Zero Trust Architecture for Cloud and Network Security: A Next-Generation Approach to Access Control

Publisher: IEEE Cite This PDF

Ramakrishnan. B ; C. Meenakshi All Authors

Abstract:
The adoption of cloud computing and network infrastructure demands security frameworks that surpass simplistic perimeter-based approaches. Zero Trust Architecture (ZTA) prevents unauthorized access through its procedures for real-time user verification and its strict limitations on system entry. The research assesses four machine learning models for zero trust anomaly detection, which include Random Forest with 96.48% accuracy, XGBoost at 95.23% alongside KNN at 77.39%, and AdaBoost at 67.84%. Random Forest, together with "XGBoost, demonstrates superior performance than KNN and AdaBoost when assessing AUC scores that reach 1.00 and 0.99. The study findings demonstrate weak security through passwords that emphasize why multiple authentication factors and biometric solutions are needed for systems protection. The research establishes tree-based methods as optimal choices for establishing zero-trust security deployments. Keywords: Zero Trust Architecture, Cloud Security, Network Security, Machine Learning, Anomaly Detection, Access Control, Random Forest, XGBoost, Authentication Methods, Multi-Factor Authentication, Biometric Security, AUC-ROC, Cyber Threats, Data Protection, Zero Trust Framework

Published in: 2025 International Conference on Biomedical Engineering and Sustainable Healthcare (ICBMESH)

Date of Conference: 08-09 August 2025

DOI: 10.1109/ICBMESH66209.2025.11182246

Date Added to IEEE *Xplore*: 01 October 2025

Publisher: IEEE

ISBN Information:

Conference Location: Manipal, India

Metrics