(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :10/10/2023

(21) Application No.202311067927 A

(43) Publication Date : 22/12/2023

(54) Title of the invention : SYSTEM AND METHOD FOR ADAPTIVE VULNERABILITY ASSESSMENT FRAMEWORK (AVAF)

(51) International classification	:G06F0021570000, G06N0020000000, G06F0021550000, G06N0005020000, G06K0009620000
(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)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 cybersecurity system (100) is a holistic defense mechanism for fortifying authorized cybersecurity services. It comprises a network of data collection nodes (102) perpetually ingesting data from diverse sources, channeled through a data preprocessing module (104) for refining and standardizing. Machine learning servers (106) with specialized processors conduct real-time data analysis, while a knowledge base server (110) maintains an updated repository of vulnerabilities and attack vectors. An adaptation and learning module (112) ensures adaptability to emerging threats by continuously updating knowledge bases and detection models. A vulnerability assessment and reporting module (114) rigorously evaluates identified vulnerabilities, prioritizing them for efficient resource allocation. Additionally, the system includes a real-time analysis module (108) for swift threat identification, a predictive analytics module for forecasting, and a continuous improvement feedback loop to enhance user-driven development, collectively offering a comprehensive and adaptable cybersecurity solution.

No. of Pages : 26 No. of Claims : 10