

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311067005 A

(19) INDIA

(22) Date of filing of Application :06/10/2023

(43) Publication Date : 27/10/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR TRUST ASSESSMENT IN NETWORK-LAYER APPLICATION-SPECIFIC ENVIRONMENTS

<p>(51) International classification :A61B0005000000, G06F0021550000, H04L0025030000, G06F0016245700, A61B0005349000</p> <p>(86) International Application No :NA Filing Date :NA</p> <p>(87) International Publication No : NA</p> <p>(61) Patent of Addition to Application Number :NA Filing Date :NA</p> <p>(62) Divisional to Application Number :NA Filing Date :NA</p>	<p>(71)Name of Applicant : 1)Chitkara University Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----</p> <p>2)Bluest Mettle Solutions Private Limited Name of Applicant : NA Address of Applicant : NA</p> <p>(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 -----</p> <p>2)PANDEY, Sakshi Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----</p> <p>3)MANTRI, Archana Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----</p>
---	--

(57) Abstract :

Embodiments of the present disclosure relates to a system (102) and method (200) for dynamically assessing trust in network-layer application-specific environments in various types of computer networks, including wired and wireless networks. The system (102) comprises a processor (104) coupled to a memory (106). The memory (106) stores processor-executable instructions. The processor (104) is configured to collect network flow data from a plurality of components of the network-layer application-specific environment. Next, the processor (104) is configured to extract one or more features from the collected network flow data. Thereafter, the processor (104) is configured to analyse the extracted one or more features. In the end, the processor (104) is configured to identify potential security threats in real-time based on the analysis.

No. of Pages : 17 No. of Claims : 10