(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :21/10/2025
(21) Application No.202541101393 A
(43) Publication Date : 28/11/2025

(54) Title of the invention : Zero-Trust Authentication Frame Work with Behavioral Metrics

(51) International classification	:H04L0009400000, H04L0009320000, G06F0021310000, A61H0001020000, G06F0021320000
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No Filing Date	: :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)Name of Applicant :
1)Swarnandhra College of Engineering and Technology (Autonomous)
Address of Applicant :Swarnandhra College of Engineering and Technology (Autonomous), Narasapur, West Godavari-534280, Andhra Pradesh, India. Narasapur Andhra Pradesh India
(72)Name of Inventor :
1)Dr. Thomurthy Murali Mohan
2)Mr. K. Karunakar
3)Mr. M. Srinivas Rao
4)Mrs. I. Lakshmi Pradeepa
5)Mrs. N. Jeevan Jyothi
6)Mrs. V. Ganga Bhavani
7)Mrs. B. Srilatha

(57) Abstract :
ABSTRACT: Title: Zero-Trust Authentication Frame Work with Behavioral Metrics The present invention discloses a novel Multi-Layered Zero-Trust Authentication Framework utilizing Continuous Behavioral Biometrics. This system implements a multi-layered cybersecurity model that combines continuous, passive behavioral biometrics with a Zero-Trust Architecture (ZTA) to establish a dynamic, context-aware trust score for every user and device access attempt. The framework continuously analyzes behavioral patterns, such as keystroke dynamics, mouse movements, and navigation rhythms, to verify identity beyond initial authentication. This method proactively detects and mitigates threats, particularly insider threats, by revoking access or escalating authentication challenges in real-time if a significant deviation from the established user behavioral profile is detected. The objective is to significantly enhance the security posture and authentication integrity within sensitive networks, providing a robust defense against evolving cyber risks.

No. of Pages : 14 No. of Claims : 2