

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202411010867 A

(19) INDIA

(22) Date of filing of Application :16/02/2024

(43) Publication Date : 23/02/2024

(54) Title of the invention : BLOCKCHAIN-BASED THREAT INTELLIGENCE SHARING SYSTEM AND METHOD THEREOF

(51) International classification :H04L0009320000, H04L0009060000, G06F0016270000, G06F0021640000, G06F0021570000

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

(57) Abstract :

A blockchain-based threat intelligence sharing system (100) including a plurality of nodes (102) distributed across a blockchain network (106) and a processing unit (104) in communication with the plurality of nodes (102), and operatively coupled with a blockchain ledger is disclosed. The system (100) acquires threat data from various entities and ensures the accuracy and authenticity of received threat data through cryptographic verification and embeds unique hash values into the blockchain. Employing a consensus protocol among nodes guarantees integrity of the system. Upon identifying predetermined threat indicators, responsive actions are triggered, and entities can selectively share threat data using cryptographic techniques.

No. of Pages : 23 No. of Claims : 10