SISTEKINFO
JURNAL SISTEM DAN TEKNOLOGI INFORMASI
e-ISSN : 3109 6522

Volume 2 • Number 2 • September 2025 • 81 - 86

DESIGNING INFORMATION TECHNOLOGY INFRASTRUCTURE BASED ON ZERO TRUST ARCHITECTURE TO IMPROVE CAMPUS DATA SECURITYM

Naufal Aditya Putra[1] , Isa Faqihuddin Hanif[2], Sandy Gio Alanza[3]

[123]Information Systems and Technology Study Program, Faculty of Industrial Technology and Informatics, Muhammadiyah University Prof. Dr. HAMKA

Received: January 10, 2026 Accepted: January 10, 2026 Published: January 10, 2026

Abstract

Virtual transformation in better education has accelerated establishments' dependence on facts technology infrastructure in dealing with instructional statistics, management, and research. This condition is observed via an growth in cyber threat risks due to machine complexity, person mobility, and the use of more than one gadgets. traditional perimeter security is considered ineffective in handling the dynamics of modern cyber threats on campus. This have a look at ambitions to design an trouble-based totally generation infrastructure the usage of zero trust structure with a view to enhance campus data safety. The technique used is design science studies the usage of a structured literature look at approach to cybersecurity standards, specially NIST unique publication 800-207, and relevant previous studies. The consequences of this take a look at are a conceptual layout of a 0 agree with structure that consists of identity and get entry to control, network segmentation, endpoint protection, and centralized safety monitoring. The proposed layout is wanted to minimize the chance of illegal access, boom safety visibility, and support access flexibility in the contemporary campus surroundings. This research affords conceptual contributions to the implementation of 0 believe structure as an adaptive and sustainable information security tactic for better education establishments.

Keywords: Zero Trust Architecture, data security, information technology infrastructure, network security, campus system issues.

INTRODUCTION

Digital transformation in higher education has notably modified the manner instructional and administrative offerings are brought. modern-day universities now operate as digital entities that manage and save a huge style of important information, consisting of student educational records, strategic studies consequences, institutional monetary data, and other highbrow assets. The excessive dependence on records technology has resulted in better training establishments turning into inclined goals for numerous cyber threats. in keeping with the NIST special book 800-207 (2020) report, the education quarter is classified as an organization with a high stage of vulnerability because of the complexity of its technological infrastructure and the variety of customers and devices related to the machine.

conventional security fashions that depend upon a perimeter security technique have established an increasing number of ineffective in addressing the dynamics of current cyber threats. This approach assumes that threats most effective originate from outside the community, and as a result, it is less able to accommodate the necessities of the trendy campus environments, that are characterised through excessive person mobility, using personal gadgets (deliver Your very own device), and the implementation of hybrid paintings and gaining knowledge of styles. these situations amplify the scope of aggression and boom the chance of unauthorized get entry to to campus structures and information.

In reaction to the constraints of conventional protection models, the concept of 0 trust architecture (ZTA) has emerged as a more adaptive and comprehensive cybersecurity paradigm. 0 consider structure carries the primary principle of "never consider, always verify," in which each get right of entry to request ought to undergo a strict verification technique irrespective of region, tool, or consumer traits. This method emphasizes the importance of continuous verification, minimal access rights regulations, and the assumption that safety breaches can occur at any time. therefore, the implementation of zero believe architecture is a applicable strategic technique to increase statistics protection and cyber resilience in data generation infrastructure in the campus environment.

METHODS

The implementation of zero agree with architecture (ZTA) in a campus environment calls for a based and phased approach. that is because of the complexity of the facts era infrastructure and the range of the systems and users concerned. referring to the NIST unique ebook 800-207 framework, there are numerous number one additives that form the muse for the implementation of 0 trust structure in higher training institutions.

FINDINGS AND DISCUSSION

To make certain the a success and sustainable implementation of 0 consider architecture (ZTA), better training establishments need to undertake implementation control strategies that focus no longer most effective on era, but also on human sources and governance. The proper strategic technique will help establishments reduce the danger of implementation failure and maximize the benefits of imposing 0 agree with architecture.

CONCLUSION

The implementation of 0 believe architecture in campus information era infrastructure is no longer simply an alternative, but a strategic necessity in facing an increasingly complex and dynamic cyber danger landscape. The high dependence of higher education institutions on virtual structures, coupled with the range of users and gadgets, demands a protection method that is able to presenting adaptive and continuous information protection. 0 agree with architecture provides a applicable security framework via the utility of continuous verification principles, get right of entry to rights restrictions, and comprehensive machine activity monitoring.

The a hit implementation of 0 agree with structure requires a comprehensive approach that takes into account era, techniques, and human assets. Institutional coverage support, periodic implementation management, and inner capability enhancement are key factors in constructing a strong cybersecurity posture. With strong organizational commitment, universities can enhance their cybersecurity resilience while making sure the continuity of instructional offerings and information safety amid the demanding situations of future virtual transformation.

REFERENCES

National Institute of Standards and Technology. (2020). Zero Trust Architecture. NIST Special Publication 800-207.

Kindervag, J., et al. (2020). The Zero Trust Evolution: Building the Cybersecurity Foundation for Digital Transformation. Forrester Research.

Alohali, M., et al. (2022). Cybersecurity Challenges in Higher Education Institutions: A Comprehensive Analysis. Computers & Security Journal.

Chowdhury, N., et al. (2021). Implementing Zero Trust in Educational Environments: A Framework for Success. Journal of Educational Technology Systems.

Smith, P., et al. (2023). Zero Trust Implementation Challenges: Lessons from Early Adopters. IEEE Security & Privacy.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology.

Zhang, Q., Chen, M., Li, L., & Zhou, X. (2021). A survey on Zero Trust Architecture: Challenges and future directions. IEEE Access, 9, 145241–145257.

Ferraiolo, D. R., Kuhn, D. R., & Chandramouli, R. (2019). Role-Based Access Control. Artech House.

Behl, A., & Behl, K. (2017). Cyberwar: The Next Threat to National Security and What to Do About It. Oxford University Press.

Alasmary, W., Alhaidari, F., & Alghamdi, A. (2022). Cybersecurity challenges in higher education institutions: Threats and mitigation strategies. International Journal of Information Security Science, 11(3), 45–58.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, 177–191.

Pendergast, M., & Rhoads, R. (2018). Cybersecurity education in higher education institutions. Journal of Higher Education Policy and Management, 40(3), 213–229.

Cloud Security Alliance. (2021). Zero Trust Guidance. Cloud Security Alliance.

Gartner. (2022). Market Guide for Zero Trust Network Access. Gartner Research.

ISO/IEC. (2018). ISO/IEC 27001: Information Security Management Systems — Requirements. International Organization for Standardization.