(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :13/06/2023

(21) Application No.202311040319 A
(43) Publication Date : 14/07/2023

(54) Title of the invention : SYSTEM AND METHOD TO ANALYZE VULNERABILITIES ON KUBERNETES

(51) International classification	:B01L 030000, C10G 450000, G06F 094550, G06F 215700, H04L 435000
(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 disclosure relates to a system (100) for detecting any security flaws, vulnerabilities or data corruption in any containers of a Kubernetes cluster (110). The system performs vulnerability scanning (104) that includes active and passive tests to check the state of the cluster in a running and stable state to detect all possible vulnerabilities. The system also consists of a feature to scan any additional storage space that may be connected to the Kubernetes cluster (110). The system can also deploy a monitoring solution (106) after each and every Git command to ensure security in every step of a code execution. The features include replacing any corrupt containers or killing them if they are completely unresponsive to increase security and also decrease any latency that it may cause. The method includes conducting penetration testing (108) that the user chooses to detect all security vulnerabilities or flaws without missing out on any.

No. of Pages : 28 No. of Claims : 10