(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :22/06/2022

(21) Application No.202241035709 A
(43) Publication Date : 01/07/2022

(54) Title of the invention : DDOS ATTACK MALICIOUS CODE MITIGATION VULNERABILITY USING FEDERATED LEARNING IN IOT-REAL TIME APPLICATIONS

(51) International classification	:G06N0020000000, H04L0029080000, G06F0021620000, H04L0029060000, G06N0005040000
(86) International Application No Filing Date	:NA :NA
(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. VISWANATHAN RAMASAMY
Address of Applicant :PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, KONERU LAKSHMAIAH EDUCATION FOUNDATION, GREENFIELDS, VADDESWARAM, GUNTUR, ANDHRA PRADESH, INDIA 522302. ---------- ----------
2)DR. U. HARIHARAN
3)DR. S. PAZHANIRAJAN
4)DR. B. NARAYANAN
5)MERRY K. P
6)DR. K. PALANIYAPPAN
7)DR. S. RAMESH
8)N. N. PRABOO
9)DR. K. MUTHUKUMAR
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)DR. VISWANATHAN RAMASAMY
Address of Applicant :PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, KONERU LAKSHMAIAH EDUCATION FOUNDATION, GREENFIELDS, VADDESWARAM, GUNTUR, ANDHRA PRADESH, INDIA 522302. ---------- ----------
2)DR. U. HARIHARAN
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, APEX INSTITUTE OF TECHNOLOGY, CHANDIGARH UNIVERSITY, LUDHIYANA, LUDHIYANA - CHANDIGARH STATE HWY, MOHALI, PUNJAB, INDIA 140103. ---------- ----------
3)DR. S. PAZHANIRAJAN
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ANNAMALAI UNIVERSITY, ANNAMALAI NAGAR, CHIDAMBARAM, TAMILNADU, INDIA 608002. ---------- ----------
4)DR. B. NARAYANAN
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ANNAMALAI UNIVERSITY, ANNAMALAI NAGAR, CHIDAMBARAM, TAMILNADU, INDIA 608002. ---------- ----------
5)MERRY K. P
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, APEX INSTITUTE OF TECHNOLOGY, CHANDIGARH UNIVERSITY, LUDHIYANA, LUDHIYANA - CHANDIGARH STATE HWY, MOHALI, PUNJAB, INDIA 140103. ---------- ----------
6)DR. K. PALANIYAPPAN
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ANNAMALAI UNIVERSITY, ANNAMALAI NAGAR, CHIDAMBARAM, TAMILNADU, INDIA 608002. ---------- ----------
7)DR. S. RAMESH
Address of Applicant :ASSISTANT PROFESSOR, DEPT OF E & I ENGG., ANNAMALAI UNIVERSITY, ANNAMALAI NAGAR, CHIDAMBARAM, TAMILNADU, INDIA 608002. ---------- ----------
8)N. N. PRABOO
Address of Applicant :ASSISTANT PROFESSOR, DEPT OF E & I ENGG., ANNAMALAI UNIVERSITY, ANNAMALAI NAGAR, CHIDAMBARAM, TAMILNADU, INDIA 608002. ---------- ----------
9)DR. K. MUTHUKUMAR
Address of Applicant :ASSISTANT PROFESSOR, DEPT OF E & I ENGG., ANNAMALAI UNIVERSITY, ANNAMALAI NAGAR, CHIDAMBARAM, TAMILNADU, INDIA 608002. ---------- ----------

(57) Abstract :
Abstract FL is a distributed machine learning strategy wherein algorithms are built on end systems without exchanging specific data and are managed centrally. During training cycle, this safeguards privacy issues. The learnt characteristics are collected on a regular basis by a server or cloud service, which further constructs and updates a newer, increasingly appropriate prediction, that is subsequently provided back towards the network edge for group training. Among the' most versatile strategies for training algorithms on endpoints is FL.Resources for IoT keep track of device-specific anomalous different classifiers and combine modeling parameters changes from IoT systems.The device particular pattern recognition gets established outlier detection models from repositories and allows network data tracking whenever additional items are added to the IoT environment. Systems are groups can create stable and efficient ML techniques using the FL technique without transmitting intelligence. Such solution is considered to be a superior alternative than ML approaches since it protects the confidentiality of user information. Showcasing the advantages of combining federated learning using ensemble to produce the best possible outcomes.

No. of Pages : 9 No. of Claims : 6