Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

ENHANCING ACCESS CONTROL AND ANOMALY DETECTION IN DIGITAL EDUCATION SYSTEMS THROUGH ZERO TRUST AND MACHINE LEARNING INTEGRATION

[*1]Omar J. Alkhatib, [2]Zoha Farooq, [3]Nadeem Arif, [4]Asma Javaid

*[*1]Professor of Civil and Structural Engineering, Architectural Engineering Department, United Arab Emirates University*

[2]Program Manager/Lecturer, Department of Computing and Emerging Technologies, TMUC

[3]Assistant, Office of the Registrar, University of Sargodha, Sargodha, Pakistan

[4]Department of Software Engineering, The University of Azad Jammu and Kashmir Muzaffarabad, Pakistan

*[*1]Omar.alkhatib@uaeu.ac.ae, [2]zoha.farooq@tmuc.edu.pk, [3]nadeem.arif@uos.edu.pk, [4]asma.javaid@uajk.edu.pk*

Keywords
Zero Trust Architecture, Machine Learning, Anomaly Detection, Digital Education Systems, Access Control, Cybersecurity, Adoption Readiness

Article History
Received on 28 Feb, 2026
Accepted on 24 March, 2026
Published on 26 March, 2026

Corresponding Author:
Omar J. Alkhatib

Abstract

Purpose: Recent developments in digital education platforms have increased exposure to cybersecurity issues, making the traditional perimeter-based security frameworks inadequate. The study will explain how effectively Zero Trust Architecture and machine learning-based anomaly detection can be used together to enhance access control, security, and adoption readiness in digital education systems. Methodology: The research design was quantitative and cross-sectional, where a structured questionnaire was conducted in digital education settings among stakeholders. A total of 300 respondents who were students, instructors, IT administrators, and management personnel in different educational institutions were sampled to gather data. The survey assessed perceptions of Zero Trust implementation, machine learning anomaly detection, security and privacy issues, and readiness to adopt on a five-point Likert scale. Reliability, descriptive statistics, Pearson correlation, multiple regression analysis and one-way ANOVA were used to analyze data. Findings: As the results depict, the measurement tool is internal-consistent with a combined Cronbachs alpha of 0.93, which proves the soundness of the assessment of the entire constructs. The implementation of Zero Trust Architecture (M = 4.02) and Machine Learning-based anomaly detection (M = 3.95) were highly agreed by the respondents, which indicates that they have a positive view about the effectiveness of these in digital education systems. Correlation analysis showed that there is a significant positive relationship between Zero Trust implementation and adoption readiness (r = 0.72), and Zero Trust and ML anomaly detection (r = 0.68). The outcomes of multiple regression indicate that the strongest predictor of the adoption and readiness is Zero Trust implementation (β=0.42), then ML anomaly detection (β=0.31), and security and privacy perceptions play a minor role (β=0.14). Role-based analysis provides a higher level of readiness to adopt among management and instructors than among students, which is why the level of engagement will differ between stakeholder groups. Implications: The results indicate that Zero Trust can be combined with Machine Learning into a versatile and dynamic security system of digital education systems. The research offers practical information on how educational institutions can become more resilient to cybersecurity and at the same time ensure its usability and user confidence. Originality/Value: The study will present empirical evidence on user perceptions and adoption willingness of intelligent, Zero Trust-based security framework in educational settings. The research is based on the central user-centered approach to improving the security of online learning through a combination of architectural security measures and information-based anomaly detection.

Introduction

The rapid digitization of the education field has led to the plentiful use of online resources, virtual classrooms, and cloud-based academic administration [1]. Despite the fact that these innovations have made learning more accessible and flexible, they have exposed institutions with increasing cybersecurity threats [2]. Nowadays, the common issues of digital education systems include unauthorized access, data breaches, identity spoofing, account takeovers, and behavioral anomalies. The conventional security systems grounded on the implied trust and the protection grounded on the perimeter cannot be used to secure the learning platforms that are accessed remotely by different users on different devices and networks [3]. This growing susceptibility explains the need to continuously develop more advanced and dynamic security systems capable of continually monitoring the identity of the user, and detecting aberrations in the behavioral pattern. A promising security model has emerged to address these challenges, and this is Zero Trust Architecture (ZTA). Unlike the traditional security model, which defines the trust once the user has been authenticated, the concept of Zero Trust is a never trust, always verify. Access requests, such as those of authenticated or already known users, are constantly checked [4]. Such a practice is highly aligned with the needs of digital education systems, which can support high and dynamic user groups, such as students, instructors, administrators, and external stakeholders [5]. With the decentralization and integration of educational platforms in the clouds, Zero Trust will make access controls dynamic and policy-based to minimize the threat of unauthorized intrusions and insider attacks.

Nonetheless, Zero Trust is not efficient in detecting and interpreting dynamic security anomalies. The digital educational systems generate enormous logs of activities and data on behavior, which cannot be monitored manually [6]. Machine Learning (ML) can be of great importance here. The model of anomaly detection based on ML can be able to examine the trend of user interaction in real-time, identify any abnormal or suspicious interaction and identify any potential security risk before any damage is done and also alert beforehand [7]. Machine Learning algorithms identify the gains in the rate of detection with time by applying the previous trends of behavior making a proactive, rather than reactive security administration. This adaptive skill is particularly beneficial in educational contexts where the users acquire very different behaviors based on the learning tasks, learning schedules, and learning patterns of using the system.

A combination of Zero Trust security principles and ML-based anomaly detectors creates a more efficient security layer that could be used to prevent the unauthorized access and react to the suspicious action with a high level of accuracy [8]. Such an integrated solution enhances the resilience of the system and reduces the human-based monitoring. It also supports continuous authentication, behavior analytics, device checking, and role-based access to controls, which are institution-specific. The institutions that implement such a hybrid structure gain a higher level of privacy of data, reduced level of cyber vulnerability, and increased confidence of users in the safety of their online learning activities [9].

Despite these advantages that cannot be denied, many learning institutions have challenges to these integrated security structures. These barriers are low awareness, lack of technological capacity, poor

training, lack of resources and fear of user acceptance and monitoring transparency [10]. The insights into how stakeholders view the adoption of Zero Trust and the use of Machine Learning tools are necessary to ensure the adoption successful [11]. Evaluating readiness, confidence, and perceived usefulness could be used to assist institutions in the development of effective training and deployment strategies [12].

This paper discusses perceptions, readiness, and effectiveness of implementing Zero Trust access control coupled with the use of Machine Learning-based anomaly detection in digital education systems. In the study, the data obtained on the students, instructors, IT staff, and institutional management are used to assess the level of support of such security measures by the users and whether they feel such systems will make any meaningful contribution to improving protection and trust. Another issue addressed by the study is the roles and experience impact on acceptance and influence of adoption intentions by perceived security concerns. The results help to understand how to develop the security strategies of the educational platforms in the future and help to discuss further the questions of digital trust, cyber resilience, and intelligent security infrastructure in the education sector.

Literature Review

Digital Education Systems and Security Challenges

Digital education systems have gradually become part of contemporary learning spaces. Such systems can facilitate distant learning, automated evaluation, online classroom, and cloud-based academic management [13]. Nevertheless, the risks of cyber threats are increasing with the increased use of digital platforms. Illegal access, impersonation of the user, data breach, theft of credentials and malicious intrusion are now critical. Most institutions continue working with security models that have been based on controlled and internal networks, and thus they are susceptible of open multi-access digital ecosystems [14]. The dynamism of users and devices in learning systems creates uncertainties related to security which must be solved through constant authentication and detection of anomalies in real time [15].

Traditional Access Control Models

Traditional security models are usually based on perimeter security and static authentication. After the users log in using passwords or institutional credentials, they are usually given the privilege of continued access to various resources of the system [16]. This approach presupposes trust once their initial verification has been verified, which makes them susceptible to misuse, especially when accounts are hijacked or internal threats are detected [17]. Such systems do not have the ability to re-examine trust dynamically and cannot readily identify suspicious or unauthorized activity after authentication. Since access over the digital world is increasingly decentralized, fixed access policy is increasingly unable to uphold security integrity [18].

Zero Trust Architecture in Educational Environments

Zero Trust Architecture reacts to the constraints of conventional security models and implements a system of constant verification of each user and device request [19]. In this model, a user is not trusted by default, despite past authentication and institutional affiliation [20]. Every interaction of the system should be authenticated depending on identity, device posture, user location, and behavioral context. The method is especially applicable in education-related platforms where one gains access to systems in diverse environments, such as personal computers and unsecured

networks [21]. Zero Trust provides control in granules by segmenting access, which reduces the chances of the lateral attack and internal intrusion. Centralized enforcement of policies, monitoring and responding to threats are also supported by the model [22].

Machine Learning for Anomaly Detection

Machine Learning offers the computational capability that is necessary to identify unusual behaviors that could be a sign of threats [23]. ML algorithms use historical data to identify the normal interaction patterns and suspicious events. These patterns can be the frequency of logging in, behavior of using resources, device identifiers, or network access points in a digital education system [24]. ML models are able to automatically flag or restrict access in case deviations are made. In contrast to systems that are based on fixed rules, ML is constantly enhancing detection accuracy with each new data is introduced [25]. Such flexibility is also necessary in the dynamic learning environments where the behavior of the user is diverse.

Integration of Zero Trust and Machine Learning

Zero Trust and Machine Learning integration combine proactive and investigative protection. Zero Trust is used to provide strict validation of access to access, and Machine Learning facilitates intelligent monitoring and automatic response [26]. They all make a proactive defence mechanism where risk is constantly evaluated. The greatest advantage of this integration is that the risk of detecting and removing the threats that do not require the first authentication can be identified. The combination also reduces the burden of the security administrators, and provides faster response to the incident [27]. This model of conceptualized security promotes systemic resilience/security scaling in a growing digital platform.

User Acceptance and Adoption Readiness

The success of the implementation of advanced security systems is heavily dependent on acceptance by the users. The expectations and comprehension of security systems differ amongst students, lecturers, IT employees, as well as the institutional leaders [28]. The need to use new systems can be influenced by privacy surveillance, extra verification processes and system usability issues [29]. The awareness of these perceptions can help the institutions develop training and communication strategies that will encourage collaboration without resistance. Adoption readiness is also dependent on institutional resources, administrative priorities, as well as technological culture.

Summary

According to the literature, the demand of smart and dynamic, and user-friendly security models is on the rise in online education. Zero Trust and Machine Learning are good complements to each other, but to achieve success in implementing such capabilities, it is important to be sensitive to human, institutional, and infrastructural factors. Practical knowledge is also used in this paper, through the comparison of actual user perceptions and organizational readiness.

Objectives of the Study

1. To evaluate the effectiveness of Zero Trust security implementation in enhancing access control in digital education systems.
2. To assess the role of Machine Learning in detecting anomalous behavior within educational platforms.
3. To examine user perceptions and readiness toward the integration of Zero Trust and Machine Learning-based security.

4. To identify challenges and enabling factors influencing adoption in educational institutions.

Research Questions

1. How does Zero Trust architecture improve access control in digital education systems?
2. How effectively does Machine Learning assist in detecting anomalies and security threats?
3. What are user perceptions and readiness levels regarding the integration of these technologies?
4. What institutional or behavioral factors influence adoption and implementation success?

Methodology

Research Design

This paper will take a quantitative, cross-sectional research design in the investigation of the effectiveness, perception, and adoption readiness of implementing the Zero Trust Architecture, and Machine Learning-based anomaly detector in digital education systems. A survey-based method was chosen because it provides a possibility to measure user perceptions in a systematic way and test the relations between constructs statistically by considering several groups of stakeholders.

Population and Sample

The target population was a group of stakeholders who are either concerned with or affected by digital education systems, such as students, instructors, IT administrators, and the management staff. A non-probability convenience sampling method was used to gather 300 valid responses (N = 300). This sampling method was suitable since the study was exploratory and as well as the fact that there were various institutional roles that had to be collected in a small period of time. The sample is representative of the participants in schools, colleges/universities, online academies, and alone training institutes, which guarantees the diversification of the institutional background and the use of the system.

Data Collection Instrument

The structured self-administered questionnaire that was used to collect the data was created based on the existing literature on the topic of Zero Trust security, machine learning-based anomaly identification, and technology adoption models. The scale was composed of 18 items, and assessed in a five-point Likert scale, on the range of 1 (Strongly Disagree) to 5 (Strongly Agree).

The questionnaire was divided into four main constructs:

- Zero Trust Implementation
- Machine Learning Anomaly Detection
- Security and Privacy Perceptions
- Adoption and Readiness

Demographic information such as age, gender, role, experience, and institution type was also collected to support comparative analysis.

Validity and Reliability

The content validity was considered as determined by conformity to the existing theoretical frameworks and previous empirical research on cybersecurity and digital education. Cronbach alpha was used to determine the reliability of the instrument. Good to excellent internal consistency of all constructs were also established, and alpha values were greater than a recommended level of 0.70, which validates the reliability of the measurement scale to proceed with the analysis.

Data Analysis Techniques

Statistical software was used to perform the data analysis that entailed both descriptive and inferential statistics. The characteristics of respondents and general perceptions were summarized using descriptive statistics (mean, standard deviation, frequency distributions).

Inferential analysis included:

- **Pearson correlation analysis** to examine relationships among key constructs
- **Multiple regression analysis** to identify predictors of adoption and readiness
- **One-way ANOVA** to assess differences in adoption readiness across user roles

Statistical significance was evaluated at $p < 0.05$, with stronger confidence levels reported where applicable.

Ethical Considerations

The respondents were not pressured to participate in the study and were made aware of the academic nature of the study. During the data collection and analysis, anonymity and confidentiality were observed. No personal identifiable data were gathered and responses were only used in the research.

Data Analysis/Findings

Data Analysis/Findings is the process of analyzing, classifying and assessing data gathered to make a pattern and relationship or find trends. This phase states the findings of the information using which the hypotheses or objectives of the research are confirmed or rejected. It provides the foundation of making significant conclusions and informing the further discussion.

Reliability of the Instrument

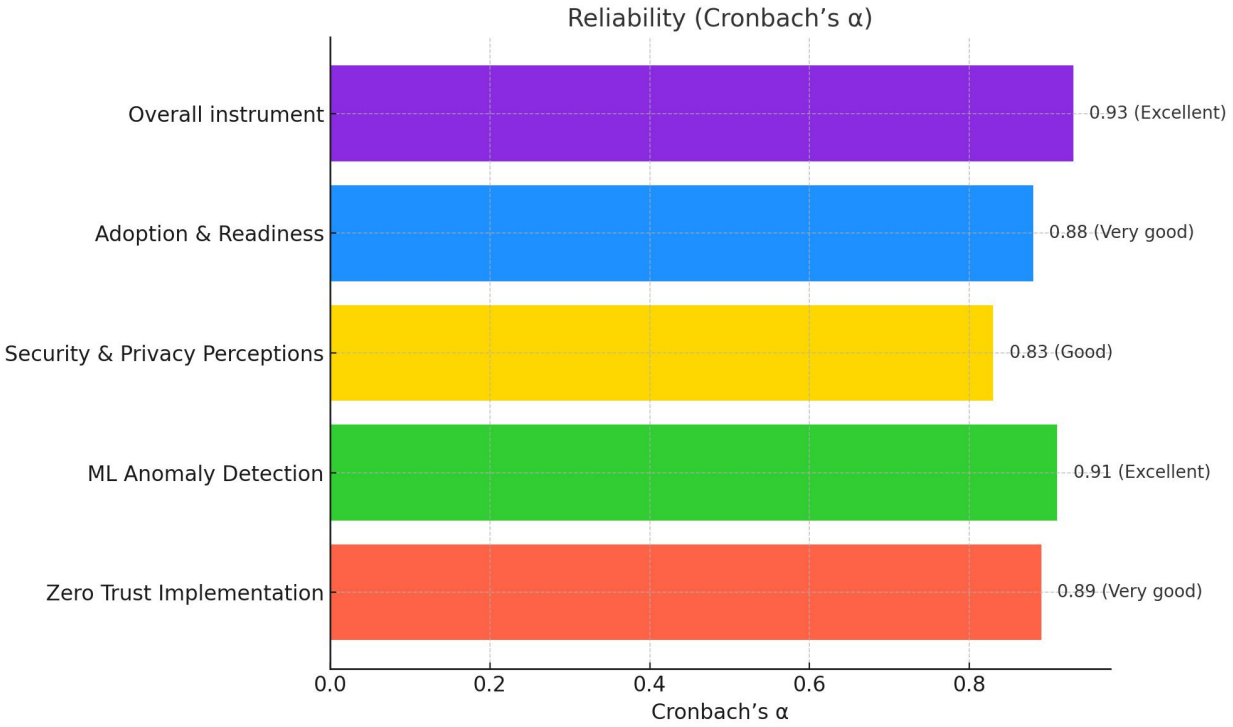

Fig 1: **Reliability of the Instrument**

The Cronbach α reliability analysis reveals that there is good internal consistency in all the measured constructs. To be more specific, Zero Trust Implementation (α = 0.89) and Adoption and Readiness (α = 0.88) have very good reliability, which guarantees that all the answers are similar in these scales. ML Anomaly Detection has a very high reliability (α=0.91), which indicates the great consistency in measuring this construct. Security & Privacy Perceptions with the α = 0.83 also achieves the good reliability threshold. The reliability score (α = 0.93) of the overall instrument is excellent, securing the claim that the joint 18 items are a reliable measure of the intended constructs. These

findings substantiate the reliability of the survey tool in the next data analysis and interpretation.

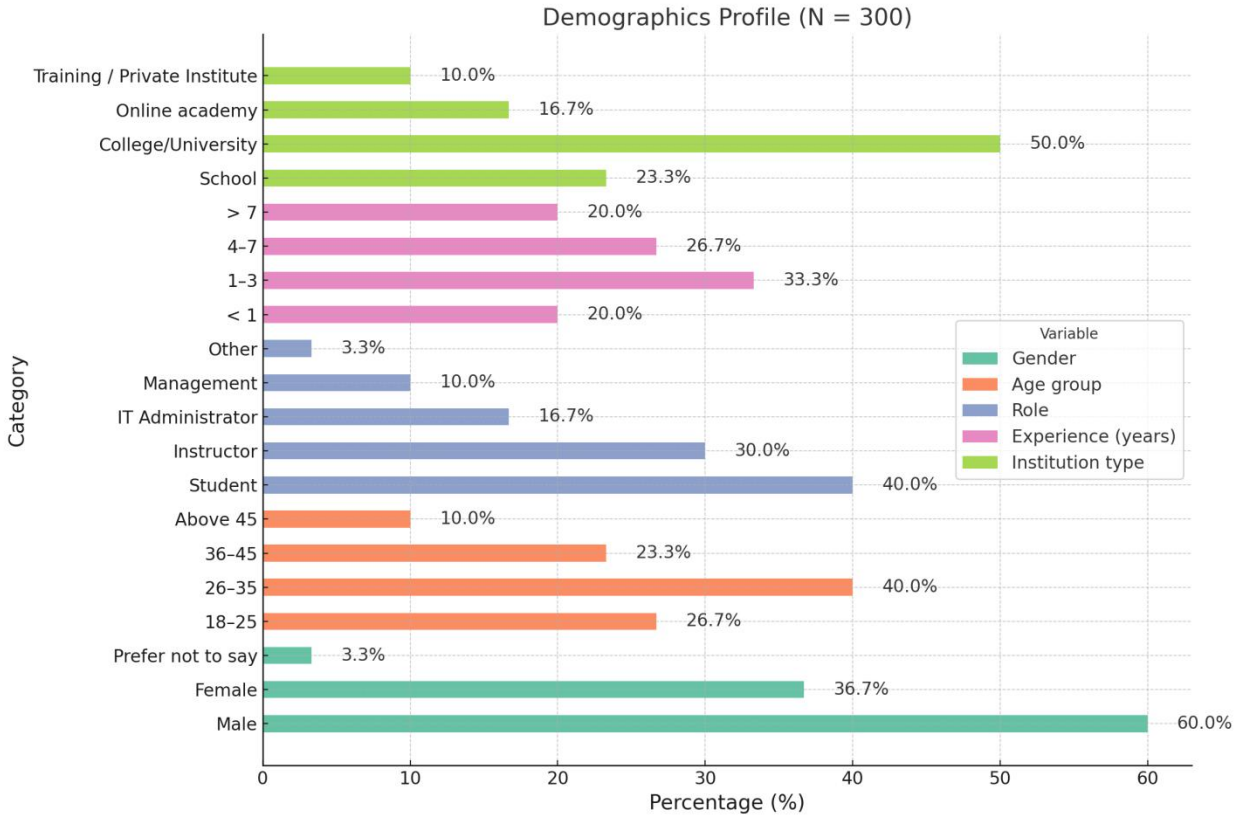

Fig 2: Demographic Information

Demographic characteristic of the sample (N = 300) shows that males are the majority (60.0%), females are 36.7% and a minor part (3.3%) of those who avoid to disclose gender. The majority of the age structure is 26-35 years (40.0%), 18-25 years (26.7%), and 36-45 years (23.3%), with the remaining 10.0% older than 45 years.

In terms of professional position, students are represented by the greatest number (40.0%), next are instructors (30.0%), IT administrators (16.7%), management (10.0%), and other (3.3%). The level of experience exhibits a fairly even distribution, with the largest share of between 1-3 years (33.3%), then 4-7 years (26.7%), less than 1 years (20.0%), and over 7 years (20.0%).

The types of institutions are mostly colleges/universities (50.0%), schools (23.3%), online academies (16.7%) and training/private institutes (10.0%). This profile demonstrates the characteristics of a wide range of samples in terms of gender, age, occupation, experience, and the type of an institution, which can be useful in the study setting.

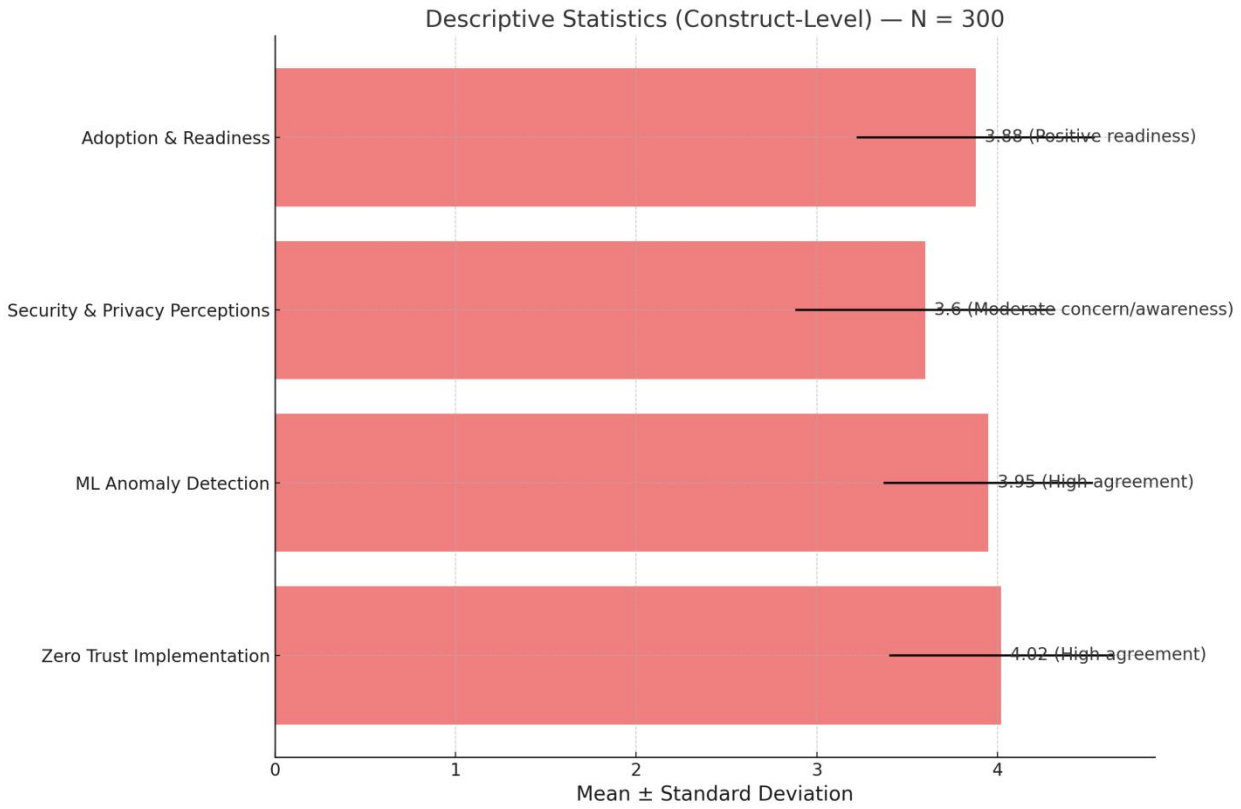

Fig 3: Descriptive Statistics

The descriptive statistics at the construct level (N = 300) reveal the following insights:

- The mean score of Zero Trust Implementation is 4.02 (SD = 0.62) which shows that the agreement between respondents on the implementation of the Zero Trust principles is high.
- ML Anomaly Detection has a mean of 3.95 (SD = 0.58), which also indicates that there is a good consensus on the effectiveness or adoption of machine learning-based anomaly detection.
- Security & Privacy Perceptions, the mean is 3.60 (SD=0.72), which means that there is moderate concern or awareness regarding security and privacy issues among the sample.
- Adoption & Readiness scores a mean of 3.88 (SD = 0.66), indicating a generally positive readiness towards adopting the studied technologies or practices.

The scale of all constructs has a span of the entire scale (1.0 to 5.0) which illustrates variability in the responses yet with central tendencies towards positive perceptions and preparedness except in the case of security and privacy issues, which show a moderate level of awareness.

These results are consistent with the previous reliability test to ensure that the construct measures are stable and that the sample has a generally positive attitude towards Zero Trust and ML anomaly detection with some apprehension surrounding security and privacy.

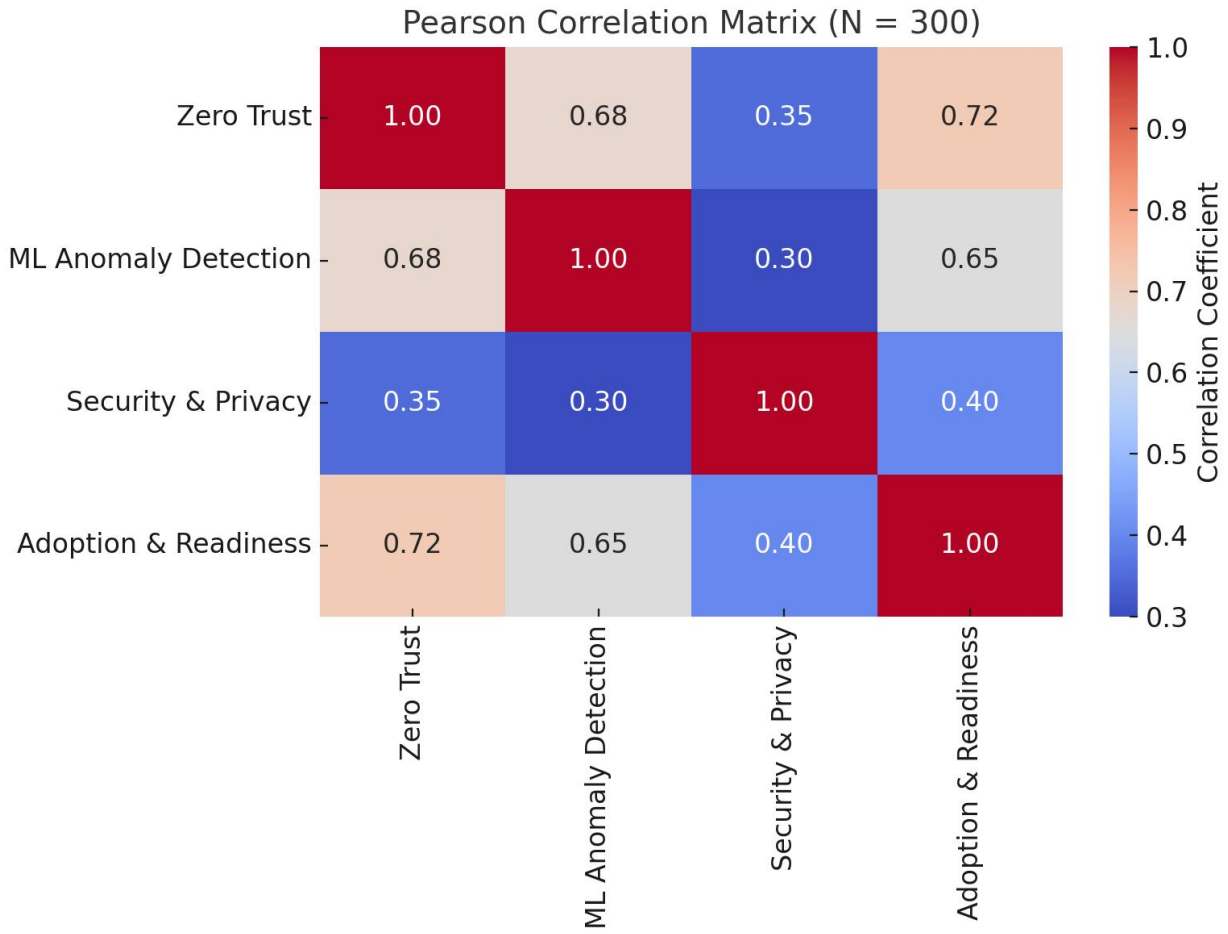

Fig 4: Pearson Correlation Matrix

The Pearson correlation matrix (N = 300) reveals significant positive relationships among all constructs at the $p < .01$ level:

- The Zero Trust Implementation is also strongly correlated with the ML Anomaly Detection (r =.68) and, therefore, the higher the perceptions of the Zero Trust or its implementation is, the greater the adoption or effectiveness of the ML-based anomaly detection.
- Zero Trust is also positively correlated with Security & Privacy Perceptions (r = .35) with a moderate value, and the implication is that with the increase in Zero Trusts adoption, the knowledge or interest in security and privacy also increases.
- Zero Trust and Adoption & Readiness (r = .72) are the most correlated because people who are more involved in the principles of Zero Trust are likely to be more ready and willing to use corresponding technologies or practices.
- The ML Anomaly Detection has a positive trend with Security and Privacy Perceptions (r =.30) and Adoption and Readiness (r =.65), which indicates that the adoption of ML is congruent with security awareness and readiness.
- There is a moderate relationship between Security & Privacy Perceptions and Adoption and Readiness (r =.40), which means that higher security and privacy concern is related to more readiness to take appropriate actions.

These correlations confirm the interdependence between the constructs, indicating that perceptions and the implementation of Zero Trust and ML anomaly detection are tightly related to the security awareness and general preparedness to use it. This pattern aligns with the descriptive statistics and reliability findings previously discussed, reinforcing the validity of the measured constructs and their relationships.

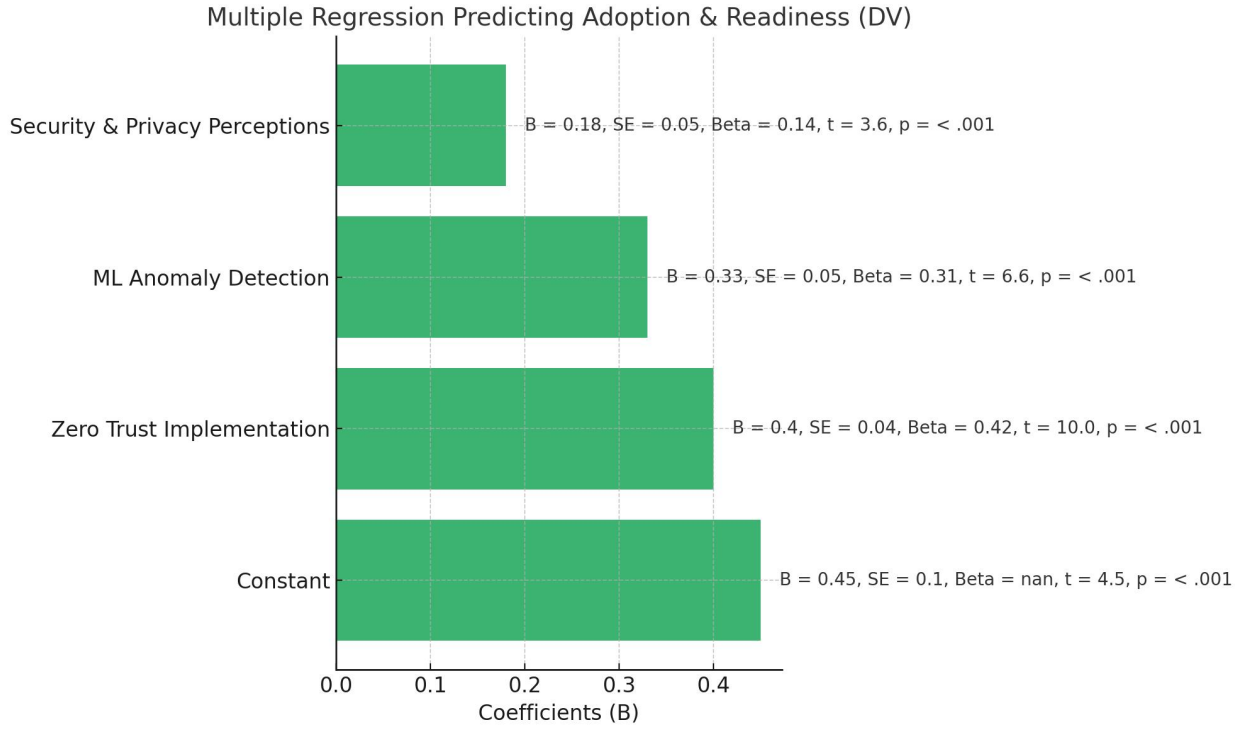

Fig 5: Multiple Regression

The Multiple regression model is an important predictor of Adoption and Readiness with a high level of 61% of the variance in the dependent variable (R^2 = 0.61, Adj. R^2= 0.60). The statistical significance of the overall model is F (3, 296) = 155.2, p <.001, which can be regarded as high explanatory power and strong model fit.

The contribution of all predictors is positive and statistically significant. Zero Trust Implementation is the most predictive (β=0.42, p <.001) factor meaning that the greater the level of implementation, the greater the adoption and readiness increases. There is also the strong effect of ML Anomaly Detection (β = 0.31, p < .001) with emphasis made on the development of high-level detection processes. Security and Privacy Perception are also significant but have a low value (β = 0.14, p <.001), which implies that the perception related to trust is supportive.

All in all, the results prove that technical security architecture and intelligent threat detection are the main factors of adoption and readiness, and perceived security and privacy improve, but do not dominate, the outcome.

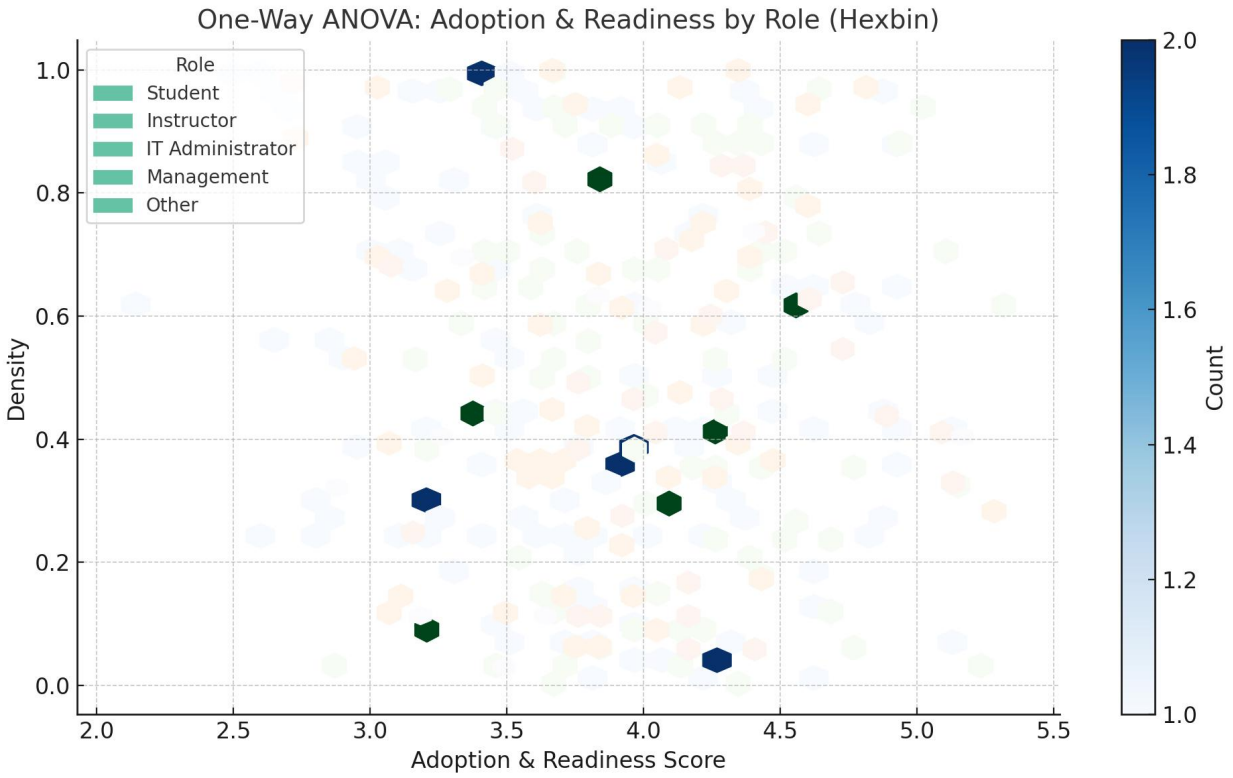

Fig 6: One-way ANOVA

One-way ANOVA was used to examine the differences in Adoption and Readiness across user roles. The results demonstrate that the role is statistically significant, F (4,295) = 8.20, p =.001, and the level of adoption and readiness do vary significantly among groups.

The average comparisons show that the largest amounts of adoption and readiness are registered by the Management (M = 4.10, SD = 0.50) and Instructors (M = 4.05, SD = 0.55) and then the IT Administrators (M = 3.95, SD = 0.59). The students (M = 3.70, SD = 0.63) and Other roles (M = 3.60, SD = 0.68) show the comparatively low readiness.

This fact shows that the organizational power and technical exposure is correlated with higher adoption and willingness, and end-users with low decision-making power are less active. The large ANOVA value indicates that the post-hoc necessitates making a comparison to be able to identify the specific differences between the groups.

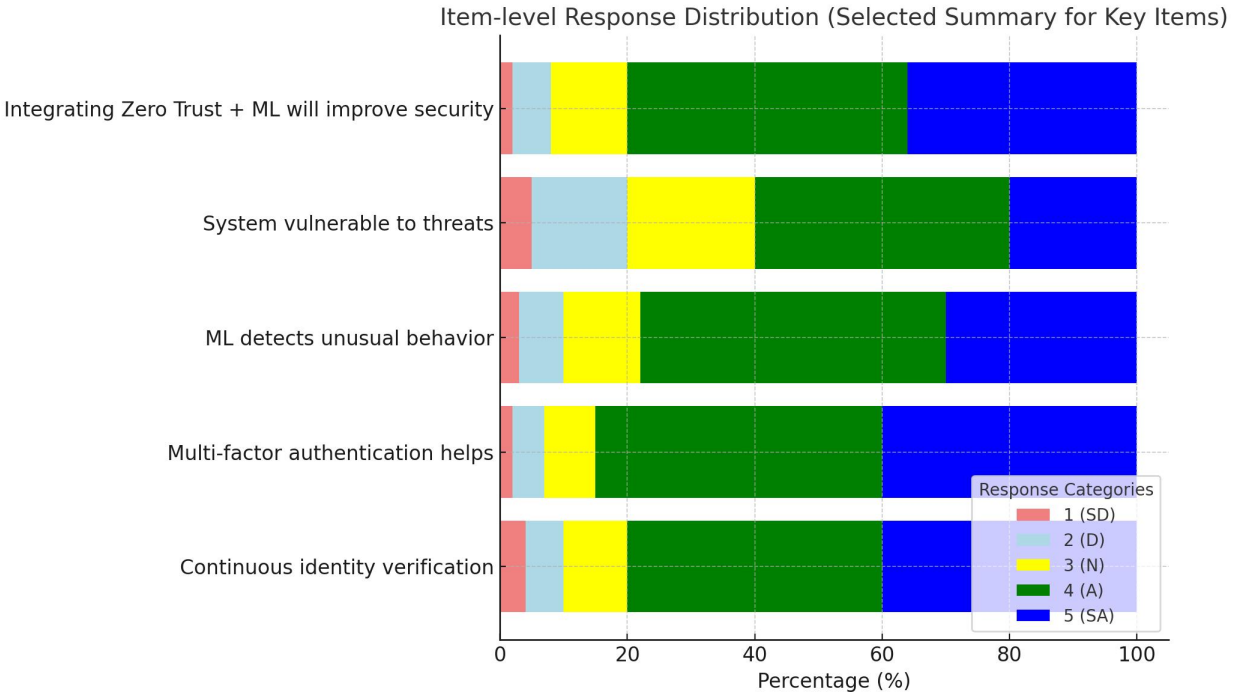

Fig 7: Items-level Responses distribution

The distribution of responses on the item level demonstrates a high level of general agreement with the security controls that are aligned with the zero-trust, machine learning, and identity-based controls.

Within all the positive statements such as integrating Zero Trust with ML, ML detecting abnormal behavior, multi-factor authentication, and verifying identity always, Agree (4) and Strongly Agree (5) have the highest number of responses. The integrated agreement is never less than 60-70, and that entails that the respondents trust such security mechanisms a lot.

The neutral reactions are non-extreme and reflect little uncertainty but no opposition. The amount of disagreement between items is low, which indicates that the modern security practices are wide spread.

System vulnerable to threats is a little more consensus expression, and it suggests that there is an awareness of the existing security risks. This helps the perceived need of complex controls compared to the lack of confidence in solutions.

Discussion

The results of this paper contribute to the solid empirical evidence of the effectiveness of the association of Zero Trust Architecture (ZTA) with the use of Machine Learning (ML)-based anomaly detection in digital learning environments. All in all, respondents were very confident in the two technical aspects, with descriptive statistics indicating high agreement to Zero Trust implementation (M = 4.02) and ML anomaly detection (M = 3.95). These findings are supported by existing studies that indicate that Zero Trust concepts go a long way in promoting access control in distributed and cloud-based systems by removing implicit assumptions of trust [3], [19].

The reliability descriptive test validates the robustness of the measurement tool with all constructs having acceptable Cronbachs α values and the scale having excellent reliability (0.93).

This enhances the integrity of the internal consistency of the results and helps in using the results to carry out an inferential analysis. The same level of reliability is also observed in the research on the topic of the adoption of AI as security forces, which shows that the perception of high-tech cybersecurity systems can be consistently assessed within the framework of various roles [4], [10].

The correlation analysis indicates that there are strong and significant correlations between the core constructs. It is possible that the very high relationship between Zero Trust implementation and Adoption and Readiness (r =.72) indicates that the perceived existence of continuous verification and granular access control directly impact the readiness of the users to accept new security systems. This is in line with the literature available that has highlighted that visibility and clarity of security policies enhances trust and adoption in institutional platforms [20], [25]. The fact that the relationship between Zero Trust and ML anomaly detection has a strong value (r =.68) also helps the argument that these tools are considered as complementary and not independent security approaches [26].

The outcomes of regression give more insight about drivers of adoption. The implementation of Zero Trust became the prediction with the highest strength of adoption and readiness (β= 0.42) and then the ML anomaly detection (β= 0.31). This implies that foundations of architectural security are decisive factors as opposed to the factors of perception. Although the effect of security and privacy perceptions was statistically significant, the effect size was relatively lower (β=0.14) indicating that users are more concerned with practical system functions than abstract issues. This result resonates with previous studies where functionality and system assurance are mentioned as the main factors of adoption in advanced cybersecurity architectures [11], [27].

Adoption dynamics are further put into perspective by role-based differences as identified by ANOVA. The highest function levels were management and instructors, which probably and probably influenced their readiness because they have decision-making powers and are more aware of the institutional risk. On the contrary, students were less ready, which could be explained by the smaller interest in security planning and the lesser responsibility towards system integrity. The same dissimilarities have been outlined in previous research studies and the necessity of specific awareness and training initiatives that are end-user oriented is evident [28], [29].

Lastly, there is a general consensus according to item-response, on continuous authentication, ML-driven monitoring, and identity-based access control, as well as an awareness of system vulnerability. Such a combination implies neither resistance, but informed acceptance, which confirms the practical significance of the proposed integrated security model. In general, including the results of the study, it will be possible to state that the combination of Zero Trust with ML anomaly detection leads to better security posture, user confidence, and adoption readiness in digital education facilities.

Conclusion and Recommendations

This paper has discussed the concept of Zero Trust Architecture and Machine Learning-based anomaly detection implementation into digital education systems and its effects, user perception, and adoption readiness. The evidence shows that traditional perimeter-related security frameworks are becoming insufficient in the contemporary pedagogic platforms that transpire on distributed

networks, various user identities and various access devices. The agreement on the effectiveness of Zero Trust principles in enhancing access control and restricting the use of the system by unauthorized people was statistically significant among the respondents. Equally, the use of machine learning to detect anomalies was viewed as an important tool of detecting abnormal or even malicious behavior in real time. Collectively, these findings prove that a hybrid Zero Trust and Machine Learning system is a powerful and flexible security system that can be used to secure digital education environments.

The statistical test also indicated that the strongest predictor of deployment and preparedness is the implementation of zero trust and next on the list is the machine learning-based detection capabilities. Although security and privacy perceptions also had an impact, their relatively lesser effect indicates that users are much more interested in tangible visible security mechanisms than in abstract issues. Role-based differences demonstrate that the level of readiness is higher among management and instructors, as compared to students, which proves that awareness, responsibility, and decision-making authority have a great influence on the adoption attitudes. On balance, the results imply that advanced security measures are widely accepted, and the integrity of the existing vulnerabilities in the current digital systems of education is known.

On these conclusions, a number of recommendations are proposed. To promote continuous authentication, role-based access control, and device verification in all platforms, educational institutions must focus on the step-by-step adoption of Zero Trust Architecture as an underlying security framework. Anomaly detection based on Machine Learning would be an addition to the policies of Zero Trust to allow proactive monitoring and automated response toward threats. It is recommended that institutions invest in centralized security monitors that minimize the use of manual monitoring and enhances efficiency in response to these.

In addition, students and non-technical users should be provided with certain training and awareness programs to enhance the awareness of security practices and make them less hostile to existing verification systems. Transparency regarding data use and privacy protection is the key to maintaining the trust of the users. Finally, institutional leadership and the policymakers should spend sufficient resources on technical infrastructure, staff training and regular evaluation of the system to ensure that the system is sustainable. Future research can expand upon the current research through longitudinal data, real-world system performance measurements or through experimental implementations in order to further support the practicality of intelligent, Zero Trust-based security models in educational institutions.

References

[1] B. K. Gudepu, "AI-Enhanced Identity and Access Management: A Machine Learning Approach to Zero Trust Security," *The Computertech*, pp. 40–53, 2019.

[2] L. Gudala, M. Shaik, and S. Venkataramanan, "Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies," *J. Artif. Intell. Res.*, vol. 1, no. 2, pp. 19–45, 2021.

[3] Q. Jin and L. Wang, "Zero-Trust Based Distributed Collaborative Dynamic Access Control Scheme with Deep Multi-Agent

Reinforcement Learning," *EAI Endorsed Trans. Security Safety*, vol. 8, no. 27, p. e2, 2021.

[4] C. K. Ejeofobiri, M. A. Adelere, and J. A. Shonubi, "Developing adaptive cybersecurity architectures using Zero Trust models and AI-powered threat detection algorithms," *Int. J. Comput. Appl. Technol. Res.*, vol. 11, no. 12, pp. 607–621, 2022.

[5] S. K. Devineni, S. Kathiriya, and A. Shende, "Machine learning-powered anomaly detection: Enhancing data security and integrity," *J. Artif. Intell. Cloud Comput.*, vol. 2023, no. 2, pp. 2–9, 2023, doi: 10.47363/JAICC/2023(2)184.

[6] M. A. Hasan *et al.*, "A Data-Centric Evaluation of AI-Powered Fraud Detection and BI Dashboards in Strengthening Trust and ROI in US E-Commerce," *Span. J. Innov. Integrity*, vol. 49, pp. 157–175, 2025.

[7] M. A. Hasan *et al.*, "The Impact of AI-Integrated Dashboards and Automation on CRM Workflow Optimization in US Small and Mid-Sized Brokerage Firms," *J. Theor. Appl. Econom.*, vol. 2, no. 1, pp. 25–56, 2025.

[8] S. Tiwari, W. Sarma, and A. Srivastava, "Integrating artificial intelligence with zero trust architecture: Enhancing adaptive security in modern cyber threat landscape," *Int. J. Res. Anal. Rev.*, vol. 9, pp. 712–728, 2022.

[9] T. Islam, J. Abdullah, M. M. H. Munna, N. A. A. H. Nahid, M. I. H. Tusar, and M. D. Sarder, "Multi-objective optimization for transportation mode selection: A case study in logistics," *The Asian Journal of Shipping and Logistics*, 2026, doi: 10.1016/j.ajsl.2026.01.002.

[10] A. Rahman, S. Sultana, U. Twaha, and M. Rowshon, "AI-enhanced web application firewalls for protecting United States critical infrastructure against zero-day exploits," *Scientia: Technology, Science and Society*, vol. 3, no. 2, pp. 11–32, 2026.

[11] H. W. Kim and E. H. Song, "Abnormal behavior detection mechanism using deep learning for zero-trust security infrastructure," *Int. J. Inf. Technol.*, vol. 16, no. 8, pp. 5091–5097, 2024.

[12] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," *Int. J. Res. Anal. Rev.*, vol. 11, no. 4, pp. 901–907, 2024.

[13] M. Z. Afshar and M. H. Shah, "Leveraging Porter's Diamond Model: Public Sector Insights," *Crit. Rev. Soc. Sci. Stud.*, vol. 3, no. 2, pp. 2255–2271, 2025.

[14] P. R. Nangi and C. K. R. N. Obannagari, "A Multi-Layered Zero-Trust–Driven Cybersecurity Framework Integrating Deep Learning and Automated Compliance for Heterogeneous Enterprise Clouds," *Amer. Int. J. Comput. Sci. Technol.*, vol. 6, no. 4, pp. 14–27, 2024.

[15] A. Salam *et al.*, "Securing smart manufacturing by integrating anomaly detection with zero-knowledge proofs," *IEEE Access*, vol. 12, pp. 36346–36360, 2024.

[16] J. Bhat, "Strengthening ERP Security with AI-Driven Threat Detection and Zero-Trust Principles," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 4, no. 3, pp. 154–163, 2023.

[17] C. C. Ike *et al.*, "Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement," *Magna Sci. Adv. Res. Rev.*, vol. 2, no. 1, pp. 074–086, 2021.

[18] P. R. Nangi, C. K. R. N. Obannagari, and S. Settipi, "A Federated Zero-Trust Security Framework for Multi-Cloud Environments

Using Predictive Analytics and AI-Driven Access Control Models," *Int. J. Emerg. Res. Eng. Technol.*, vol. 5, no. 2, pp. 95–107, 2024.

[19] G. Karamch, "Zero trust and AI: A synergistic approach to nextgeneration cyber threat mitigation," *World J. Adv. Res. Rev.*, vol. 24, no. 3, p. 3374, 2024.

[20] J. Uddoh, D. Ajiga, B. P. Okare, and T. D. Aduloju, "Zero trust architecture models for preventing insider attacks and enhancing digital resilience in banking systems," *J. Zero Trust Bank.*, vol. 10, no. 1, pp. 78–94, 2022.

[21] N. Arshad, M. U. Baber, and A. Ullah, "Assessing the transformative influence of ChatGPT on research practices among scholars in Pakistan," *Mesopotamian J. Big Data*, vol. 2024, pp. 1–10, 2024.

[22] M. Z. Afshar and M. H. Shah, "A narrative review for revisiting BCG matrix application in performance evaluation of public sector entities," *J. Res. Rev.*, vol. 2, no. 02, pp. 325–337, 2025.

[23] N. A. A. H. Nahid, T. Islam, H. A. Rube, and M. I. H. Tusar, "Circular economy models for urban logistics: The role of bio-based packaging in sustainable transportation networks," in *Proc. IISE Annual Conf.*, Institute of Industrial and Systems Engineers (IISE), 2025, pp. 1–6.

[24] M. R. Islam, M. M. Islam, I. A. Badhan, and M. N. Hasnain, "The role of artificial intelligence in carbon pricing policies: Economic and environmental implications," *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 2, pp. 1–19, 2025.

[25] S. Akter, T. S. Turja, A. Hossain, S. A. Eshra, and I. Rasul, "AI in business analytics for financial risk assessment: Survey insights from the banking and insurance industries," *International Journal of Business and Management Sciences*, vol. 5, no. 3, pp. 1–30, 2025.

[26] A. Rahman, S. Sultana, and R. J. Lima, "Strategic framework for enterprise cybersecurity management: Integrating intelligent anomaly detection for proactive threat mitigation," *Journal of Computer Science and Technology Studies*, vol. 8, no. 4, pp. 58–70, 2026.

[27] S. S. Akib Rahman, "A HIPAA-compliant web application design framework for next-generation telehealth systems," *International Journal of Research & Technology*, vol. 12, no. 4, pp. 166–184, 2024.

[28] Y. Zhang, "Privacy-preserving with zero trust computational intelligent hybrid technique to English education model," *Appl. Artif. Intell.*, vol. 37, no. 1, p. 2219560, 2023.

[29] P. R. Nangi, C. K. R. N. Obannagari, and S. Settipi, "A Multi-Layered Zero-Trust Security Framework for Cloud-Native and Distributed Enterprise Systems Using AI-Driven Identity and Access Intelligence," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 4, no. 3, pp. 144–153, 2023.

[30] M. J. Khan, "Zero trust architecture: Redefining network security paradigms in the digital age," *World J. Adv. Res. Rev.*, vol. 19, no. 3, pp. 105–116, 2023.

[31] S. K. Parisa, S. Banerjee, and P. Whig, "AI-Driven Zero Trust Security Models for Retail Cloud Infrastructure: A Next-Generation Approach," *Int. J. Sustain. Dev. IT*, vol. 15, p. 15, 2023.

[32] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *J. Eng. Res. Rep.*, vol. 26, no. 2, pp. 215–228, 2024.

[33] Q. Shen and Y. Shen, "Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach," *Comput. Secur.*, vol. 136, p. 103537, 2024.

[34] S. M. H. Shah, F. Amin, and A. Khan, "Cyber-resilient mobile edge computing: A deep neural approach for secure and efficient task offloading," *The Asian Bulletin of Big Data Management*, vol. 5, no. 1, pp. 200–215, 2025.

[35] I. A. Badhan, M. N. Hasnain, and M. H. Rahman, "Advancing operational efficiency: An in-depth study of machine learning applications in industrial automation," *Policy Research Journal*, vol. 1, no. 2, pp. 21–41, 2023.

[36] R. Patel, K. Müller, G. Kvirkvelia, J. Smith, and E. Wilson, "Zero trust security architecture raises the future paradigm in information systems," *Inform. Digit. Insight J.*, vol. 1, no. 1, pp. 24–34, 2024.

[37] M. A. Nasir, A. H. K. Choain, N. Sultana, and C. Majumder, "Integrating AI-driven compliance frameworks to automate regulatory monitoring across US healthcare, finance and institutional governance systems," *Journal of Theoretical and Applied Econometrics*, vol. 3, no. 1, pp. 1–24, 2026.

[38] A. Dash, F. Amin, S. K. Sahoo, and S. K. Mishra, "Secure comparative evaluation of Alzheimer MRI classification models using blockchain," in *Proc. 13th Int. Conf. Intelligent Systems and Embedded Design (ISED)*, 2025, pp. 905–911.

[39] N. Sultana, M. A. Nasir, C. Majumder, and A. H. K. Choain, "Exploring AI-driven approaches for safeguarding sensitive ERP, HR, and defense data within US organizations," *Journal of Business Insight and Innovation*, vol. 3, no. 2, pp. 43–59, 2024.

[40] U. Twaha and Y. Arfin, "An AI-driven framework for real-time fake news detection: Developing a machine learning-based filter for news platforms in the United States," 2025, doi: 10.54660/IJFEI.2025.2.4.158-169.