(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :19/02/2024

(21) Application No.202411011473 A
(43) Publication Date : 23/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR REAL-TIME DETECTION AND MITIGATION OF CYBER-HACKING ACTIVITIES

(51) International classification :G06F0021550000, H04L0009080000, G06N0020000000, G06F0021570000, G06F0021560000
(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)KAUR, Sehajpreet
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
A system (102) for real-time detection and mitigation of cyber-hacking activities within a network infrastructure is disclosed. The system (102) generates individualized behavioral profiles for users and computing devices, allowing for dynamic adaptation to evolving cyber threats. Additionally, the system continuously monitors network events, identifying anomalies, changes in topology, and security incidents. Further, the system (102) system employs an adaptive response orchestration mechanism to prioritize response actions, adjust execution sequences based on threat nature, and provide real-time threat assessments. Furthermore, including behavioral fingerprinting and hierarchical anomaly scoring, enhance ability of the system (102) to preemptively respond to emerging threats. The integration of quantum cryptography, DDoS attack mitigation, and real-time threat intelligence further fortifies robust cybersecurity capabilities of the system (102). Moreover, the proposed system represents a comprehensive solution for safeguarding digital assets, minimizing risks, and contributing to a secure and resilient network environment.

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