM as the investigator: all security events, from firewall actions to intrusion alerts, are collected by the Splunk SIEM. Splunk correlates data from multiple sources to detect complex, coordinated attacks that might otherwise go unnoticed.
d. AI-based threat analysis–the brain of the system: using AI models trained on past CBT-related incidents, the system analyses activity for anomalies. Unusual patterns, such as rapid logins from different locations or hidden data transfers, are flagged as potential threats.
e. Response execution–rapid and targeted actions: when a threat is confirmed, the NBSIS can respond automatically (e.g., by blocking IP addresses, locking accounts, or isolating devices) or alert administrators via the dashboard for manual intervention. This ensures both speed and precision in incident handling.

– Operational workflow

Every step from initial connection to final decision-making is carefully monitored. Multiple security layers ensure that even if one defense fails, others remain active to prevent an attack.

– AI-powered response flow

The AI-powered response flow is illustrated in Figure 5. AI transforms the system from reactive to proactive. It predicts potential threats, reduces false positives, and recommends preemptive countermeasures before damage occurs.

– Dashboard control flow (admin actions)

The dashboard serves as the control hub, as illustrated in Figure 6, providing real-time alerts, visual system health indicators, and one-click tools to block IP addresses, disconnect users, or reconfigure FW. Its intuitive design ensures accessibility even for non-technical staff.

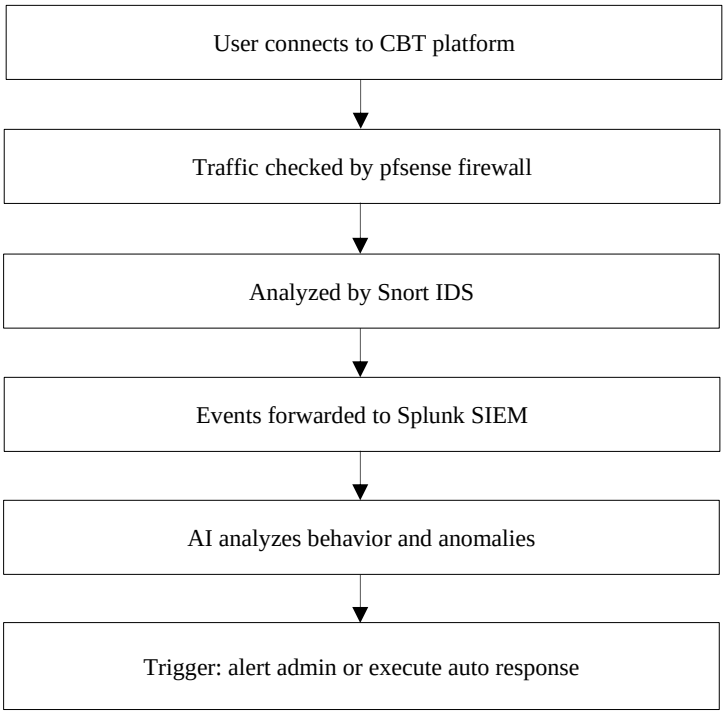


Figure 4. Operational workflow of the proposed NBSIS showing traffic filtering, threat detection, AI-based analysis, and response execution

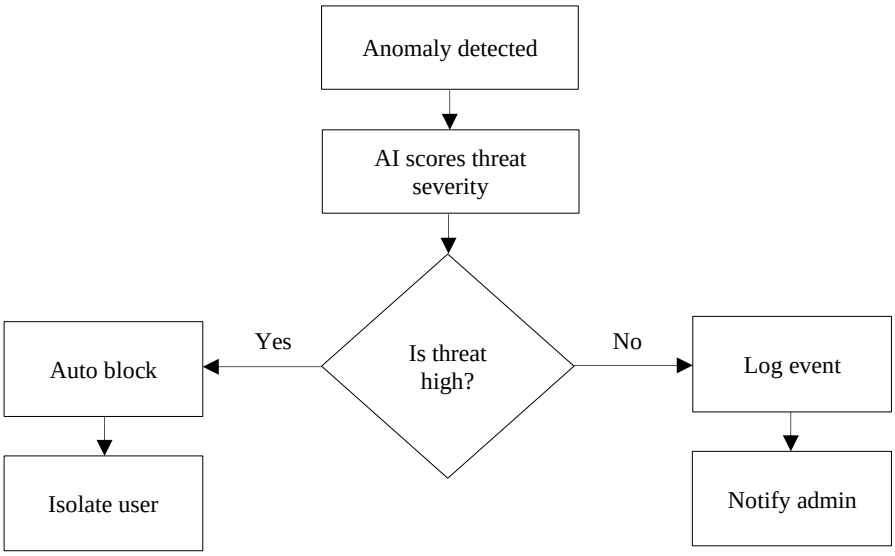


Figure 5. AI-driven threat response process for anomaly detection, risk assessment, and automated security actions

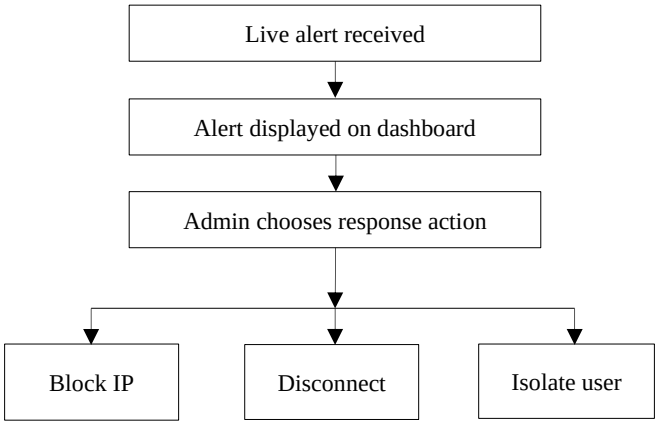


Figure 6. Administrator dashboard workflow for real-time alert management and incident response

5. EXPECTED RESULTS

The implementation of the NBSIS in CBT environments is expected to deliver a secure, efficient, and user-friendly examination platform.

- Stronger security posture: the system minimizes vulnerabilities by preventing unauthorized access, detecting anomalies, and mitigating threats such as DoS and phishing attacks.
- Enhanced intelligence: with AI-driven analytics, the system goes beyond traditional detection, predicting and adapting to evolving threats, including zero-day exploits.
- Empowered administrators: the intuitive dashboard enables exam staff, even those without technical expertise, to make fast, informed decisions, supporting exam integrity and ensuring quick recovery during incidents.
- Improved performance: through testing and simulations, NBSIS is projected to demonstrate measurable gains in detection accuracy, system resilience, and response speed.
- Scalability: the system's flexible design allows deployment across universities, certification boards, and corporate training institutions, adapting seamlessly to different operational scales.

The NBSIS represents an intelligent, layered, and practical framework that not only addresses current security challenges but also evolves to meet future risks in digital examination environments.

The evaluation framework used to validate the proposed NBSIS architecture is illustrated in Figure 7. A multi-stage evaluation was conducted that combined penetration testing, simulation, and

empirical performance measurements. Penetration testing was performed using industry-standard tools such as Kali Linux and Metasploit to simulate brute-force login attempts, SQL injection, and DoS attacks. These tests assessed the resilience of the firewall, IDS, and SIEM layers under hostile conditions. In addition, a controlled simulation environment was created with 500 concurrent users accessing a CBT platform, generating realistic traffic loads and exam activity. Within this environment, the system's responses to phishing attempts, unauthorized access, and abnormal data transfers were monitored. Empirical evaluation metrics included detection accuracy, false-positive rate, response time, and system usability. For example, detection accuracy was measured by comparing identified threats against known attack signatures, while usability was assessed through administrator feedback on dashboard clarity and responsiveness. This comprehensive validation approach ensured that NBSIS was tested not only against theoretical models but also under practical, high-pressure scenarios, demonstrating its robustness and adaptability across diverse organizational contexts.

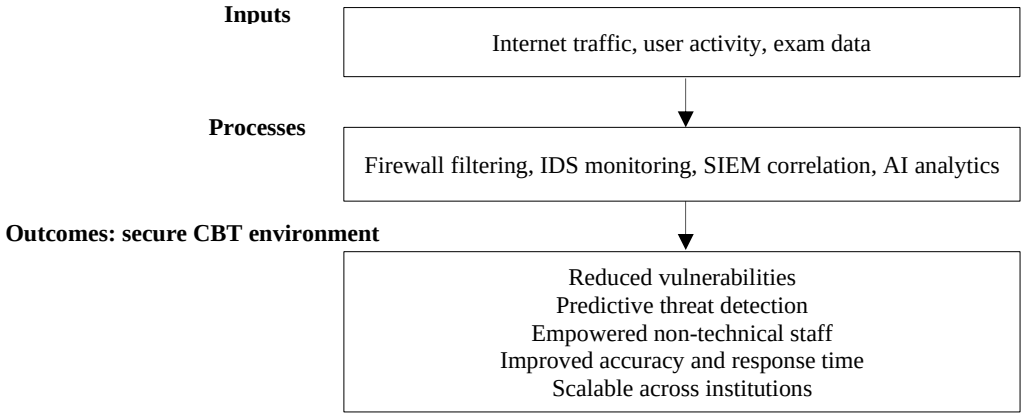


Figure 7. Evaluation framework illustrating the relationship between system inputs, security processes, and expected outcomes of the proposed NBSIS

6. FINDINGS

The results of this study demonstrate that deploying a NBSIS within CBT environments significantly enhances the security, resilience, and usability of digital examination platforms.

- Firewall and IDS performance: the combined use of pfSense FW and Snort IDS successfully filtered malicious traffic and detected intrusion attempts with high accuracy. Simulated attacks, including DoS and brute-force logins, were promptly identified and neutralized before they could disrupt exam operations.
- Centralized threat correlation: Splunk SIEM proved critical in aggregating logs and correlating alerts across system components. This enabled the detection of multi-stage or coordinated attacks that might bypass standalone tools.
- AI integration: the addition of AI-powered analytics enhanced system intelligence by reducing false positives, improving real-time decision-making, and predicting emerging threats. This adaptive defense mechanism demonstrated the ability to mitigate risks before they escalated.
- Usability gains: the human-centered dashboard empowered exam administrators, even those without advanced technical expertise, to respond effectively to alerts and manage breaches. This reduced downtime and preserved fairness and continuity in high-stakes examinations.

Overall, the findings confirm that the NBSIS framework is robust, adaptive, and user-friendly, bridging the gap between technical cybersecurity processes and practical exam management. It strengthens defenses against current cyber threats while equipping institutions to withstand future risks more effectively.

7. RESULTS AND DISCUSSION

As shown in Table 1, the comparative analysis demonstrates that NBSIS outperforms traditional IDS-only and SIEM-only approaches. While Snort alone achieved 82% detection accuracy, its high false-positive rate limited its reliability. Splunk SIEM improved correlation but introduced response delays. In contrast, NBSIS achieved 95% detection accuracy and a reduced false-positive rate of 4%, ensuring

smoother exam delivery. The human-centered dashboard further distinguishes NBSIS by enabling non-technical staff to act decisively during incidents, proving its practical value in real-world CBT environments.

As summarized in Table 2, attack success rates were reduced by approximately 90% compared to IDS-only systems. Latency overhead introduced by NBSIS averaged 12 ms per transaction, which remained within acceptable thresholds for exam delivery. System resilience was demonstrated by maintaining 98% uptime during simulated DoS attacks with 500 concurrent users. These measurable outcomes confirm that NBSIS strengthens security without compromising exam performance or user experience

Table 1. Comparative analysis table

Approach	Detection accuracy (%)	False positive rate	Response time	Usability for non-technical staff
IDS-only (Snort baseline)	82	High (15%)	Moderate	Low–requires technical expertise
SIEM-only (Splunk baseline)	88	Moderate (10%)	Slow (log-heavy)	Moderate–dashboards complex
Proposed NBSIS (pfSense+Snort+Splunk+AI)	95	Low (4%)	Fast (real-time alerts)	High–intuitive dashboard

Table 2. Comparative benchmarks

Approach	Detection accuracy (%)	False positives	Latency overhead	Resilience (DoS)
Firewall-only	70	Low	Low	Weak
IDS-only	82	High (15%)	Moderate	Moderate
SIEM-only	88	Moderate (10%)	High	Strong
Proposed NBSIS	95	Low (4%)	Moderate (12 ms)	Very strong (98% uptime)

8. CONCLUSION

This research contributes meaningfully to core computer science domains by advancing secure architectures for CBT. From a network security perspective, the integration of pfSense FW and Snort IDS demonstrates how layered defenses can be adapted to high-stakes educational environments. In AI, the deployment of anomaly detection models highlights the growing role of machine learning in predictive cybersecurity, reducing false positives and anticipating zero-day threats. Finally, the human-centered dashboard reflects principles of human-computer interaction, ensuring that complex security processes remain accessible to non-technical exam administrators. Together, these contributions position the NBSIS as both a technical innovation and a practical solution, bridging theory and application in computer science. By safeguarding exam integrity, confidentiality, and availability, NBSIS strengthens institutional trust and sets a foundation for future research in adaptive, AI-driven security systems for education and beyond.

Beyond its immediate application in safeguarding CBT platforms, the NBSIS framework is broadly relevant to ICT applications and distributed systems. Its layered architecture can be integrated into cloud-native infrastructures, enabling secure exam delivery across geographically dispersed centers. By leveraging distributed SIEM and AI-driven analytics, NBSIS supports scalability in environments where multiple servers and networks must coordinate in real time. This adaptability ensures resilience not only in education but also in corporate training and professional certification contexts. Furthermore, the system's modular design aligns with distributed computing principles, allowing institutions to deploy components incrementally based on their resources. In this way, NBSIS advances computer science research in cybersecurity, distributed systems, and ICT applications, while offering a practical solution for institutions seeking secure, scalable, and future-ready digital assessment environments.

NBSIS can be adopted by universities, certification bodies, and corporate training centers as part of their ICT infrastructure. Its modular design allows integration into cloud computing environments, enabling distributed exam delivery across multiple locations. For high-performance computing contexts, NBSIS can leverage parallel processing to handle large-scale traffic analysis, making it suitable for national-level certification exams. This scalability ensures that the framework remains relevant across diverse organizational scales and infrastructures.

Despite its strengths, the proposed NBSIS framework has limitations that must be acknowledged. First, deployment across smaller institutions may be constrained by the cost and technical requirements of SIEM infrastructure, limiting accessibility. Second, CBT centers in low-bandwidth or resource-constrained environments may experience delays in real-time monitoring and response. Third, the AI models integrated into NBSIS require continuous retraining with updated attack data to remain effective against evolving threats. This requirement may demand expertise not readily available in all organizations. Finally, while simulations demonstrated resilience under controlled conditions, further empirical testing in diverse real-world infrastructures are necessary to validate scalability and adaptability. Addressing these limitations will be critical to ensuring the framework's widespread adoption and long-term sustainability.

Based on this research, the following recommendations are proposed to enhance the effectiveness and sustainability of the NBSIS framework in CBT environments: i) institutional deployment: universities, certification boards, and corporate training centers should adopt the NBSIS as part of their core examination infrastructure to safeguard integrity and minimize disruptions from cyber-attacks; ii) continuous updates: security tools such as FW, IDS signatures, and AI models should be regularly updated and fine-tuned to remain effective against new and evolving threats; iii) training for non-technical staff: exam administrators and invigilators should receive periodic training on using a human-centered dashboard. This will improve confidence, speed, and accuracy in responding to incidents during live examinations; iv) scalability and stress testing: organizations should simulate real-world, high-traffic exam conditions before full rollout. This ensures that the system is resilient under pressure and capable of handling peak demand; and v) future research and innovation: scholars and practitioners should explore extending the framework with technologies such as blockchain for tamper-proof exam records, biometric authentication for secure logins, and cloud-native SIEM for scalability across distributed environments.

REFERENCES

[1] C. Pascoe, S. Quinn, and K. Scarfone, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST Cybersecurity White Paper 29, Gaithersburg, MD: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29.

[2] M. Nakip and E. Gelenbe, "Online self-supervised deep learning for intrusion detection systems," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 5668–5683, 2024, doi: 10.1109/TIFS.2024.3402148.

[3] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: a systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4150, Jan. 2021, doi: 10.1002/ett.4150.

[4] X. Liu, J. Liang, Q. Yan, M. Ye, J. Jia, and Z. Xi, "Cyber defense reinvented: large language models as threat intelligence copilots," *arXiv*:2502.20791, 2025.

[5] A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir, and Y. Rasheed, "A systematic review of online exams solutions in e-learning: techniques, tools, and global adoption," *IEEE Access*, vol. 9, pp. 32689–32712, 2021, doi: 10.1109/ACCESS.2021.3060192.

[6] S. Watini, G. Davies, and N. Andersen, "Cybersecurity in learning systems: data protection and privacy in educational information systems and digital learning environments," *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 26–35, Oct. 2024, doi: 10.33050/itee.v3i1.665.

[7] C. Boin, X. Guillaume, G. Grimaud, T. Groleat, and M. Hauspie, "One year of DDoS attacks against a cloud provider: an overview," in *2022 4th International Conference on Advances in Computer Technology, Information Science and Communications (CTISC)*, Apr. 2022, pp. 1–5, doi: 10.1109/CTISC54888.2022.9849755.

[8] T. Susnjak and T. McIntosh, "ChatGPT: the end of online exam integrity?," *Education Sciences*, vol. 14, no. 6, p. 656, Jun. 2024, doi: 10.3390/educsci14060656.

[9] N. Begou, J. Vinoy, A. Duda, and M. Korczyński, "Exploring the dark side of AI: advanced phishing attack design and deployment using ChatGPT," in *2023 IEEE Conference on Communications and Network Security (CNS)*, Oct. 2023, pp. 1–6, doi: 10.1109/CNS59707.2023.10288940.

[10] N. Kshetri, "Cybersecurity in higher education: the case of the United States," *Journal of Cybersecurity Education, Research and Practice*, vol. 2021, no. 1, p. 5, 2021.

[11] S. Han, S. Nikou, and W. Y. Ayele, "Digital proctoring in higher education: a systematic literature review," *International Journal of Educational Management*, vol. 38, no. 1, pp. 265–285, 2024, doi: 10.1108/IJEM-12-2022-0522.

[12] R. Butler-Henderson and J. Crawford, "A systematic review of online examinations: a pedagogical innovation for scalable authentication and integrity," *Computers & Education*, vol. 159, p. 104024, 2020, doi: 10.1016/j.compedu.2020.104024.

[13] Y. Xin *et al*., "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[14] M. Sarhan, S. Layeghy, M. R. Gallagher, and M. Portmann, "From zero-shot machine learning to zero-day attack detection," *International Journal of Information Security*, vol. 22, no. 4, pp. 947–959, 2023, doi: 10.1007/s10207-023-00676-0.

[15] W. Xu, M. J. Dainoff, L. Ge, and Z. Gao, "Transitioning to human interaction with AI systems: new challenges and opportunities for HCI professionals to enable human-centered AI," *International Journal of Human–Computer Interaction*, vol. 39, no. 8, pp. 1778–1794, 2023.

[16] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: a comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[17] B. W. O'Hara and B. C. O'Hara, *pfSense: the definitive guide*. Houston, TX: Reed Media Services, 2017.

[18] J. M. L. Velásquez, S. M. M. Monterrubio, L. E. S. Crespo, and D. G. Rosado, "SIEM-SC initial assessments: towards a Sustainable and Compliant proposal for Security Information and Event Management," *International Journal of Information Security*, vol. 24, no. 5, p. 195, Oct. 2025, doi: 10.1007/s10207-025-01109-w.

[19] OpenAI, "GPT-4 Technical Report," *arXiv*:2303.08774, 2023.

[20] National Institute of Standards and Technology, *Security and privacy controls for information systems and organizations*, NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: National Institute of Standards and Technology, Sep. 2020, doi: 10.6028/NIST.SP.800-53r5.

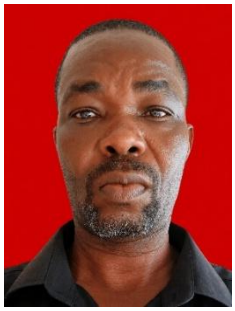
[21] M. Malatji, S. V. Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Information & Computer Security*, vol. 27, no. 2, pp. 233–272, Jun. 2019, doi: 10.1108/ICS-03-2018-0031.

[22] S. Mahmood, M. Chadhar, and S. Firmin, "Addressing cybersecurity challenges in times of crisis: extending the sociotechnical systems perspective," *Applied Sciences*, vol. 14, no. 24, p. 11610, Dec. 2024, doi: 10.3390/app142411610.

[23] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 27–49, Feb. 2015, doi: 10.1007/s11416-014-0231-x.

[24] B. Shneiderman, C. Plaisant, M. Cohen, S. Jacobs, N. Elmqvist, and N. Diakopoulos, *Designing the user interface: strategies for effective human–computer interaction*, 6th ed. Boston, MA: Pearson, 2016.

BIOGRAPHIES OF AUTHORS



Ajani Dele is a lecturer in the Department of Computer Science, School of Secondary Education (Science), Federal College of Education (Technical), Asaba, Nigeria. His research interests include network security, computer-based testing systems, and ICT applications in education. He can be contacted at email: dele.ajani@fcetasaba-edu.ng.

Owolabi Abdulhakim Adewale is a researcher in the Department of Computer Science, School of Secondary Education (Science), Federal College of Education (Technical), Asaba, Nigeria. His work focuses on cybersecurity frameworks, intrusion detection systems, and distributed computing for educational platforms. He can be contacted at email: abdulhakimowolabi@gmail.com.

Inaya Adesuwa is affiliated with the Department of Computer Science, School of Secondary Education (Science), Federal College of Education (Technical), Asaba, Nigeria. Her research interests include artificial intelligence applications in cybersecurity, human-computer interaction, and secure e-learning systems. She can be contacted at email: debbietupsy@yahoo.co.uk.