(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :18/08/2023

(21) Application No.202311055512 A

(43) Publication Date : 15/09/2023

(54) Title of the invention : A SYSTEM AND A METHOD FOR CLOUD-BASED SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

| | |
|---|---|
| (51) International classification | :G06F0021550000, G06F0021620000, G06F0021570000, G06F0016250000, G06N0020000000 |
| (86) International Application No<br>   Filing Date | :NA<br>:NA |
| (87) International Publication No | : NA |
| (61) Patent of Addition to Application Number<br>   Filing Date | :NA<br>:NA |
| (62) Divisional to Application Number<br>   Filing Date | :NA<br>: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 :
A system and a method for cloud-based security information and event management (SIEM) is provided. The system involves machine learning algorithms and real-time monitoring to identify potential security threats and anomalies, providing organizations with a centralized view of security events across multiple cloud environments to better manage security risks and respond to threats. The system 100 provides real-time monitoring, integration with other security tools, customization options, and multi-tenancy capabilities to ensure data privacy. The system 100 also offers automated incident response to quickly mitigate security threats. The system 100 offers scalability, flexibility, cost savings, ease of deployment, and enhanced security capabilities, enabling organizations to proactively protect their cloud-based assets.

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