(12) PATENT APPLICATION PUBLICATION (21) Application No.202311064589 A

(19) INDIA

(22) Date of filing of Application :26/09/2023 (43) Publication Date : 13/10/2023

(54) Title of the invention : APT ATTACK DETECTION AND EARLY WARNING SYSTEM FOR ELECTRIC SYSTEMS BASED ON NETWORK ARCHITECTURE

(51) International classification	:G06N0020000000, G06F0021550000, G06N0007000000, H04L0041220000, G06F0011300000
(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, Rahul

Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------

2)SINGH, Dhiraj

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 ----------- -----------

(57) Abstract :

The present invention relates to a APT Attack Detection and Early Warning System which offers an advanced solution tailored for safeguarding electric systems against Advanced Persistent Threats (APTs). Comprising strategically deployed sensor nodes within the electric system's network, the system captures and continuously monitors network traffic. Data from these nodes is consolidated by central data collection mechanisms, ensuring comprehensive visibility of network activities. Real-time data analysis, employing techniques such as machine learning, anomaly detection, and behavior profiling, scans the aggregated data for potential APT threats. Upon detecting anomalies or threats, alerts are generated and disseminated to system administrators through diverse channels. A centralized management console provides administrators with a comprehensive overview of the system's security status, enabling swift response actions. This holistic approach ensures timely detection, alerting, and mitigation of APT threats, fortifying the security and resilience of critical electric infrastructures.

No. of Pages : 23 No. of Claims : 10