

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311049953 A

(19) INDIA

(22) Date of filing of Application :25/07/2023

(43) Publication Date : 25/08/2023

(54) Title of the invention : MALWARE SIMULATOR

(51) International classification :G06F0021560000, G06F0021570000, G06F0009455000, G06F0030200000, G09B0023280000
(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)MITTAL, Ruchi

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

(57) Abstract :

The current invention discloses a computer-implemented method and system for simulating malware spread in a virtual cloud environment to evaluate and improve cloud security measures. The method involves creating a virtual cloud environment using cloud simulation system, injecting simulated malware strains that replicate real-world malware behavior, running the simulation to observe malware behavior and impact, analyzing the simulation results to identify vulnerabilities and evaluate existing security measures, and developing improved security measures based on the analysis. The system consists of cloud simulation system, a library of simulated malware strains, a simulation engine, an analysis engine, and a security measure development engine. Additionally, the system may include a user interface for configuring the virtual cloud environment, selecting malware strains, and viewing simulation results. This method and system provide a cost-effective and data-driven approach to enhancing cloud security by effectively simulating malware spread and guiding the development of robust security measures.

No. of Pages : 20 No. of Claims : 10