(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :03/08/2023

(21) Application No.202311052296 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : DETECTION AND MITIGATION OF ADVANCED PERSISTENT THREAT (APT) ATTACK

(51) International classification :G06F0021550000, H04L0005000000, G06F0021570000, B60R0025102000, H04M0003420000
(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)KAUSHAL, Rajesh**
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India Patiala ---------- ----------

(57) Abstract :
Embodiments of the present disclosure provide a system (100) and method (300) designed for detecting and mitigating Advanced Persistent Threat (APT) attacks. The method (300) begins with monitoring (302) network traffic between one or more computing devices and networks, extracting (304) relevant features from the traffic. The extracted (304) relevant features are then compared (306) with a database of known features associated with the APT attack. Based on the comparison, the system (100) detects (308) the presence or absence of the APT attack and takes appropriate measures to mitigate (310) the detected APT attack. Additionally, the system (100) generates and transmits (312) alert signals to the one or more computing devices (110) upon detecting presence of the APT attack.

No. of Pages : 24 No. of Claims : 10