(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :18/11/2024

(21) Application No.202431089111 A
(43) Publication Date : 22/11/2024

(54) Title of the invention : ADAPTIVE MACHINE LEARNING SYSTEM FOR REAL-TIME CYBER THREAT DETECTION AND AUTOMATED MITIGATION

(51) International classification :H04L0009400000, G06N0020000000, G06F0021550000, G06N0020200000, G06N0003088000
(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. Santanu Koley
Address of Applicant :S/o. Mr. Siba Prasad Koley, Professor, Department of Computer Science & Engineering, Haldia Institute of Technology, ICARE Complex, Hatiberia, Haldia, Purba Medinipur - 721657, West Bengal, India. Haldia ---------- ----------
2)Dr. Monika Saxena
3)Subhasis Patra
4)Sudip Diyasi
5)Subhajit Roy
6)Rajesh Kumhar
7)Ankita Ghosh
8)Shouvik Sarkar
9)Dr. T. K. Senthil Kumar
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr. Santanu Koley
Address of Applicant :S/o. Mr. Siba Prasad Koley, Professor, Department of Computer Science & Engineering, Haldia Institute of Technology, ICARE Complex, Hatiberia, Haldia, Purba Medinipur - 721657, West Bengal, India. Haldia ---------- ----------
2)Dr. Monika Saxena
Address of Applicant :W/o. Mr. Mohit Kumar Saxena, Associate Professor, School of Management, Bennett University, Plot Nos 8, 11, Tech Zone 2, Greater Noida - 201310, Uttar Pradesh, India. Greater Noida ---------- ----------
3)Subhasis Patra
Address of Applicant :S/o. Mr. Mantu Patra, Instructor, Department of Computer Science and Engineering, Birla Institute of Technology and Science, Pilani (BITS Pilani) – Dubai Campus, Dubai International Academic City, P. O. Box - 345055, Dubai, UAE. ---------- ----------
4)Sudip Diyasi
Address of Applicant :S/o. Mr. Arun Diyasi, Assistant Professor, Department of Computer Application, Global Institute of Science & Technology, Haldia, Purba Medinipur - 721657, West Bengal, India. Haldia ---------- ----------
5)Subhajit Roy
Address of Applicant :S/o. Late. B. K. Roy, Research Scholar, Department of Electrical and Electronics Engineering, NIT Silchar, and Ex - Head of the Department DF & CS, Indian School of Ethical Hacking (Kolkata), NIT Road, Fakiratilla, Silchar, Cachar - 788010, Assam, India. Silchar ---------- ----------
6)Rajesh Kumhar
Address of Applicant :S/o. Mr. Manik Kumhar, Research Scholar, Department of Electrical and Electronics Engineering, NIT Silchar, NIT Road, Fakiratilla, Silchar, Cachar - 788010, Assam, India. Silchar ---------- ----------
7)Ankita Ghosh
Address of Applicant :D/o. Mr. Swarup Ghosh, Assistant Professor, Department of Computer Application, George College of Management and Science, South 24 Parganas - 700141, Kolkata, India. Kolkata ---------- ----------
8)Shouvik Sarkar
Address of Applicant :S/o. Mr. Swapan Kumar Sarkar, Assistant Professor, Department of Computer Science and Engineering -Artificial Intelligence, Brainware University, Barasat, North Twenty Four Parganas - 700030, West Bengal, India. Barasat ---------- ----------
9)Dr. T. K. Senthil Kumar
Address of Applicant :S/o. Mr. T. K. Krishnamurthy, Subject Matter Expert, Artificial Intelligence and Data Science, Larsen & Toubro EduTech, Chennai - 600125, Tamil Nadu, India. Chennai ---------- ----------

(57) Abstract :
This invention presents a machine learning-driven cybersecurity system designed to detect and mitigate cyber threats in real time across distributed network environments, including enterprise, cloud, and IoT networks. The system integrates supervised learning for identifying known threats, unsupervised learning for anomaly detection, and reinforcement learning to adapt to emerging attack patterns. The invention includes an automated threat mitigation module that can initiate actions such as isolating infected devices, blocking malicious traffic, and generating alerts without human intervention. A continuous feedback loop allows the system to improve its accuracy over time by reducing false positives and adapting to new threat vectors. This robust, scalable system enhances network security by rapidly identifying and responding to cybersecurity threats, offering reliable defense against both known and unknown attacks.

No. of Pages : 20 No. of Claims : 5