(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :17/06/2026

(21) Application No.202641075243 A

(43) Publication Date : 26/06/2026

(54) Title of the invention : ADAPTIVE ZERO-TRUST SECURITY SYSTEM WITH ANOMALY-RESPONSIVE POLICY ENFORCEMENT FOR HETEROGENEOUS INTERNET OF THINGS NETWORK ENVIRONMENTS

(51) International classification	:H04L 29/06, H04L 9/40, H04L 12/24, G06F 21/57, H04W 12/08
(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)Dr. Mahesh Lokhande
Address of Applicant :Associate Professor and Head, Department of CSE (AI & ML), Guru Nanak Institute of Technology, Ibrahimpatnam, Ranga Reddy District, Telangana, India. Pin Code:501506 Telangana India
2)Mrs. R. Nirmala
3)Dr. Venkata Kishore Kumar Rejeti
4)Ms. D. Annie Selina
5)Dr. Amar Choudhary
6)Mr. Ganesh Shankar Sargam
7)Mr. Kalyan Savalapurapu
8)Dr. Usha Papineni
9)Dr. Duraimurugan S
10)Dr. K. Prabhu Chandran
(72)**Name of Inventor :**
1)Dr. Mahesh Lokhande
2)Mrs. R. Nirmala
3)Dr. Venkata Kishore Kumar Rejeti
4)Ms. D. Annie Selina
5)Dr. Amar Choudhary
6)Mr. Ganesh Shankar Sargam
7)Mr. Kalyan Savalapurapu
8)Dr. Usha Papineni
9)Dr. Duraimurugan S
10)Dr. K. Prabhu Chandran

(57) Abstract :
1. An adaptive zero-trust security system for a heterogeneous Internet of Things network environment, comprising a device identity binding module, a telemetry normalization engine, a trust evaluation engine, an anomaly detection engine, and an adaptive policy enforcement engine, wherein the telemetry normalization engine converts heterogeneous device telemetry into normalized security features, the trust evaluation engine generates a continuously updated trust-state vector for each connected device, and the adaptive policy enforcement engine applies a dynamic access policy based on the trust-state vector and an anomaly score generated by the anomaly detection engine. 2. The adaptive zero-trust security system as claimed in claim 1, wherein the device identity binding module binds a device identity with at least one of a hardware identity parameter, firmware integrity parameter, gateway association, cryptographic credential, device class, expected communication protocol, permitted command set, and authorized resource group. 3. The adaptive zero-trust security system as claimed in claim 1, wherein the trust-state vector includes a plurality of security indicators comprising authentication confidence, device posture, firmware conformity, behavioural conformity, command validity, protocol consistency, network location, anomaly severity, historical reliability, and resource sensitivity. 4. The adaptive zero-trust security system as claimed in claim 1, wherein the anomaly detection engine detects abnormal behaviour by comparing real-time device activity with a device-specific behavioural baseline, a device-class behavioural baseline, and a network-segment behavioural baseline. 5. The adaptive zero-trust security system as claimed in claim 1, wherein the adaptive policy enforcement engine applies an enforcement action selected from allowing access, restricting access, rate-limiting communication, blocking selected commands, requesting re-authentication, redirecting traffic to an inspection path, assigning the device to a quarantine segment, and terminating a device session. 6. The adaptive zero-trust security system as claimed in claim 1, wherein a protocol interpretation module identifies protocol-specific commands, message frequency, destination pattern, session sequence, and command-response behaviour to enable protocol-aware anomaly detection and policy enforcement. 7. The adaptive zero-trust security system as claimed in claim 1, wherein the adaptive policy enforcement engine performs progressive restriction by applying a limited access state for a low-risk deviation and escalating the device to quarantine or disconnection when subsequent telemetry confirms continued abnormality. 8. The adaptive zero-trust security system as claimed in claim 1, wherein a feedback update module updates at least one of a behavioural baseline, anomaly weight, trust evaluation parameter, and policy selection parameter based on enforcement results, administrator validation, device recovery status, re-authentication result, or confirmed incident indicator. 9. The adaptive zero-trust security system as claimed in claim 1, wherein the quarantine segment permits limited diagnostic communication for firmware verification, credential refresh, configuration inspection, malware scanning through a gateway, or administrator-approved recovery command while preventing access to sensitive protected resources. 10. A computer-implemented operating process executed by the adaptive zero-trust security system as claimed in claim 1, comprising onboarding a device by binding device identity attributes, collecting heterogeneous telemetry from the device and associated gateway, normalizing the telemetry into security features, generating a trust-state vector, detecting an anomaly score from behavioural deviation, selecting a dynamic access policy based on the trust-state vector and anomaly score, enforcing the selected dynamic access policy at a gateway, edge node, network control point, or protected resource boundary, and updating a behavioural baseline or policy parameter based on feedback from the enforcement action.

No. of Pages : 26 No. of Claims : 10