(12) PATENT APPLICATION PUBLICATION (21) Application No.202311040610 A

(19) INDIA

(22) Date of filing of Application :14/06/2023 (43) Publication Date : 14/07/2023

(54) Title of the invention : PLATFORM AUDIT SECURITY SYSTEM AND METHOD THEREOF

(51) International classification	:G06F 215500, G06F 215700, G07C 090000, G08B 131960, H04N 071800
(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)MITTAL, Ruchi
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present invention discloses a platform audit security system (100) that includes a processor (102) to perform various functions that include receiving information about modifications made to a platform and group policy across multiple computing devices, capturing details such as entities involved, timing, location, and values before and after the modifications. The system also monitors and reports the logon history of entities, including both successful and unsuccessful attempts. Furthermore, the system identifies vulnerabilities and attack vectors that target specific points within the platform. In the event of two or more unsuccessful logon attempts, vulnerabilities, or attack vectors, the system promptly transmits an alert. The processor can additionally identify weaknesses in the configuration of the platform and web server of the computing devices. To facilitate comprehensive analysis and reporting, the system generates detailed reports based on the received information, logon history, vulnerabilities, and attack vectors.

No. of Pages : 26 No. of Claims : 10