(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :10/08/2023

(21) Application No.202311053603 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR DETECTING AND BLOCKING UNAUTHORIZED ACCESS TO A NETWORK

(51) International classification	:G06F0021550000, G06F0021620000, H04W0012080000, G06F0021310000, H04W0012060000
(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)PANDEY, Sakshi
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)SINGH, Gurjinder
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 detecting and blocking unauthorized access to a network. The system comprises a server (106), a processor (102), and a memory (104) containing a set of instructions to be executed by the processor (102). The system (100) operates by receiving network traffic between one or more computing devices (110) and one or more networks (108). The received network traffic is compared with a database of known malicious network traffic to identify potential threats. Additionally, the system (100) receives authentication data from one or more users (112) through the computing devices (110), which is analyzed against a database of authorized user authentication data. By correlating the detected malicious network traffic and the verified identity of users (112), the system (110) can grant or deny access rights to the networks accordingly. Furthermore, upon detecting malicious network traffic and unauthorized user identity, the system (100) generates and transmits one or more alert signals to the computing devices 110 to promptly notify relevant users 112.

No. of Pages : 28 No. of Claims : 10