(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :02/08/2023

(21) Application No.202311051996 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : SYSTEM FOR WEBPAGE TEMPERING DETECTION

(51) International classification :G06F0021550000, G06N0020000000, G06F0021620000, A61B0005160000, 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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The proposed system in the present disclosure leverages real-time monitoring and granular tracking to continuously scrutinize web pages and their components, including files, directories, and specific elements. By comparing the current state with known thresholds (112) or previous versions, unauthorized modifications can be promptly identified, providing detailed insights into the tampering nature and location. The system incorporates behavioral analysis and anomaly detection techniques, enabling the identification of suspicious patterns in web traffic, user interactions, or server logs. Machine learning algorithms establish baseline behavior and intelligently detect anomalies associated with tampering attempts, ensuring effective detection and minimizing false positives. It includes integration with existing security frameworks, such as intrusion detection systems (IDS) and security information and event management (SIEM) systems, offers a comprehensive view of web security. Correlating tampering events with other security events enhances the system's context and response capabilities.

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