(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :18/12/2023

(21) Application No.202341086430 A
(43) Publication Date : 12/01/2024

(54) Title of the invention : DETECTING CYBER-ATTACKS IN THE INTERNET OF MEDICAL THINGS USING FUZZY LOGIC AND LSTM NETWORKS

(51) International classification :G06N0003040000, G06N0003080000, G06N0020000000, G06F0021550000, G16H0050200000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Dr.Sowjanya M N
Address of Applicant :Assistant Professor, Master of Computer Applications VTU CPGS Mysore, Karnataka, India. ---------- ----------
2)S Dr.Ravish G K
3)Vinaykumar Hittalamani
4)Velladurai Narayanan
5)Neha pandey
6)Gade Venkata Subba Reddy
7)Pavithra T S
8)Gunjali Singh
9)A.Catherine Esther Karunya
10)B.Suresh kumar
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr.Sowjanya M N
Address of Applicant :Assistant Professor, Master of Computer Applications VTU CPGS Mysore, Karnataka, India. ---------- ----------
2)S Dr.Ravish G K
Address of Applicant :Assistant Professor, Master of Computer Applications VTU CPGS Mysore, Karnataka, India. ---------- ----------
3)Vinaykumar Hittalamani
Address of Applicant :Assistant Professor / CSE(MCA) Dept. OF CSE (MCA), PG Center, Visvesvaraya Technological University, Belagavi, Karnataka, India. ---------- ----------
4)Velladurai Narayanan
Address of Applicant :Professor / Nursing, Rohilkhand College of nursing, RMCH CAMPUS, Pilibhit Bypass Road, Bareilly, Uttar Pradesh, India. ---------- ----------
5)Neha pandey
Address of Applicant :Associate Professor, OBG in Nursing, Panna Dhai Maa Subharti Nursing College and Meerut, Uttar Pradesh, India. ---------- ----------
6)Gade Venkata Subba Reddy
Address of Applicant :Associate Professor, Electronics and Communication, Gokaraju Rangaraju Institute of engineering and technology, Hyderabad, Telangana, India. ---------- ----------
7)Pavithra T S
Address of Applicant :Assistant professor / MCA PES university, RR campus, Bengaluru, Karnataka, India. ---------- ----------
8)Gunjali Singh
Address of Applicant :Assistant lecturer, Mental Health Nursing Department Panna Dhai Maa Subharti Nursing College, Meerut, Uttar Pradesh, India. ---------- ----------
9)A.Catherine Esther Karunya
Address of Applicant :Assistant Professor, Artificial Intelligence and Machine Learning, SNS College of Technology, Coimbatore-641035, Tamilnadu, India. ---------- ----------
10)B.Suresh kumar
Address of Applicant :Associate professor / EEE, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, Telangana, India. ---------- ----------

(57) Abstract :
DETECTING CYBER-ATTACKS IN THE INTERNET OF MEDICAL THINGS USING FUZZY LOGIC AND LSTM NETWORKS A method for the development of the methods like as intrusion detection systems, log monitoring, and threat intelligence are used to detect and neutralize attacks on the IoMT. However, as attackers improve their methods, there is a growing trend towards applying machine learning and deep learning to detect attacks in a more precise and predictive manner. We propose a fuzzy-based self-tuning Long Short-Term Memory (LSTM) intrusion detection system (IDS) for the IoMT in this study. Several customized network security techniques and frameworks are used to divert attention away from generalized attacks such as botnet-based distributed denial of service (DDoS) and zero-day network attacks. To detect and prevent intrusions, healthcare institutions may use artificial intelligence (AI) techniques and cyber-physical systems (CPS). This study proposes a novel machine learning threat detection framework for secure healthcare data transfer. Smart Healthcare Cyber-Physical Systems (SHCPS) can send collected data to the cloud. These advancements allow the healthcare sector to successfully communicate with and care for its patients. Every IoT-enabled technology can pose a significant security risk. In the event of such an attack, critical IoT connectivity data may be revealed, modified, or even rendered unavailable to authenticated users. As a result, safeguarding IoT/IoMT systems against cyber-attacks has become critical. FIG.1

No. of Pages : 17 No. of Claims : 1