(12) PATENT APPLICATION PUBLICATION
(21) Application No.202531091220 A
(19) INDIA
(22) Date of filing of Application :24/09/2025
(43) Publication Date : 10/10/2025

(54) Title of the invention : FL-IDSense: Privacy-Preserving Intrusion Detection Using Federated Learning in Distributed IoT Networks

(51) International classification	:H04L0009400000, G06F0021620000, H04L0009000000, G06N0020000000, G06N0003080000
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No	:
Filing Date	:01/01/1900
(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)Abhinandan Ghosh
Address of Applicant :Assistant Professor Computer Science And Engineering Adamas University 24 Parganas North West Bengal West Bengal India
2)Gopinathan S
3)Nithya E
4)Nivethitha N
5)Jeetesh Kumar Srivastava
6)Reenu
7)Satheeshkumar S
8)Dr Debarpita Santra
9)Chandrashekhar
10)Dhainje Prakash Bhagwan
11)Ruba M
12)Prof. Dr. Indraneel Mukhopadhyay
(72)**Name of Inventor :**
1)Abhinandan Ghosh
2)Gopinathan S
3)Nithya E
4)Nivethitha N
5)Jeetesh Kumar Srivastava
6)Reenu
7)Satheeshkumar S
8)Dr Debarpita Santra
9)Chandrashekhar
10)Dhainje Prakash Bhagwan
11)Ruba M
12)Prof. Dr. Indraneel Mukhopadhyay

(57) Abstract :

Abstract Because of the growing number and complexity of cyber threats, it is now critical to maintain secure communication and device safety in the Internet of Things (IoT). Aggregating data centrally in a traditional IDS makes it harder to protect privacy, keeps the system from growing and slows down responses. FL-IDSense is an invention that provides a unique, private way to prevent cyber-attacks on IoT devices by training detection models across all nodes and protecting private information via federated learning. On their own, each edge device teaches a small neural network with local traffic data and the encrypted updates are passed back to a central server for compiling. With trust scoring, our system can quickly discard any contributions deemed suspicious and stay strong against model poisoning attacks. Because the system is built on asynchronous updates, safe data grouping with homomorphic encryption and differential privacy procedures, sensitive user information is still protected for security and adapting to new threats. The FL-IDSense approach learns in two phases, first making general rules and then fine-tuning them locally which helps improve the accuracy of detecting intrusions in heterogeneous systems. Thanks to its universal design, the invention is useful in smart cities, healthcare and the industrial IoT, giving a secure and effective way to manage threats in today’s networked environments.

No. of Pages : 19 No. of Claims : 10