INTELLECTUAL PROPERTY INDIA
एकस्व/PATENTS|अभिकल्प/DESIGNS|
व्यापार चिह्न/TRADE MARKS|भौगोलिक
उपदर्शन/GEOGRAPHICAL INDICATIONS

सत्यमेव जयते

भारत सरकार
GOVERNMENT OF INDIA

एकस्व कार्यालय / THE PATENT OFFICE
बौद्धिक सम्पदा भवन / I.P.O. BUILDING
जी.एस.टी.रोड, गिंडी/ G.S.T.Road, Guindy,
चेन्नई/ Chennai- 600032
दूरभाष/ Tel. No. : (091)(044)22502081-84
फ़ैक्स/ Fax: 044 22502066

Email/ई मेल : Chennai-patent@nic.in
वेबसाइट /Website: http://ipindia.nic.in

सं. \ No. 202141006477 दिनांक \ Dated the 22/03/2023

सेवा मे, \ To :

Address of Service:- K&S PARTNERS Intellectual Property Attorneys 4121/B, 6th Cross, 19A Main, HAL II Stage (Extension), Bangalore – 560 038, Karnataka, INDIA
Email Id:- IPO@knspartners.com,bangalore@knspartners.com

विषय :- पेटेंट आवेदन संख्या 202141006477 के संबंध मे अधिनियम की धारा 43 के तहत पेटेंट अनुदान तथा पेटेंट रजिस्टर मे प्रविष्टि की सूचना
Sub :- Intimation of the grant and recordal of patent under section 43 of the Act in respect of patent application no. 202141006477

महोदय/महोदया,
Sir/Madam,

आपको सूचित किया जाता है कि पेटेंट अधिनिय, 1970 की धारा 12 व 13 तथा उस आधार पर बने नियम के तहत उपर्युक्त पेटेंट आवेदन के परीक्षण [व -------- को हुई सुनवाई] के उपरांत एतद्द्वारा पेटेंट अनुदान किया जाता है। तथा पेटेंट अनुदान की प्रविष्टि 22/03/2023 को पेटेंट रजिस्टर मे कर दी गयी है।

This is to Inform you that following the examination of above mentioned patent application under section 12 and 13 of The Patents Act, 1970 and Rules made thereunder [and hearing held on -------] a patent is hereby granted and recorded in the Register of Patents on the 22/03/2023. The Patent Certificate is enclosed herewith.

पेटेंट संख्या \ Patent No	: 426359
आवेदक का नाम \ Name Of Applicant	: INDIAN INSTITUTE OF SCIENCE
पेटेंट दिनांक \ Date of Patent	: 16/02/2021
पूर्विक्ता तिथि \ Priority Date	: 16/02/2021
परीक्षण हेतु अनुरोध दाखिल करने की तिथि \ Filling date of Request for examination	: 14/02/2022
शीर्षक \ Title	: A METHOD AND SYSTEM FOR IMPLEMENTING PRIVACY COMPLIANCE ASSOCIATED WITH HOST AREAS ON AGENT DEVICES
दावों की संख्या \ Number of claims	: 1-20

उपर्युक्त पेटेंट के अनुदान का प्रकाशन अधिनियम की धारा 43 के तहत पेटेंट कार्यालय के आधिकारिक जर्नल मे किया जाएगा।
The grant of above mentioned patent will be published in the Official Journal of the patent Office under section 43 of the Act.

पेटेंट अधिनियम 1970 यथा संशोधित पेटेंट (संशोधन) नियम, 2005/ पेटेंट नियम, 2003 यथा संशोधित पेटेंट (संशोधन) नियम, 2016 की धारा 142 की उप-धारा (4) के प्रावधानों के तहत उपरोक्त प्रविष्टि की तिथि से 3 माह के भीतर इस कार्यालय मे नवीकरण शुल्क जमा किया जाना चाहिए।
The payment of renewal fee is required to be made at this office within three(3) months from the aforesaid date of recording according to the proviso in sub-section(4) of Section 142 of The Patents Act,1970, as amended by The Patents (Amendment) Act, 2005 / The Patents Rules, 2003 as amended by The Patents (Amendment) Rules, 2016.

Niranjan Kumar
(नियंत्रक पेटेंट)
Controller of Patents

टिप्पणी / Note :

1. संशोधित नवीकरण शुल्क हेतु कृपया महानियंत्रक पेटेंट, अभिकल्प एवं व्यापार चिह्न की आधिकारिक वैबसाइट www.ipindia.gov.in पर उपलब्ध पेटेंट (संशोधन) नियम 2016 की प्रथम अनुसूची (शुल्क) देखें।
For revised renewal fees kindly refer to the First Schedule (fees) of The Patents (Amendment) Rules 2016 available on the official website of Controller General of Patents, Designs and Trade Marks www.ipindia.gov.in
2. कार्यालय द्वारा पेटेंट प्रमाणपत्र की कोई भी कागजी प्रति अलग से जारी नहीं की जाएगी।
No hard copy of Patent Certificate shall be issued separately by the office.

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

सत्यमेव जयते

क्रमांक : 044151550
SL No :

भारत सरकार
GOVERNMENT OF INDIA
पेटेंट कार्यालय
THE PATENT OFFICE

पेटेंट प्रमाणपत्र
PATENT CERTIFICATE

(Rule 74 of The Patents Rules)

पेटेंट सं. / Patent No.	:	426359
आवेदन सं. / Application No.	:	202141006477
फाइल करने की तारीख / Date of Filing	:	16/02/2021
पेटेंटी / Patentee	:	INDIAN INSTITUTE OF SCIENCE

प्रमाणित किया जाता है कि पेटेंटी को, उपरोक्त आवेदन में यथाप्रकटित A METHOD AND SYSTEM FOR IMPLEMENTING PRIVACY COMPLIANCE ASSOCIATED WITH HOST AREAS ON AGENT DEVICES नामक आविष्कार के लिए, पेटेंट अधिनियम, 1970 के उपबंधों के अनुसार आज तारीख फरवरी 2021 के सोलहवें दिन से बीस वर्ष की अवधि के लिए पेटेंट अनुदत्त किया गया है।

It is hereby certified that a patent has been granted to the patentee for an invention entitled A METHOD AND SYSTEM FOR IMPLEMENTING PRIVACY COMPLIANCE ASSOCIATED WITH HOST AREAS ON AGENT DEVICES as disclosed in the above mentioned application for the term of 20 years from the 16th day of February 2021 in accordance with the provisions of the Patents Act,1970.

एकस्य कार्यालय THE PATENT OFFICE GOVT.OF INDIA भारत सरकार

अनुदान की तारीख :
Date of Grant : 22/03/2023

पेटेंट नियंत्रक
Controller of Patent

टिप्पणी - इस पेटेंट के नवीकरण के लिए फीस, यदि इसे बनाए रखा जाना है, फरवरी 2023 के सोलहवें दिन को और उसके पश्चात प्रत्येक वर्ष मे उसी दिन देय होगी।

Note. - The fees for renewal of this patent, if it is to be maintained will fall / has fallen due on 16th day of February 2023 and on the same day in every year thereafter.

WE CLAIM:

1. A method of implementing privacy compliance associated with host area on agent devices, the method comprising:

transmitting, by a compliance system (102) implemented on an agent device (101), to a central server (103), information comprising identification details of the agent device (101), details of destination host area (307), and a navigation route along with geographical coordinates to the destination host area (307);

receiving, by the compliance system (102), from the central server (103), an authorization certificate for using the navigation route along with one or more privacy policies associated with at least one or more intermediate areas (303, 305) located in the navigation route and of the destination host area (307) upon authentication of the agent device (101);

monitoring, by the compliance system (102), geographical coordinates of the agent device (101), wherein a notification is triggered by the compliance system (102) when the geographical coordinates of the agent device (101) match with geographical coordinates of at least one of, the one or more intermediate areas (303, 305) located in the navigation route and the destination host area (307); and

implementing, by the compliance system (102), the one or more privacy policies associated with one of the at least one or more intermediate areas (303, 305) located in the navigation route and the destination host area (307) when the notification is triggered, wherein the one or more privacy policies are implemented by using respective predetermined communication graph.

2. The method as claimed in claim 1, wherein the identification details comprise a registered public key.

3. The method as claimed in claim 1, wherein authentication of the agent device (101) comprises checking whether the navigation route intersects any sensitive zones and altitude restrictions.

4. The method as claimed in claim 1 comprising providing a Trusted Execution Environment (TEE) attestation to at least one of the one or more intermediate areas (303, 305) and the destination host area (307) to verify integrity of the policy enforcement system implemented on the agent device (101).

5. The method as claimed in claim 1, wherein the one or more privacy policies associated with each intermediate areas (303, 305) is provided by the respective control device to the central server (103).

6. The method as claimed in claim 1 comprising verifying integrity of the agent device (101), upon being challenged by destination host area (307), by performing hardware attestation of the compliance system to the destination host area (307).

7. The method as claimed in claim 6, wherein each of the agent device (101) is equipped with a hardware TEE to store respective private key.

8. The method as claimed in claim 1 comprising confirming to control devices associated with at least one or more intermediate areas (303, 305) and destination host area (307) regarding implementation of one or more predefined applications in the agent device (101) via hardware attestation, wherein the one or more predefined applications are provided by the respective control device of the at least one or more intermediate areas (303, 305) and the destination host area (307).

9. The method as claimed in claim 1 comprising implementing a mandatory access control (MAC) mechanism at operating system (OS) of the compliance system to regulate inter-application communication, wherein the MAC mechanism comprises allowing restrictions to applications communicate directly via operating system (OS) abstractions or bypassing of the compliance system (102), allowing modifications enabling the OS about the abstractions, and redirecting communication via one or more predefined application.

10. The method as claimed in claim 1, wherein the communication graph identifies a list of permitted flows between one more application in the compliance system (102).

11. A compliance system (102) for implementing the method of privacy compliance associated with host area on agent devices, comprising:

a transmitter (107) to:

transmit to a central server (103), information comprising identification details of the agent device (101), details of destination host area (307), and a navigation route along with geographical coordinates to the destination host area (307);

a receiver (109) to:

receive from the central server (103), an authorization certificate for using the navigation route along with one or more privacy policies associated with at least one or more intermediate areas (303, 305) located in the navigation route and for the destination host area (307);

a processor (113); and

a memory (111) communicatively coupled to the processor (113), wherein the memory (111) stores processor instructions, which on execution, causes the processor (113) to:

monitor geographical coordinates of the agent device (101), wherein a notification is triggered when the geographical coordinates of the agent device (101) match with geographical coordinates of at least one of, one or more intermediate areas (303, 305) located in the navigation route and the destination host area (307); and

implement the one or more privacy policies associated with one of, the at least one or more intermediate areas (303, 305) located in the navigation route and the destination host area (307) when the notification is triggered, wherein the one or more privacy policies are implemented by using respective predetermined communication graph.

12. The compliance system (102) as claimed in claim 11, wherein the identification details comprise a registered public key.

13. The compliance system (102) as claimed in claim 11, wherein the processor (113) authenticates the agent device (101) by checking whether the navigation route intersects any sensitive zones, altitude restrictions.

14. The compliance system (102) as claimed in claim 11, wherein the processor (113) provides a Trusted Execution Environment (TEE) attestation to at least one of the one or more intermediate areas (303, 305) and the destination host area (307) to verify integrity of the policy enforcement system implemented on the agent device (101).

15. The compliance system (102) as claimed in claim 11, wherein the one or more privacy policies associated with each intermediate areas (303, 305) is provided by respective control device to the central server (103).

16. The compliance system (102) as claimed in claim 11, wherein the processor (113) verifies integrity of the agent device (101), upon being challenged by destination host area

(307), by performing hardware attestation of the compliance system to the destination host area (307).

17. The compliance system (102) as claimed in claim 16, wherein each of the agent device (101) is equipped with a hardware TEE to store respective private key.

18. The compliance system (102) as claimed in claim 11, wherein the processor (113) confirms regarding implementation 5 of one or more predefined applications in the agent device
(101) via hardware attestation to control devices associated with the at least one or more intermediate areas (303, 305) and destination host, wherein the one or more predefined applications are provided by the respective control device of at least one or more intermediate areas (303, 305) and the destination host area (307).

19. The compliance system (102) as claimed in claim 11, wherein the processor (113) implements a mandatory access control (MAC) mechanism at operating system (OS) of the compliance system to regulate inter-application communication, wherein the MAC mechanism comprises allowing restrictions to applications communicate directly via operating system (OS) abstractions or bypassing of the compliance system, allowing modifications enabling the OS about the abstractions, and redirecting communication via one or more predefined application.

20. The compliance system (102) as claimed in claim 11, wherein the communication graph identifies a list of permitted flows between one more application in the compliance system.

Dated this 16th day of February, 2021

R. Ramya Rao
Of K&S Partners
Agent for the Applicant
IN/PA-1607