(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :01/08/2023

(21) Application No.202311051503 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : SENSOR BASED VULNERABILITY DETECTION

(51) International classification :G06F0021570000, H04L0041220000, H04L0043000000, G06F0021550000, H04L0043045000
(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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The proposed invention discloses a system and method for sensor-based wireless network vulnerability detection to enhance the security of wireless networks. The sensor-based wireless network vulnerability detection system comprises at least one sensor (102), a data processing unit (104), and a communication module (106). The sensors (102) are strategically deployed to monitor network traffic and detect potential vulnerabilities by analyzing anomalies or patterns in the network traffic. The data processing unit (104) receives data from the sensors and performs thorough analysis to identify potential vulnerabilities in the wireless network. It utilizes advanced techniques such as machine learning algorithms and predefined vulnerability signatures to enhance detection accuracy. When a potential vulnerability is detected, the system generates real-time alerts to promptly notify the network administrator. These alerts, transmitted via communication channels such as email, SMS, instant messaging, or a web-based dashboard, ensure that the network administrator is promptly informed about the identified vulnerabilities.

No. of Pages : 19 No. of Claims : 10