(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :01/05/2023

(21) Application No.202311031094 A

(43) Publication Date : 09/06/2023

(54) Title of the invention : SYSTEM AND METHOD FOR DETECTING AND MITIGATING PRIVILEGE ESCALATION

(51) International classification	:A61K 393950, A61P 010400, A61P 011600, A61P 290000, H04W 764500
(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)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
3)KAUSHAL, Rajesh
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present disclosure relates to a system (100) to detect and mitigate privilege escalation in computing devices (106). The system identifies various issues, including vulnerabilities, misconfigurations, and inappropriate access rules, using a privilege escalation detection module. Additionally, the privilege escalation detection module may monitor passwords for testing sudo rules, and a recommendation engine may facilitate generating instructions for issue remediation. Also, the system monitors and analyzes user account activities using a reconnaissance module, generates an audit log of user activities using an audit logging module, and transmits the audit log to a remote syslog host through a remote syslog forwarding module. Further, reconnaissance module may identify suspicious activity and send warnings to administrators, and the remote syslog forwarding module may encrypt the audit log prior to transmission. The system further transmits notifications to administrators about detected issues and recommends actions to remediate them.

No. of Pages : 27 No. of Claims : 10