Patent Search

Invention Title	An Intelligent Risk Assessment System for Predicting Healthcare Attacks Using Reinforcement Learning on Network Traffic
Publication Number	33/2025
Publication Date	15/08/2025
Publication Type	INA
Application Number	202541072873
Application Filing Date	31/07/2025
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	BIO-MEDICAL ENGINEERING
Classification (IPC)	H04L0009400000, G16H0010600000, G06N0003080000, G06Q0010063500, G06N0020000000

Inventor

Name	Address	Country
Chekka Sravani	Assistant Professor Computer Science and Engineering, Marri Laxman Reddy Institute of Technology and Management, Dundigal, Hyderabad-500043, Telangana , INDIA.	India
Venkatesh Kumbar	Master of Engineering in Internetworking, Dalhousie University, Canada	India
Ms. Shubhangi Sudhir Mahadik	Department of MCA, Bharati Vidyapeeth Institute of Management and Information Technology, Navi Mumbai, Maharashtra, India	India
Dr. Pramod Vishwakarma	Computer Science & Engineering - Apex Chandigarh University, Mohali, Punjab, India	India
Bidyutlata Sahoo	Assistant Professor, Department of CSE (Artificial Intelligence and Machine Learning), Institute of Aeronautical Engineering, Hyderabad, Telangana, India	India

Applicant

Name	Address	Country
Chekka Sravani	Assistant Professor Computer Science and Engineering, Marri Laxman Reddy Institute of Technology and Management, Dundigal, Hyderabad-500043, Telangana , INDIA.	India
Venkatesh Kumbar	Master of Engineering in Internetworking, Dalhousie University, Canada	Canada
Ms. Shubhangi Sudhir Mahadik	Department of MCA, Bharati Vidyapeeth Institute of Management and Information Technology, Navi Mumbai, Maharashtra, India	India
Dr. Pramod Vishwakarma	Computer Science & Engineering - Apex Chandigarh University, Mohali, Punjab, India	India
Bidyutlata Sahoo	Assistant Professor, Department of CSE (Artificial Intelligence and Machine Learning), Institute of Aeronautical Engineering, Hyderabad, Telangana, India	India

Abstract:

The present invention relates to an intelligent risk assessment system for predicting cyber threats in healthcare networks using reinforcement learning. The system m network traffic in real-time, extracts features indicative of potential threats, and uses a deep reinforcement learning model to predict and categorize cybersecurity ris system dynamically adapts to emerging threats and minimizes false positives through continuous learning. It provides actionable alerts and recommendations, ensu integrity, confidentiality, and availability of healthcare data and services

Complete Specification

Description:The present invention relates to an intelligent risk assessment system for predicting cyber threats in healthcare networks using reinforcement learning. system monitors network traffic in real-time, extracts features indicative of potential threats, and uses a deep reinforcement learning model to predict and categori cybersecurity risks. The system dynamically adapts to emerging threats and minimizes false positives through continuous learning. It provides actionable alerts and recommendations, ensuring the integrity, confidentiality, and availability of healthcare data and services , C , C , C , C , C , Claims:1. An intelligent risk assessmen for predicting healthcare cyber-attacks using reinforcement learning, comprising:

- a data acquisition module to monitor and collect network traffic data from healthcare infrastructure;
- a preprocessing and feature extraction engine to convert traffic data into structured features;
- a deep reinforcement learning-based threat prediction engine configured to evaluate risk and predict potential cyber-attacks in real-time;
- an alert generation module to notify administrators upon detection of suspicious activity;
- and a feedback loop mechanism for continuous learning and model adaptation.

2. The system of claim 1, wherein the reinforcement learning model comprises a deep Q-network (DQN) or actor-critic model tailored for healthcare network beh
3. The system of claim 1, wherein the feature extraction engine identifies behavioral indicators such as protocol anomalies, device communication patterns, and a frequencies.
4. The system of claim 1, wherein the feedback loop utilizes outcomes of administrator actions and threat mitigation success to refine the model's reward functio
5. The system of claim 1, wherein the system is operable on-premises, in cloud environments, or as a hybrid deployment for securing distributed healthcare netw

View Application Status