(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :04/08/2023

(21) Application No.202311052586 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : LATERAL MOVEMENT DETECTION FOR NETWORK ANALYSIS

(51) International classification :G06F0021550000, G06F0021570000, G06F0021620000, H04L0043000000, H04L0041142000
(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)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 :
The primary objective of the system in the present disclosure is to identify and detect lateral movement activities within a network promptly. By analysing network traffic (106) and user behaviors, the system aims to identify anomalous activities and suspicious behaviors that may indicate unauthorized access or malicious activities. Through continuous monitoring and analysis, the system establishes baseline patterns of normal network behavior and compares them to real-time activities to detect deviations and anomalies associated with lateral movement. Integrating with existing security infrastructure, such as intrusion detection and prevention systems, firewalls, and Security Information and Event Management (SIEM) platforms, the system provides a comprehensive view of network security. It correlates security events, identifies attack pathways used by attackers for lateral movement, and generates alerts and notifications to inform security administrators. Detailed reports and visualizations aid in incident response and remediation efforts. The system operates in real-time, continuously monitoring network traffic (106) and analysing activities to identify ongoing or new lateral movement attempts. By doing so, it enables security teams to respond swiftly, implement countermeasures, and prevent further unauthorized access or data breaches.

No. of Pages : 27 No. of Claims : 12