

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311042457 A

(19) INDIA

(22) Date of filing of Application :24/06/2023

(43) Publication Date : 21/07/2023

(54) Title of the invention : ARTIFICIAL INTELLIGENCE-BASED SYSTEM AND METHOD FOR CRYPTOGRAPHIC KEY DISTRIBUTION

| | |
|--|---|
| <p>(51) International classification :G16H 502000, H04B 107000, H04L 090800, H04L 093200, H04W 120431</p> <p>(86) International Application No :NA Filing Date :NA</p> <p>(87) International Publication No : NA</p> <p>(61) Patent of Addition to Application Number :NA Filing Date :NA</p> <p>(62) Divisional to Application Number :NA Filing Date :NA</p> | <p>(71)Name of Applicant : 1)Chitkara University Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----</p> <p>2)Bluest Mettle Solutions Private Limited Name of Applicant : NA Address of Applicant : NA</p> <p>(72)Name of Inventor : 1)MISHRA, Saket Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----</p> <p>2)PANDEY, Sakshi Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----</p> <p>3)SINGH, Gurjinder Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----</p> |
|--|---|

(57) Abstract :

A system (100) a system (100) for key distribution by trusted nodes for a vehicular ad hoc network (VANET) is disclosed. The system includes a plurality of nodes, a node being either a mobile vehicle node equipped with an on-board unit or a static road-side unit node, herewith referred respectively as vehicle nodes (A, B, C, D, E, F, G) and RSU nodes (R1, R2, R3), wherein said RSU nodes have a permanent connection to a certificate authority (CA), said CA being responsible for a specific geographic region in which the VANET is comprised and said CA acting as the root of trust for the VANET, and wherein the VANET nodes have at least one pair of public-private keys and the corresponding certificates, issued by said CA. Each node comprises a data processing unit configured to request a set of keys from an RSU node that is within range and within that region on entering said specific geographic region, either by direct communication, or by through multi-hop communication, wherein said vehicle node sends a key request to said RSU node, said request including the vehicle node public key. The data processing unit further configured to receive a list with the key identifiers of the private keys shared by said vehicle node at said vehicle node and the other vehicle nodes that have most recently contacted said RSU node for a predetermined period of time. The data processing unit further configured to inform the VANET nodes, within a neighbourhood of a predetermined number of hops from said RSU node, of the presence of said vehicle node and of the identifiers of keys obtained by said vehicle node.

No. of Pages : 33 No. of Claims : 6