Patent Search

Invention Title	A SYSTEM AND METHOD FOR REAL-TIME INTRUSION DETECTION AND FORENSIC LOGGING IN INTERNET OF MEDICAL THINGS USING EXTEN BILSTM AND BLOCKCHAIN
Publication Number	07/2026
Publication Date	13/02/2026
Publication Type	INA
Application Number	202641010398
Application Filing Date	01/02/2026
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06N 3/08, H04L 9/06, G06N 3/04, G16H 40/20, H04L 9/32

Inventor

Name	Address	Country	Nati
Shaik Johny Basha	Department of CSE School of Engineering and Sciences (SEAS) SRM UNIVERSITY - AP, Mangalagiri, Andhra Pradesh - 522502	India	Indi
Dr. D. Veeraiah	Professor Department of CSE Lakireddy Bali Reddy College of Engineering (A) Mylavaram, NTR District, Andhra Pradesh - 521230	India	Indi
Dr. L. Sumalatha	Professor Department of CSE Jawaharlal Nehru Technological University Kakinada, Kakinada, Andhra Pradesh, 533003	India	Indi

Applicant

Name	Address	Country	Nationality
Jawaharlal Nehru Technological University Kakinada, Kakinada	Kakinada	India	India

Abstract:

Healthcare Internet of Medical Things (IoMT) security failures are not merely technical events but also clinical and legal incidents, where intrusion alerts may disrupt care d and require forensic accountability. Most existing intrusion detection systems primarily emphasize detection accuracy, while overlooking auditability, decision interpretabil attention mechanisms, and post-incident trust, such requirements that are critical in regulated healthcare environments. This paper proposes a practical, forensic-aware, r time intrusion detection framework that integrates an attention-enhanced Extended Bidirectional Long Short-Term Memory (BiLSTM) model with a lightweight blockchain l jointly enable accurate detection, accountability, and automated response. The Extended BiLSTM captures bidirectional temporal dependencies in IoMT traffic and highligh clinically significant anomalous patterns through attention mechanisms, while the blockchain component ensures tamper-proof logging, verifiable alerts, and automated mitigation via smart contracts. Experiments conducted on the UNSW-NB15, CICIDS2017, and Bot-IoT datasets demonstrate high detection accuracy with low false-positive alongside immutable forensic traceability and real-time response capability. The results indicate that aligning AI-based intrusion detection with healthcare accountability requirements substantially enhances the trustworthiness and deployability of IoMT security systems.

Complete Specification

Description:The system operates within a healthcare IoMT environment comprising a plurality of interconnected medical devices that generate continuous network traffi Such traffic includes device telemetry, control signals, patient monitoring data, and communication metadata exchanged over a network communication layer.

Data Acquisition and Preprocessing:

The network traffic generated by the IoMT devices is captured by a data acquisition and preprocessing module. The preprocessing module is configured to perform one more of the following operations:

- data cleaning and removal of corrupted or incomplete records,
- normalization of numerical features,
- encoding of categorical attributes, and
- segmentation of traffic into temporal windows suitable for sequential learning.

The preprocessing module ensures that heterogeneous IoMT traffic is transformed into a structured and normalized format before being supplied to the intrusion detec engine.

Extended BiLSTM-Based Intrusion Detection Engine:

The pre-processed data is provided to an Extended BiLSTM-based intrusion detection engine. The detection engine is configured to analyze network traffic sequences in both forward and backward temporal directions to capture short-term and long-range dependencies.

The Extended BiLSTM engine incorporates enhancements including temporal feature extraction, residual connections, and attention mechanisms, enabling the system t

View Application Status

Page last updated on: 26/06/2019