(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :14/09/2023

(21) Application No.202311061972 A
(43) Publication Date : 15/12/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR DETECTING CYBERSECURITYVULNERABILITIES IN INDUSTRIAL INTERNET OF THINGS (IIOT) DEVICES

(51) International classification	:G06N0020000000, G06F0021570000, G06F0021550000, G06N0020200000, G06N0005040000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India Pune ---------- ----------
2)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India Pune ---------- ----------
3)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
Embodiments of the present disclosure relates to a system (100) and method (300) for detecting cybersecurity vulnerabilities in a network of IIoT devices. In an aspect, the present disclosure discloses a system (102) for detecting cybersecurity vulnerabilities in a network of IIoT devices by applying machine learning, artificial intelligence, data analytics, and network security to efficiently identify, assess, and mitigate security vulnerabilities in IIoT devices, thereby enhancing the overall cybersecurity posture of industrial environments. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to collect data from the network of IIoT devices and analyse the collected data. Next, the processor (202) is configured to detect vulnerabilities in the network of IIoT devices and assign a risk score to the detected vulnerabilities.

No. of Pages : 29 No. of Claims : 10