(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :18/10/2023

(21) Application No.202311070831 A
(43) Publication Date : 24/11/2023

(54) Title of the invention : SYSTEM AND METHOD FOR SONIFICATION-BASED CYBER-THREAT DETECTION

(51) International classification :G06F0021550000, G06F0021560000, G06N0020000000, G10H0001000000, G06F0009455000
(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)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)PANDEY, Sakshi
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 :
The present invention discloses a system (100) for the detection of cyber threat through data sonification. The system (100) consists of a server (106) for secure communication with one or more computing devices (110) via a network (108), a processor (102), and a memory (104) containing a set of instructions. When executed, the processor (102) receives a set of network traffic data from the one or more computing devices (110), extracts one or more features from the received data, and converts the extracted features into audio patterns that represent a sonified based network traffic data. Correspondingly, the audio patterns are compared against a plurality of audio patterns associated with known cyber threats stored in a database (220). The system (100) can subsequently detect the presence of malicious audio patterns in the sonified network traffic data and identify the specific cyber threat, including type and severity of the identified cyber threat.

No. of Pages : 26 No. of Claims : 10