(12) PATENT APPLICATION PUBLICATION (21) Application No.202411008670 A

(19) INDIA

(22) Date of filing of Application :08/02/2024 (43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR ENHANCED CYBERSECURITY THROUGH NEURAL EMBEDDING

(51) International classification	:G06N0003080000, G06N0003040000, G06F0011340000, G06F0021550000, G06F0021570000
(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, 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, Yuvraj
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :
Aspect of the present disclosure relates to method and a system (100) for optimizing the efficiency and effectiveness of cyber-attack detection, forecasting, and classification is disclosed. The method includes collecting and curating, via a data collection module (212), historical cyber-attack datasets; training, via a training module (214), deep neural networks and incorporating neural embeddings to the said curated historical cyber-attack datasets; optimizing, via an optimization module (216), weights and parameters to capture nuanced patterns and relationships; analyzing, via a data analysis module (218), real-time analysis of incoming data streams, and enabling the identification of anomalies, similarities, and patterns; comparing, via a detection module (220), real-time data with learned embeddings to identify known attack patterns, facilitating timely alerting of security personnel or automated response systems.

No. of Pages : 28 No. of Claims : 8