(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :22/08/2020

(21) Application No.202041036196 A

(43) Publication Date : 04/09/2020

(54) Title of the invention : ENERGY AUDITING FOR IOT SYSTEM SECURITY BY DEEP LEARNING CONVOLUTION NEURAL NETWORK

(51) International classification	:G06N 3/08
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(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)Mr.M V Pathi Amudalapalli

Address of Applicant :Assistant Professor, Department of ECE, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India. Pin-534201. Andhra Pradesh India

2)Mr.Prabira Kumar Sethy
3)Mr.Ch Mohammad Akram
4)Mr.Gundala Sunil Dayakar
5)Mr.Subramanyam kunisetti
6)Dr. Arun Sadanand Tigadi
7)Mr.Sanket Raval
8)Mrs.Seelaboyina Radha
9)Dr.G.Anandbabu
10)Mr. Nagarjuna Reddy Gujjula

(72)Name of Inventor :

1)Mr.M V Pathi Amudalapalli
2)Mr.Prabira Kumar Sethy
3)Mr.Ch Mohammad Akram
4)Mr.Gundala Sunil Dayakar
5)Mr.Subramanyam kunisetti
6)Dr. Arun Sadanand Tigadi
7)Mr.Sanket Raval
8)Mrs.Seelaboyina Radha
9)Dr.G.Anandbabu
10)Mr. Nagarjuna Reddy Gujjula

(57) Abstract :

IOT (Internet of Things) devices are small devices which can be located at any place and then this devices will sense data and send to require destination by using internet connections. This devices are not monitored by humans and can be tampered physically (manipulating internal parts to sense wrong data or to consume heavy energy) and it can be attacked using cyber technique such as DOS (denial of service). In dos technique malicious IOT can send huge amount of request to genuine neighbour or destination IOT which can lead to overheating of genuine device and it will be busy in reading huge request data and raise DOS error to other devices. To detect physical and cyber-attack, energy auditing technique by Machine Learning Convolutional Neural Network introduced. In this technique if any physical alteration done to IOT devices present in IOT system then huge amount of power consumption occurs and whenever any cyber DOS attack occurred then IOT devices present in IOT system get overheating which lead to more energy consumption. By auditing IOT devices energy consumption behaviour, we can detect attacks/anomalies in IOT system. To detect such attacks, we train Deep Learning Convolution Neural Network with past data which contains normal and attack energy consumption. After building model we will monitor/audit IOT energy consumption and then apply deep learning model to predict behaviour. If deep learning model predict abnormal energy consumption then it will predict that IOT device as under attack.

No. of Pages : 13 No. of Claims : 3

Home (http://ipindia.nic.in/index.htm) About Us (http://ipindia.nic.in/about-us.htm) Who's Who (http://ipindia.nic.in/whos-who-page.htm)
Policy & Programs (http://ipindia.nic.in/policy-pages.htm) Achievements (http://ipindia.nic.in/achievements-page.htm)
RTI (http://ipindia.nic.in/right-to-information.htm) Feedback (https://ipindiaonline.gov.in/feedback) Sitemap (shttp://ipindia.nic.in/itemap.htm)
Contact Us (http://ipindia.nic.in/contact-us.htm) Help Line (http://ipindia.nic.in/helpline-page.htm)
Skip to Main Content Screen Reader Access (screen-reader-access.htm)

inPASS Indian Patent Advanced Search System (http://ipindia.nic.in/index.htm) INTELLECTUAL PROPERTY INDIA PATENTS | DESIGNS | TRADE MARKS GEOGRAPHICAL INDICATIONS (http://ipindia.nic.in/inc

Patent Search

Invention Title	ENERGY AUDITING FOR IOT SYSTEM SECURITY BY DEEP LEARNING CONVOLUTION NEURAL NETWORK
Publication Number	36/2020
Publication Date	04/09/2020
Publication Type	INA
Application Number	202041036196
Application Filing Date	22/08/2020
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0029060000, G06N0003040000, G06N0003080000, G06N0020000000, H04L0029080000

Inventor

Name	Address	Country	Nat
Mr.M V Pathi Amudalapalli	Assistant Professor, Department of ECE, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India. Pin-534201.	India	Indi
Mr.Prabira Kumar Sethy	Assistant Professor, Department of Electronics, Sambalpur University, Jyoti Vihar, Burla, Odisha, India. Pin-768019	India	Indi
Mr.Ch Mohammad Akram	Department of Mechanical Engineering, KL (Deemed To Be) University, Vaddeswaram, Guntur District, Andhra Pradesh, India. Pin-522502.	India	Indi
Mr.Gundala Sunil Dayakar	Assistant Professor, Department of Electronics & Communication Engineering, VRS & YRN College of Engineering and Technology, Chirala, Andhra Pradesh, India. Pin-523157.	India	Indi
Mr.Subramanyam kunisetti	Assistant Professor, Department of IT R.V.R & J.C College of Engineering, Chowdavaram, Guntur, Andhra Pradesh, India. Pin-522019.	India	Indi
Dr. Arun Sadanand Tigadi	Associate Professor, Department of Electronics and Communication Engineering, KLE Dr.M.S.Sheshgiri College of Engineering & Technology, Udyambag, Belgaum, Karnataka, India. Pin-590008?	India	Indi
Mr.Sanket Raval	Lecturer, Department of Electrical Engineering, GMB Polytechnic, Rajula, Amreli District , Gujarat, India. Pin- 365560	India	Indi
Mrs.Seelaboyina Radha	Assistant Professor, Department of CSE Geethanjali College of Engineering and Technology, Hyderabad, Telangana, India. Pin-501301	India	Indi
Dr.G.Anandbabu	Department of Electronics and Communication Engineering, MVR College of Engineering and Technology, Paritala, Vijayawada, Krishna District, Andhra Pradesh, India. Pin-521180.	India	Indi
Mr. Nagarjuna Reddy Gujjula	Department of Electronics and Communication Engineering, MVR College of Engineering and Technology, Paritala, Vijayawada, Krishna District, Andhra Pradesh, India. Pin-521180	India	Indi

Applicant

Name	Address	Country	Nat
Mr.M V Pathi Amudalapalli	Assistant Professor, Department of ECE, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India. Pin-534201.	India	Indi
Mr.Prabira Kumar Sethy	Assistant Professor, Department of Electronics, Sambalpur University, Jyoti Vihar, Burla, Odisha, India. Pin-768019	India	Indi
Mr.Ch Mohammad Akram	Department of Mechanical Engineering, KL (Deemed To Be) University, Vaddeswaram, Guntur District, Andhra Pradesh, India. Pin-522502.	India	Indi
Mr.Gundala Sunil Dayakar	Assistant Professor, Department of Electronics & Communication Engineering, VRS & YRN College of Engineering and Technology, Chirala, Andhra Pradesh, India. Pin-523157.	India	Indi
Mr.Subramanyam kunisetti	Assistant Professor, Department of IT R.V.R & J.C College of Engineering, Chowdavaram, Guntur, Andhra Pradesh, India. Pin-522019.	India	Indi
Dr. Arun Sadanand Tigadi	Associate Professor, Department of Electronics and Communication Engineering, KLE Dr.M.S.Sheshgiri College of Engineering & Technology, Udyambag, Belgaum, Karnataka, India. Pin-590008?	India	Indi
Mr.Sanket Raval	Lecturer, Department of Electrical Engineering, GMB Polytechnic, Rajula, Amreli District , Gujarat, India. Pin- 365560	India	Indi
Mrs.Seelaboyina Radha	Assistant Professor, Department of CSE Geethanjali College of Engineering and Technology, Hyderabad, Telangana, India. Pin-501301	India	Indi
Dr.G.Anandbabu	Department of Electronics and Communication Engineering, MVR College of Engineering and Technology, Paritala, Vijayawada, Krishna District, Andhra Pradesh, India. Pin-521180.	India	Indi
Mr. Nagarjuna Reddy Gujjula	Department of Electronics and Communication Engineering, MVR College of Engineering and Technology, Paritala, Vijayawada, Krishna District, Andhra Pradesh, India. Pin-521180	India	Indi

Abstract:

IOT (Internet of Things) devices are small devices which can be located at any place and then this devices will sense data and send to require destination by using internet connections. This devices are not monitored by humans and can be tampered physically (manipulating internal parts to sense wrong data or to consume heavy energy) ar be attacked using cyber technique such as DOS (denial of service). In dos technique malicious IOT can send huge amount of request to genuine neighbour or destination I which can lead to overheating of genuine device and it will be busy in reading huge request data and raise DOS error to other devices. To detect physical and cyber-attack, auditing technique by Machine Learning Convolutional Neural Network introduced. In this technique if any physical alteration done to IOT devices present in IOT system th huge amount of power consumption occurs and whenever any cyber DOS attack occurred then IOT devices present in IOT system get overheating which lead to more ene consumption. By auditing IOT devices energy consumption behaviour, we can detect attacks/anomalies in IOT system. To detect such attacks, we train Deep Learning Conv Neural Network with past data which contains normal and attack energy consumption. After building model we will monitor/audit IOT energy consumption and then apply learning model to predict behaviour. If deep learning model predict abnormal energy consumption then it will predict that IOT device as under attack.

Complete Specification

Claims:1. An Energy Auditing for IOT System Security by Deep Learning Convolution Neural Network by which the security of the Internet of Things (IOT) system comprising of various Internet of Things (IOT) Devices is known by the Energy Auditing comprises: Generating Random Power Consumption values for various IOT device by the Internet of Things (IOT) simulation; Pre-processing to replace the negative values of the Energy consumed by the some IOT devices by a Median filter; Energy Disaggregation to store all energy values consumed by Internet of Things (IOT); System Performance Metrics to audit the energy model using deep learning algorithm to predict whether system is in attack or normal state; Predicting the trust value by the training the Machine Learning Convolutional Neural network.

2. The Energy Auditing for IOT System Security by Deep Learning Convolution Neural Network as claimed in claim 1, wherein is Energy Disaggregation model auditing t energy consumption of all Internet of Things (IOT) devices present in the Internet of Things (IOT) system.

3. The Energy Auditing for IOT System Security by Deep Learning Convolution Neural Network as claimed in claim 1, wherein is the trained Deep Learning Convolution Neural Network is pre-loaded with normal and abnormal energy consumption values of IOT devices, with this training Deep Learning Convolution Neural Network can au the energy consumed by each IOT devices and identify the abnormal IOT devices and the security of all the IOT devices present in the IOT system.
, Description:The entire Energy Auditing for IOT System Security by Deep Learning Convolution Neural Network is explored and the Energy Auditing for security in the Internet of Things (IOT) system by train the Deep Learning Convolution Neural Network is provide in the following layout that explain the entire view of the implementati of the technology that provides the security for Internet of Things (IOT) devices connected together in an Internet of Things (IOT) System (101) referring Figure 1. The Dat

View Application Status

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)

Page last updated on: 26/06/2019