(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :17/11/2023
(21) Application No.202311078182 A
(43) Publication Date : 23/05/2025

(54) Title of the invention : CLOUD-BASED SECURITY INCIDENT RESPONSE AND MANAGEMENT SYSTEM

(51) International classification	:G06F0009455000, A61B0005024000, G06F0021550000, G16H0040670000, G06F0009500000
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(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)Noida Institute of Engineering and Technology
Address of Applicant :19, Institutional Area, Knowledge Park Il, Greater Noida, Uttar Pradesh – 201306, India Greater Noida Uttar Pradesh India
(72)**Name of Inventor :**
1)Bhawna Wadhva
2)Subash Chandra
3)Archana Verma
4)Dr. Raman Batra

(57) Abstract :
Accordingly, embodiments herein disclose a cloud-based security incident response and management system that enables efficient detection, analysis, and mitigation of security incidents in cloud environments, facilitating rapid incident response and minimizing potential damages. The proposed system comprises a plurality of processors, and a plurality of memory devices comprising instructions that, when executed by the one or more processors, cause the one or more processors to perform operations comprising: obtaining activity data from a service provider system, identifying a pattern in the activity data, generating or updating a plurality of models associated with the cloud service, and outputting the set of actions and an indicator that identifies the set of actions as anomalous in response to a determination that the additional activity data does not include the pattern.

No. of Pages : 10 No. of Claims : 2