Patent Search

Invention Title	IOT SECURITY AND PRIVACY ENHANCEMENT WITH MACHINE AND DEEP LEARNING
Publication Number	50/2023
Publication Date	15/12/2023
Publication Type	INA
Application Number	202341077050
Application Filing Date	10/11/2023
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06N0003080000, H04W0004700000, G06N0003040000, H04W0084180000, H04L0009320000

Inventor

Name	Address	Country
Elavarasi M	Assistant professor, Senior Faculty-IT, Department of Computer science iNurture Education Solutions VISTAS Pallavaram, Chennai, Tamilnadu, India.	India
Mr. Harshal Vishvanath Patil	Assistant Professor/ Department of Computer Science and I. T. Bhusawal Arts Science and P O Nahata Commerce College Bhusawal 425201, Jalgaon, Maharashtra, India.	India
Prof. Dr. Bhojaraj Hanumant Barhate	Professor/ Department of Computer Science and I. T. Bhusawal Arts Science and P O Nahata Commerce College Bhusawal 425201, Jalgaon, Maharashtra, India.	India
Dr. Vaibhav P. Sonaje	Department of Computer Science & Application, SOCSE, Sandip University, Nashik, Maharashtra, India.	India
Dr. Kaushik V S	Assistant Professor, Mechanical Department, SNS College of Technology, Coimbatore-641035, Tamilnadu, India.	India
Dr. J Sirisha Devi	Institute of Aeronautical engineering, Dundigal, Hyderabad, Medchal- Malkajgiri, Telangana- 500043, India.	India
Dr. M.Anitha	Assistant Professor, Dept.of EEE, St.Joseph's College of Engineering, OMR, Chennai, 600119, Tamilnadu, India.	India
B.V. Sai Thrinath	Assistant Professor, EEE Department, Mohan Babu University, Tirupati, 517102, Chittoor, Andhra Pradesh, India	India
N Jagadeesh	Assistant Professor, Computer Science and Applications, St.Peter's Institute of Higher Education and Research, Chennai, Thiruvallur, Tamilnadu, India.	India
Dr. Ashish Avasthi	Associate Professor, CSE, Maharana Pratap Engineering College, Kanpur, 209217, Uttar Pradesh, India.	India
Dr. Vijay Singh	Associate Professor, CSE, Maharana Pratap Engineering College, Lucknow, Kanpur, 209217, Uttar Pradesh, India.	India
S.Ramya	Assistant Professor/Master of Computer Applications, M.Kumarasamy College of Engineering, Karur,639004, Tamilnadu, India.	India

Applicant

Name	Address	Country
Elavarasi M	Assistant professor, Senior Faculty-IT, Department of Computer science iNurture Education Solutions VISTAS Pallavaram, Chennai, Tamilnadu, India.	India
Mr. Harshal Vishvanath Patil	Assistant Professor/ Department of Computer Science and I. T. Bhusawal Arts Science and P O Nahata Commerce College Bhusawal 425201, Jalgaon, Maharashtra, India.	India
Prof. Dr. Bhojaraj Hanumant Barhate	Professor/ Department of Computer Science and I. T. Bhusawal Arts Science and P O Nahata Commerce College Bhusawal 425201, Jalgaon, Maharashtra, India.	India
Dr. Vaibhav P. Sonaje	Department of Computer Science & Application, SOCSE, Sandip University, Nashik, Maharashtra, India.	India
Dr. Kaushik V S	Assistant Professor, Mechanical Department, SNS College of Technology, Coimbatore-641035, Tamilnadu, India.	India
Dr. J Sirisha Devi	Institute of Aeronautical engineering, Dundigal, Hyderabad, Medchal- Malkajgiri, Telangana- 500043, India.	India
Dr. M.Anitha	Assistant Professor, Dept.of EEE, St.Joseph's College of Engineering, OMR, Chennai, 600119, Tamilnadu, India.	India
B.V. Sai Thrinath	Assistant Professor, EEE Department, Mohan Babu University, Tirupati, 517102, Chittoor, Andhra Pradesh, India	India
N Jagadeesh	Assistant Professor, Computer Science and Applications, St.Peter's Institute of Higher Education and Research, Chennai, Thiruvallur, Tamilnadu, India.	India
Dr. Ashish Avasthi	Associate Professor, CSE, Maharana Pratap Engineering College, Kanpur, 209217, Uttar Pradesh, India.	India
Dr. Vijay Singh	Associate Professor, CSE, Maharana Pratap Engineering College, Lucknow, Kanpur, 209217, Uttar Pradesh, India.	India
S.Ramya	Assistant Professor/Master of Computer Applications, M.Kumarasamy College of Engineering, Karur,639004, Tamilnadu, India.	India

Abstract:

IOT SECURITY AND PRIVACY ENHANCEMENT WITH MACHINE AND DEEP LEARNING A method for the development of a system for providing security services to IoT de system comprising a computer device and one or more processors operatively coupled to a storage device on which are stored modules of instruction code that whe by processors implements a Controlled Network, interfacing an IoT cellular Network, said Cellular Network hosting a plurality of IoT devices. The processing device is to determine a representation characterizing data from one or more sensor devices in at least one sensor network, to determine a privacy impact indicator for the da present the representation and its associated privacy impact indicator in a user device's user interface. The requesting device is illustratively a resource-constrained d comparison to the service providing device in terms of the particular service, and the particular service is a service that is capable of being performed in the requestir is offloaded from the requesting device to the service providing device via the request in order to conserve the requesting device's resources. Novel tools and strategi implementing the Internet of Things ("IoT") are presented. Microphones on an IoT human interface device may receive user voice input in some examples. The frame receives from the client computing device an encrypted first subnet model of the neural network. The first subnet model is one of a number of neural network partiti

Complete Specification

Description:IOT SECURITY AND PRIVACY ENHANCEMENT WITH MACHINE AND DEEP LEARNING

Technical Field

[0001] The embodiments herein generally relate to a method for an IoT security and privacy enhancement with machine and deep learning.

Description of the Related Art

[0002] Different policies may be complementary, with each providing a unique set of security approaches or attributes. Based on the behavior of the IOT device, s policies can be assigned to each IOT. 5G mobile communication systems are already in commercial use, but as a complex ecosystem, a 5G network has a variety of t participants, including infrastructure providers, mobile communication network operators, virtual operators, and various vertical industries, and user data is stored, transmitted, and processed in the complex network where a variety of access technologies, devices, and participants interact, resulting in a great deal of privacy is e Traditional sensor-based systems, such as alarm systems, lack intelligence and rely on the triggering of sensors coupled to a controller, which generates alarms in response. Traditional sensor-based systems, such as alarm systems, lack intelligence and rely on the triggering of sensors coupled to a controller, which generates a in response. There is a need for more robust and scalable solutions for implementing Internet of Things functionality, including techniques, systems, apparatus, and computer software for implementing Internet of Things ("IoT") human interface functionality. Modern deep learning models are built on artificial neural networks, b also include propositional expressions or potential variables constructed layer by layer in deep generative models like nodes and deep Boltzmann machines in deep networks. As a result, it is critical to identify and quantify what type of information will be disclosed, to what extent such information will be exposed during the dee

View Application Status

Department of Industrial Policy and Promotion
Government of India

Terms & conditions (http://ipindia.gov.in/terms-conditions.htm) Privacy Policy (http://ipindia.gov.in/privacy-policy.htm)
Copyright (http://ipindia.gov.in/copyright.htm) Hyperlinking Policy (http://ipindia.gov.in/hyperlinking-policy.htm)
Accessibility (http://ipindia.gov.in/accessibility.htm) Archive (http://ipindia.gov.in/archive.htm) Contact Us (http://ipindia.gov.in/contact-us.htm)
Help (http://ipindia.gov.in/help.htm)

Content Owned, updated and maintained by Intellectual Property India, All Rights Reserved.

Page last updated on: 26/06/2019