(12) PATENT APPLICATION PUBLICATION (21) Application No.202311066709 A

(19) INDIA

(22) Date of filing of Application :05/10/2023 (43) Publication Date : 22/12/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR NETWORK SECURITY THROUGH DYNAMICSIGNALLING MANAGEMENT WITH NEXT-GENERATION FIREWALL TECHNOLOGY

(51) International classification	:H04L0043045000, A61B0005055000, H04L0041000000, A61B0005000000, H04L0051046000
(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)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 enhanced network layer security through dynamic signaling management by applying next-generation firewall techniques. In an aspect, the system comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to initiate a communication session in a network. Further, the processor (202) is configured to detect security threats through the communication session. Next, the processor (202) is configured to manage firewall rules and configurations in real-time based on the detected security threats. In the end, the processor (202) is configured to provide greater visibility and control over network activity through a centralized management console based on the firewall rules and configurations.

No. of Pages : 24 No. of Claims : 10