(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :14/03/2024

(21) Application No.202411018697 A

(43) Publication Date : 12/04/2024

(54) Title of the invention : SYSTEM TO IDENTIFY MALWARE BY USING BLOCKCHAIN TECHNOLOGY-ENABLED INCIDENT RESPONSE AND METHOD THEREOF

(51) International classification	:H04L0009320000, G06F0021560000, H04L0009060000, G06N0020000000, G06F0021620000
(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)Chitkara Innovation Incubator Foundation
Name of Applicant : NA
Address of Applicant : NA

(72)**Name of Inventor :**
1)SHARMA, Preeti
Address of Applicant :Computer Science Engineering, CUIET, Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------
2)SANIA
Address of Applicant :Northcap University, Huda, Sector 23A, Gurugram, Haryana – 122017, India. Gurugram ----------- -----------
3)MEENAKSHI
Address of Applicant :OD30, 3rd Floor, Malibu Town, Sec 47, Gurugram, Haryana – 122017, India. Gurugram ----------- -----------
4)HOODA, Sushila
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present invention is related to the field of malware detection, and more specifically relates to the system (100) and method (300) for identifying malware by using Blockchain technology-enabled incident response. The system (100) for enhancing cybersecurity through blockchain-enabled incident response for malware detection, employing a four-stage process integrating various components and technologies. In Stage 1, data collection and analysis are facilitated by network and system logs, supported by a Blockchain-based data sharing platform ensuring secure and decentralized data sharing. Stage 2 involves Blockchain-enabled incident response, leveraging smart contracts for automated response procedures. In Stage 3, advanced malware detection techniques, including machine learning techniques, are utilized alongside a Blockchain-based malware detection platform for real-time access and secure sharing of malware data. Finally, Stage 4 focuses on threat intelligence and sharing, utilizing a platform for secure sharing of threat intelligence and real-time information exchange to enhance awareness of cybersecurity threats.

No. of Pages : 26 No. of Claims : 10