

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311033673 A

(19) INDIA

(22) Date of filing of Application :12/05/2023

(43) Publication Date : 23/06/2023

(54) Title of the invention : SYSTEM TO DETECT INTRUSION AND ACCESS OF CONFIDENTIAL INFORMATION BY UNAUTHORIZED USERS IN A NETWORK

(51) International classification :G06F 215700, G06F 216200, G06Q 201000, G08B 131860, H04L 090600
(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)SINGH, Dhiraj

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

3)SHARMA, Ishu

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

(57) Abstract :

The present disclosure relates to an intrusion detection system (100) and method (300) that includes a processor (102) and memory (104) that execute a set of instructions to detect various forms of network intrusion. The system downloads an SSL certificate, extracts information from it, compare it to a trusted local copy, and detects seized networks, wildcard certificates, and subject alternative names with DNS entries. Additionally, the system records signal strength indicator data and declare a rogue access point if there are discrepancies in the received RSSI values. The processor (102) also generates an alert and transmits the alert in real-time to security personnel computing devices (114). The system correspondingly performs at least one action to prevent the impact of detected intrusion and unauthorized access.

No. of Pages : 27 No. of Claims : 10