

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

<p>(51) International classification :G06N 3/08</p> <p>(31) Priority Document No :NA</p> <p>(32) Priority Date :NA</p> <p>(33) Name of priority country :NA</p> <p>(86) International Application No :NA Filing Date :NA</p> <p>(87) International Publication No :NA</p> <p>(61) Patent of Addition to Application Number :NA Filing Date :NA</p> <p>(62) Divisional to Application Number :NA Filing Date :NA</p>	<p>(71)Name of Applicant :</p> <p>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</p> <p>2)Mr.Prabira Kumar Sethy</p> <p>3)Mr.Ch Mohammad Akram</p> <p>4)Mr.Gundala Sunil Dayakar</p> <p>5)Mr.Subramanyam kunisetti</p> <p>6)Dr. Arun Sadanand Tigadi</p> <p>7)Mr.Sanket Raval</p> <p>8)Mrs.Seelaboyina Radha</p> <p>9)Dr.G.Anandbabu</p> <p>10)Mr. Nagarjuna Reddy Gujjula</p> <p>(72)Name of Inventor :</p> <p>1)Mr.M V Pathi Amudalapalli</p> <p>2)Mr.Prabira Kumar Sethy</p> <p>3)Mr.Ch Mohammad Akram</p> <p>4)Mr.Gundala Sunil Dayakar</p> <p>5)Mr.Subramanyam kunisetti</p> <p>6)Dr. Arun Sadanand Tigadi</p> <p>7)Mr.Sanket Raval</p> <p>8)Mrs.Seelaboyina Radha</p> <p>9)Dr.G.Anandbabu</p> <p>10)Mr. Nagarjuna Reddy Gujjula</p>
---	--

(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