(12) PATENT APPLICATION PUBLICATION   (21) Application No.202311049954 A

(19) INDIA

(22) Date of filing of Application :25/07/2023   (43) Publication Date : 25/08/2023

---

(54) Title of the invention : A SYSTEM FOR PREDICTING AND PREVENTING A PASSWORD ATTACK

(51) International classification : G06N0020000000, G06N0003080000, G06N0003040000, G06N0007000000, G06N0005000000	(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 ----------- -----------

(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	

(57) Abstract :
Aspects of the present disclosure relate to cybersecurity technologies, and more particularly, to a system and method for predicting and preventing a password attack in networks using machine learning. The present disclosure relates to a method for predicting and preventing a password attack in networks using machine learning. The method (200) for predicting and preventing a password attack begins with analysing (202) user behaviour patterns and network traffic data to indicate the password attack. Next, the method proceeds to implement and train (204) a model for detecting the password attack. Thereafter, the method ends with preventing (206) the detected password attack.

No. of Pages : 20 No. of Claims : 10