INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-695 PAGE NO: 008-013

A ZERO-TRUST SECURITY FRAMEWORK WITH CONTINUOUS AUTHENTICATION FOR SECURE SYSTEMS

E.Swathi
Scholar,
Department of Computer Application,
A.V.V.M. Sri Pushpam College (Autonomous),
Tiruvallur, Tamil Nadu, India.

Dr. D. Ragupathi
Head of the Department,
Department of Computer Applications,
A.V.V.M. Sri Pushpam College (Autonomous),
Tiruvallur, Tamil Nadu, India.

Abstract

Traditional perimeter-based security models are increasingly inadequate in protecting modern distributed systems. This paper presents a zero-trust security model implemented through continuous authentication mechanisms. The proposed framework continuously evaluates user identity and device behavior using contextual and behavioral attributes rather than relying on one-time authentication. Machine learning techniques are employed to dynamically assess trust levels and enforce adaptive access control policies. Experimental analysis indicates that continuous authentication significantly reduces unauthorized access risks while maintaining usability. The proposed zero-trust model provides a robust security foundation for cloud and enterprise environments.

Keywords: Zero-Trust, Continuous Authentication, Adaptive Access Control, Behavioral Biometrics, Cybersecurity, Risk Assessment.

1. Introduction

With the rapid growth of cloud computing, remote work environments, and distributed enterprise networks, traditional perimeter-based security models have become increasingly ineffective. Conventional security approaches assume that users and devices inside the network can be trusted, which creates significant vulnerabilities when attackers gain internal access. To address these challenges, the Zero-Trust Security Model has emerged as a modern and robust security paradigm that operates on the principle of "never trust, always verify".

The Zero-Trust model eliminates implicit trust by continuously validating the identity, device posture, and behavior of users and systems, regardless of their location within or outside the network. One of the most critical components of Zero-Trust architecture is continuous authentication, which goes beyond one-time login verification. Continuous authentication monitors user behavior, access patterns, device health, and contextual factors to ensure that access remains legitimate throughout a session.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-695 PAGE NO: 094-098

This project focuses on implementing a Zero-Trust Security Model using continuous authentication mechanisms to enhance protection against insider threats, credential theft, and advanced persistent attacks. By leveraging real-time monitoring, adaptive access control, and behavioral analysis, the system dynamically evaluates trust levels and enforces security policies accordingly. The proposed approach aims to improve security resilience, minimize unauthorized access, and ensure secure access to critical resources in modern, dynamic network environments.

The motivation for this project arises from the increasing complexity of modern IT environments and the growing number of cyber threats targeting organizations. Traditional security models rely heavily on perimeter defenses and assume that users inside the network can be trusted, which often leads to severe security breaches when attackers gain internal access. With the widespread adoption of cloud services, remote work, and bring-your-own-device (BYOD) policies, network boundaries have become blurred, making conventional security approaches ineffective.

Continuous authentication strengthens Zero-Trust by constantly monitoring user behavior, device health, and contextual factors throughout a session. This project is motivated by the need to design a proactive and adaptive security solution that minimizes risk, enhances trust evaluation, and provides stronger protection against evolving cyber threats. By combining identity verification, behavioral analysis, and adaptive access control, the project enhances security and ensures reliable access to critical systems.

Literature Survey:

John Kindervag introduced the foundational concept of Zero-Trust Network Architecture (ZTNA) in 2010, challenging the traditional perimeter-based security approach. The study emphasizes that trust should never be assumed based on network location and instead advocates strict identity verification for every access request. Key principles such as least-privilege access, micro-segmentation, and continuous verification were highlighted as central to this new paradigm.

The National Institute of Standards and Technology (NIST) provides a comprehensive and standardized framework for implementing Zero-Trust Architecture through SP 800-207. This publication defines core components such as policy engines, policy enforcement points, and continuous monitoring mechanisms. It strongly emphasizes continuous verification of identity, device health, and contextual attributes before granting or maintaining access.

Teixeira et al. explored continuous authentication specifically through behavioral biometrics such as keystroke dynamics, mouse movement, and user interaction patterns. The authors demonstrated that continuous authentication can significantly reduce the risk of session hijacking and unauthorized access. The work highlights the advantages of transparent authentication mechanisms that operate without disrupting user experience.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-695 PAGE NO: 094-098

Rose et al. provided a practical discussion on the evolution of Zero-Trust from theory to enterprise deployment. Their research analyzed real-world use cases and highlighted the importance of identity-centric security and continuous assessment of trust. The study emphasized that authentication should not be a one-time process but must adapt dynamically based on behavior and risk.

Fagan and Khan proposed an adaptive access control framework that integrates continuous authentication into Zero-Trust environments. They used contextual data such as location, device posture, and user behavior to dynamically adjust access privileges. Their system demonstrated improved resistance to insider threats and credential compromise attacks, showing reduced unauthorized access incidents compared to static systems.

Methodology

The proposed system implements a Zero-Trust Security Model using Continuous Authentication to overcome the limitations of traditional security approaches. In this system, no user or device is trusted by default, regardless of their location or prior authentication status. Every access request is verified continuously using multiple parameters such as user identity, behavioral patterns, device posture, and contextual information.

The system architecture is divided into several specialized modules, starting with the Access Request & Identity Verification Module. This module handles initial access requests and verifies user credentials using secure authentication methods like MFA or biometric validation. It validates user identity against centralized repositories before granting any initial access, ensuring no user is trusted by default.

The Device Validation & Context Evaluation Module assesses the security posture of the device requesting access. It checks parameters such as device type, OS version, security patches, and antivirus status. Additionally, it considers contextual factors like geographic location, IP address, and network type to prevent compromised devices from accessing sensitive resources.

The Continuous Authentication & Behavior Monitoring Module maintains security throughout an active session. It monitors user behavior such as keystroke patterns, access frequency, and resource usage in real time. Any deviation from established normal behavior patterns is detected immediately, helping to identify session hijacking or insider threats without interrupting the user experience.

Finally, the Risk Assessment & Adaptive Access Control Module calculates a dynamic risk score by aggregating data from the previous modules. Based on this risk score, the module adaptively grants, restricts, or revokes access privileges. High-risk activities trigger immediate restrictions, ensuring that access control decisions are always current and aligned with Zero-Trust principles.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-695 PAGE NO: 094-098

Results and Discussion

Experimental analysis indicates that continuous authentication significantly reduces unauthorized access risks while maintaining usability. The system was implemented using Python in a Google Colab environment to test the efficiency of the trust scoring algorithms. Snapshots of the implementation show that the authentication success rate increases over time as the system stabilizes and accurately identifies legitimate users.

The device trust level distribution confirms that most devices fall within the moderate to high trust range, complying with set security policies. This posture assessment effectively filters out compromised or unknown systems that fall into lower trust scores. The visualization of this distribution highlights the critical importance of contextual evaluation in a Zero-Trust architecture.

Monitoring user behavior risk scores over time shows how the system remains vigilant after the initial login. While the score remains low during normal activity, sudden spikes occur when abnormal patterns—like unusual access timing—are detected. This proves that the model successfully shifts authentication from a one-time event to a continuous process.

The adaptive access control decision distribution illustrates that the majority of access requests are granted based on low risk levels. However, a measurable percentage of requests are restricted or revoked due to moderate or high risk, respectively. This demonstrates that the system does not rely on static rules but adapts to the evolving threat landscape of a session.

Overall, the data validates that Zero-Trust enforcement minimizes unauthorized access while maintaining operational efficiency. The reduction in unauthorized access incidents compared to static systems confirms the robustness of the identity and behavior verification modules. Comprehensive logging and alerting also ensure that security administrators can respond quickly to any high-risk incidents detected by the engine.

Conclusion

The Zero-Trust Security Model Implementation Using Continuous Authentication provides a robust and modern approach to securing systems in dynamic computing environments. By eliminating implicit trust and continuously verifying identity, device posture, and behavior, the system significantly reduces risks associated with insider threats and session hijacking. Unlike traditional models, this approach ensures trust is never assumed and must be validated throughout the entire user session. The framework offers a scalable and effective solution for protecting critical resources in cloud-based and remote enterprise networks. Future enhancements may include AI-based risk prediction and biometric continuous authentication to further strengthen the model against next-generation threats.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-695 PAGE NO: 094-098

Future Work

- **Advanced AI:** Future systems can integrate Deep Learning and Recurrent Neural Networks to enable predictive risk modeling and more accurate behavioral anomaly detection.
- **Expanded Biometrics:** Incorporating passive behavioral biometrics, such as keystroke dynamics and mouse movement patterns, will strengthen identity verification without disrupting the user experience.
- **Edge Computing:** Security enforcement can be extended to cloud-native and edge environments to ensure low-latency protection for distributed applications.
- **Privacy Preservation:** Utilizing federated learning can help organizations collaborate on security intelligence while strictly preserving individual user privacy.
- **Immutable Auditing:** The integration of blockchain technology can provide tamper-proof, immutable audit trails for all access decisions and behavioral logs.
- **IoT Integration:** Expanding the "never trust, always verify" principle to the IoT ecosystem will secure diverse devices that currently lack robust built-in protection.

References

1. J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," Forrester Research, Tech. Rep., 2010.
2. NIST, "Zero Trust Architecture," NIST Special Publication 800-207, Gaithersburg, MD, USA, 2020.
3. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST SP 800-207, Aug. 2020.
4. D. Ferraiolo, M. Kuhn, and R. Chandramouli, "Role-based access control," IEEE Computer, vol. 38, no. 7, pp. 96-99, Jul. 2005.
5. A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," Pattern Recognition, vol. 38, no. 12, pp. 2270-2285, Dec. 2005.
6. Y. Sun, Z. Wang, and Y. Liu, "Continuous authentication using behavioral biometrics," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2745-2757, 2020.
7. M. Conti, N. Dragoni, and V. Lesyk, "A survey of man-in-the-middle attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, Third Quarter 2016.
8. T. Z. Tan, J. Chen, and S. Li, "Continuous user authentication based on keystroke dynamics," IEEE Access, vol. 7, pp. 110431-110442, 2019.
9. R. B. Basnet, S. Mukkamala, and A. H. Sung, "Detection of phishing attacks: A machine learning approach," IEEE Computer Society, pp. 1-8, 2008.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-695 PAGE NO: 094-098

10. M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-based cloud computing security management framework," IEEE International Conference on Cloud Computing, pp. 364-371, 2011.
11. Teixeira et al., "Continuous Authentication Using Behavioral Biometrics," IEEE Security & Privacy, vol. 12, no. 4, pp. 52-60, 2014.
12. Rose et al., "Zero Trust Architecture," IEEE Computer, vol. 52, no. 6, pp. 40-48, 2019.
13. M. E. Fagan and M. M. Khan, "Adaptive Access Control and Continuous Authentication in Zero Trust Environments," IEEE Access, vol. 9, pp. 145321-145334, 2021.
14. Microsoft, "Windows 11 Core Philosophy and Security," Official Documentation, 2021.
15. Python Software Foundation, "Python History and Key Features," PSF Documentation, 2023