(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :28/07/2023

(21) Application No.202311051028 A
(43) Publication Date : 25/08/2023

(54) Title of the invention : PASSWORD ATTACK PREDICTOR

(51) International classification :G06N0003080000, G06N0020000000, G06N0003040000, G06F0021620000, G06F0021550000
(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)KAUSHAL, Rajesh
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India Patiala ---------- ----------

(57) Abstract :
The present disclosure presents a system and method for predicting and preventing password attacks. The system comprises a data obtainment module, a prediction module equipped with machine learning techniques, a database, and a feedback module. The data obtainment module collects login attempts, while the prediction module utilizes supervised and unsupervised learning analyzes to accurately predict and prevent password attacks. The collected data and output are stored in the database, facilitating analysis and feedback control through the feedback module. The system employs various features, including feature engineering, anomaly detection, real-time monitoring, adaptive learning, risk scoring, user profiling, two-factor authentication integration, continuous improvement, and privacy protection measures. By leveraging these components, the system enhances the security of password-based systems, ensuring effective defense against a wide range of password attacks.

No. of Pages : 22 No. of Claims : 10