(12) PATENT APPLICATION PUBLICATION (21) Application No.202311038311 A

(19) INDIA

(22) Date of filing of Application :04/06/2023 (43) Publication Date : 07/07/2023

(54) Title of the invention : SYSTEM FOR DETECTING ZERO-DAY ATTACKS

(51) International classification	:G01B 090201, G01R 332800, G06F 215300, H04L 090000, H04W 241000
(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, 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)SHARMA, Bhanu

Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present disclosure relates to a system (100) and method (300) for zero-attack detection that includes a processor (102) and memory (104) that executes a set of instructions to detect one or more zero-day attacks. The system detects one or more zero-day attacks by combining a supervised and an unsupervised machine learning algorithm and monitors behavior to identify the one or more zero-day attacks based on deviation from usual behavior. Additionally, the system responds to the one or more zero-day attacks in real-time upon identification of the one or more zero-day attacks and sends alerts through one or more computing devices (112) to respond to the detection of the one or more zero-day attacks.

No. of Pages : 22 No. of Claims : 7