

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202411008121 A

(19) INDIA

(22) Date of filing of Application :06/02/2024

(43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR AUTOMATED GENERATION OF SECURITY POLICIES

(51) International classification :G06N0020000000, G06F0021570000, G06F0021550000, G06F0021560000, H04L0051000000

(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, Saket
 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)SINGH, Manjot
 Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----

(57) Abstract :

The system (100) of the present disclosure employs advanced threat intelligence analytics to identify and assess a diverse array of cybersecurity threats and vulnerabilities. Utilizing a machine learning model (106) with heuristic mechanisms, the system (100) dynamically analyzes risk factors, including malware, phishing attacks, and zero-day exploits, derived from cyber threat feeds and vulnerability databases and generates automated security policies (108). The method involves training the machine learning model (106) on historical security incidents, continually adapting to evolving threat landscapes. The system (100) assigns priority levels to identified threats and vulnerabilities based on risk analysis (104) and dynamically adjusts security configurations in real time. It addresses technical aspects such as the correlation of threats with compliance standards, adaptive access controls, and periodic updates to the machine learning model (106) for sustained effectiveness.

No. of Pages : 33 No. of Claims : 10