

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311052961 A

(19) INDIA

(22) Date of filing of Application :07/08/2023

(43) Publication Date : 01/09/2023

(54) Title of the invention : SYSTEM FOR IDENTIFYING AND BLOCKING MALICIOUS INSIDER ACTIVITIES AND METHOD THEREOF

(51) International classification :G06F0021550000, G06F0021560000, G06N0020000000, A61B0005110000, H04W0004029000

(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)PANDEY, Sakshi**  
 Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----

**3)SHARMA, Manish**  
 Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----

(57) Abstract :

The present invention relates to a system (100) for identifying and blocking malicious insider activities. The system (100) includes a processing unit (104) and a server (106). The processing unit (104) consists of three main components to collect analyze and take appropriate action of the data which is collected through one or more resources (110). The system (100) utilizes one or more techniques such as behavioral analysis, real-time monitoring, and policy enforcement to identify suspicious activities and mitigate potential risks posed by trusted insiders, including employees, contractors, and partners. By continuously monitoring user behavior and analyzing various data resources, the system 100 establishes baseline patterns of normal activities and detects deviations or anomalous actions that may indicate malicious intent. The system 100 provides real-time alerts to security teams, enabling to respond promptly and take appropriate actions to prevent data breaches, intellectual property theft, or sabotage.

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