(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :07/12/2021

(21) Application No.202111056677 A
(43) Publication Date : 17/12/2021

(54) Title of the invention : MITIGATION OF CYBER-ATTACKS ON THE IOT DEVICES IN FOG ENVIRONMENT USING CIPHER PHYSICAL SYSTEM

(51) International classification :H04L0029080000, H04L0029060000, G06N0003040000, G16H0050200000, G06N0020000000
(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. Aftab Alam Abdussami
Address of Applicant :Department of Computer Application, Integral University, Lucknow, Uttar Pradesh, India - 226026 ---------- ----------
2)Dr Mohammad Faizan Farooqui
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Mr. Aftab Alam Abdussami
Address of Applicant :Department of Computer Application, Integral University, Lucknow, Uttar Pradesh, India - 226026 ---------- ----------
2)Dr Mohammad Faizan Farooqui
Address of Applicant :Department of Computer Application, Integral University, Lucknow, Uttar Pradesh, India ---------- ----------

(57) Abstract :
After the rapid growth of internet technology and lightweight IoT (Internet of Things) computational devices, sensing the information from any environment has become possible. IoT devices are well-profound of tracking the real-time data from the environments. Each IoT devices has a unique identification number (IP address), and they have an ability to connect to the internet and can transfer data over a network automatically. However, the IoT ecosystem and the number for systems connected to cloud increases the security vulnerabilities in all layers. Due to the lack of high computation power, implementing heavily weighted security algorithms are not possible. The proposed invention creates a machine learning based Cipher Physical Systems (CPS) on the IoT and Fog environment to monitor the IoT data packets that are transferred between them. Continuously monitoring the data packets helps in mitigating the risks and help in protecting the data and build confidence in digital transformation processes. Also, the proposed CPS hardware system uses a convolution neural network (CNN) based machine learning to predict the intrusion in the system proactively.

No. of Pages : 15 No. of Claims : 5