पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 50/2023	शुक्रवार	दिनांक: 15/12/2023
ISSUE NO. 50/2023	FRIDAY	DATE: 15/12/2023

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

INTRODUCTION

In view of the recent amendment made in the Patents Act, 1970 by the Patents (Amendment) Act, 2005 effective from 01st January 2005, the Official Journal of The Patent Office is required to be published under the Statute. This Journal is being published on weekly basis on every Friday covering the various proceedings on Patents as required according to the provision of Section 145 of the Patents Act 1970. All the enquiries on this Official Journal and other information as required by the public should be addressed to the Controller General of Patents, Designs & Trade Marks. Suggestions and comments are requested from all quarters so that the content can be enriched.

(PROF. (DR) UNNAT P. PANDIT)
CONTROLLER GENERAL OF PATENTS, DESIGNS & TRADE MARKS

15nd DECEMBER, 2023

CONTENTS

THE PATENT OFFICE
KOLKATA, 15/12/2023
Address of the Patent Offices/Jurisdictions
The following are addresses of all the Patent Offices located at different places having their Territorial Jurisdiction on a Zonal basis as shown below:-

1	Office of the Controller General of Patents, Designs & Trade Marks, Boudhik Sampada Bhavan, Near Antop Hill Post Office,S.M.Road,Antop Hill, Mumbai – 400 037 Phone: (91)(22) 24123311, Fax : (91)(22) 24123322 E-mail: cgpdtm@nic.in	4	The Patent Office, Government of India, Intellectual Property Rights Building, G.S.T. Road, Guindy, Chennai – 600 032. Phone: (91)(44) 2250 2081-84 Fax : (91)(44) 2250 2066 E-mail: chennai-patent@nic.in ❖ The States of Andhra Pradesh, Telangana, Karnataka, Kerala, Tamil Nadu and the Union Territories of Puducherry and Lakshadweep.
2	The Patent Office, Government of India, Boudhik Sampada Bhavan, Near Antop Hill Post Office,S.M.Road,Antop Hill, Mumbai – 400 037 Phone: (91)(22) 24137701 Fax: (91)(22) 24130387 E-mail: mumbai-patent@nic.in ❖ The States of Gujarat, Maharashtra, Madhya Pradesh, Goa and Chhattisgarh and the Union Territories of Daman and Diu & Dadra and Nagar Haveli	5	The Patent Office (Head Office), Government of India, Boudhik Sampada Bhavan, CP-2, Sector –V, Salt Lake City, Kolkata- 700 091 Phone: (91)(33) 2367 1943/44/45/46/87 Fax: (91)(33) 2367 1988 E-Mail: kolkata-patent@nic.in ❖ Rest of India
3	The Patent Office, Government of India, Boudhik Sampada Bhavan, Plot No. 32., Sector-14, Dwarka, New Delhi – 110075 Phone: (91)(11) 25300200 & 28032253 Fax: (91)(11) 28034301 & 28034302 E.mail: delhi-patent@nic.in ❖ The States of Haryana, Himachal Pradesh, Jammu and Kashmir, Punjab, Rajasthan, Uttar Pradesh, Uttaranchal, Delhi and the Union Territory of Chandigarh.		

Website: www.ipindia.nic.in
www.patentoffice.nic.in

All applications, notices, statements or other documents or any fees required by the Patents Act, 1970 and The Patents (Amendment) Act, 2005 or by the Patents (Amendment) Rules, 2006 will be received only at the appropriate offices of the Patent Office.

Fees: The Fees may either be paid in cash or may be sent by Bank Draft or Cheques payable to the Controller of Patents drawn on a scheduled Bank at the place where the appropriate office is situated.

पेटेंट कार्यालय

कोलकाता, दिनांक 15/12/2023

• कार्यालयों के क्षेत्राधिकार के पते

विभिन्न जगहों पर स्थित पेटेंट कार्यालय के पते आंचलिक आधार पर दर्शित उनके प्रादेशिक अधिकार क्षेत्र के साथ नीचे दिए गए है:-

1	कार्यालय : महानियंत्रक, एकस्व, अभिकल्प तथा व्यापार चिहन, एंटोप हिल डाकघर के समीप, एस. एम. रोड, एंटोप हिल, मुम्बई- 400 037, भारत, फोन: (91) (22) 24123311 फ़ैक्स: (91) (22) 24123322 ई. मेल: cgpdtm@nic.in	4	पेटेंट कार्यालय, भारत सरकार इंटेलेक्चुअल प्रॉपर्टी राइट्स बिल्डिंग, इंडस्ट्रियल इस्टेट एसआईडीसीओ आरएमडी गोडाउन एरिया एडजसेन्ट टु ईगल फ्लास्क, जी. एस. टी. रोड, गायन्डी चेन्नई - 600 032. फोन: (91)(44) 2250 2081-84 फ़ैक्स: (91)(44) 2250-2066 ई. मेल: chennai-patent@nic.in ❖ आन्ध्र प्रदेश, तेलंगाना, कर्नाटक, केरल, तमिलनाडु तथा पुडुचेरी राज्य क्षेत्र एवं संघ शासित क्षेत्र, लक्षदीप
2	पेटेंट कार्यालय, भारत सरकार बौद्धिक संपदा भवन, एंटोप हिल डाकघर के समीप, एस. एम. रोड, एंटोप हिल, मुम्बई- 400 037, फोन: (91) (22) 24137701 फ़ैक्स: (91) (22) 24130387 ई. मेल: Mumbai-patent@nic.in ❖ गुजरात, महाराष्ट्र, मध्य प्रदेश, गोवा तथा छत्तीसगढ़ राज्य क्षेत्र एवं संघ शासित क्षेत्र, दमन तथा दीव, दादर और नगर हवेली.	5	पेटेंट कार्यालय, भारत सरकार कोलकाता, (प्रधान कार्यालय) बौद्धिक संपदा भवन, सीपी-2, सेक्टर- V, साल्ट लेक सिटी, कोलकाता-700 091, भारत. फोन: (91)(33) 2367 1943/44/45/46/87 फ़ैक्स:/Fax: (91)(33) 2367 1988 ई. मेल: kolkata-patent@nic.in ❖ भारत का अवशेष क्षेत्र
3	पेटेंट कार्यालय, भारत सरकार बौद्धिक संपदा भवन, प्लॉट सं. 32, सेक्टर- 14, द्वारका, नई दिल्ली- 110 075. फोन: (91)(11) 25300200, 28032253 फ़ैक्स: (91)(11) 28034301, 28034302 ई. मेल: delhi-patent@nic.in हरियाणा, हिमाचल प्रदेश, जम्मू तथा कश्मीर, पंजाब,राजस्थान, उत्तर प्रदेश, दिल्ली तथा उत्तरांचल राज्य क्षेत्रों, एवं संघ शासित क्षेत्र चंडीगढ़		

वेबसाइट: http://www.ipindia.nic.in
www.patentoffice.nic.in

पेटेंट अधिनियम, 1970 तथा पेटेंट (संशोधन) अधिनियम, 2005 अथवा पेटेंट (संशोधन) नियम, 2006 द्वारा वांछित सभी आवेदन, सूचनाए, विवरण या अन्य दस्तावेज़ या कोई शुल्क पेटेंट कार्यालय के केवल उपयुक्त कार्यालय में स्वीकृत होंगे।

शुल्क: शुल्क या तो नगद रूप में या Controller of Patents के नाम में देय बैंक ड्राफ्ट या चेक के द्वारा भेजी जा सकती है जो उसी स्थान के किसी अनुसूचित बैंक में प्रदत्त हो जहाँ उपयुक्त कार्यालय स्थित है ।

SPECIAL NOTICE

18 Months publication as required under Section 11A of the Patents Act, 1970 as amended by the Patents (Amendment) Act, 2005.

Notice is hereby given that any person at any time before the grant of Patent may give representation by way of opposition to the Controller of Patents at appropriate office on the ground and in a manner specified under section 25(1) of the Patents (Amendment) Act, 2005 read with Rule 55 of the Patents (Amendment) Rules, 2006.

Notice is also given that if any interested person requests for copies of the complete specification, drawing and abstract of any application already published, the photocopy of the same can be supplied by the Patent Office as per the jurisdiction on payment of prescribed fees of Rs.8/- per page. If any further details are required to be obtained, the same can be provided by the respective Patent Offices on request.

(PROF. (DR) UNNAT P. PANDIT)
CONTROLLER GENERAL OF PATENTS, DESIGNS & TRADE MARKS

SPECIAL NOTICE

Under the new provision of the Patents Act, 1970 as amended by the Patents (Amendment) Act, 2005 and Rules there under, Publication of the matter relating to Patents in the Official Gazette of India Part III, Section 2 has been discontinued and instead The Official Journal of the Patent Office is being published containing all the activities of The Patent Office such as publication of all the patent applications after 18th months , grant of patents & all other information in respect of the proceedings as required under the provisions of the Patents (Amendment) Act, 2005 and Rules thereunder on weekly basis on every **Friday**.

The Journal is uploaded in the website every Friday. So Paper form and CD-ROM form of the Journal are discontinued from 01/01/2009.

SPECIAL NOTICE

Every effort is being taken to publish all the patent applications under section 11(A) of the Patents Act. However, if duplication of publication of any application is found, then earlier date of publication will be taken for the purpose of provisional protection for applicant and Patent Office will grant Patent not before six months from the date of second publication, provided that there is there is no third party representation.

(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :10/11/2023

(21) Application No.202341076807 A
(43) Publication Date : 15/12/2023

(54) Title of the invention : DETECTION OF MALICIOUS BLOCKCHAIN ATTACKS USING FEDERATED LEARNING

(51) International classification :G06N0020000000, G06N0003080000, G06F0021560000, G06N0003040000, G06F0021550000
(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)Mr. Nazeer Shaik
Address of Applicant :Asst. Professor, Dept.of.CSE, Srinivasa Ramanujan Institute of Technology, Autonomous-Anantapur, Andhra Pradesh, 515001, India ---------- ----------
2)J L. Sarwani Theeparthi
3)Mrs. Muddana.Rishitha Bhavani
4)Mrs. Inaganti Bhavana
5)Dr. Rahul Sharma
6)Abarna. S
7)Mr. Rayavarapu Bhavani Sankar
8)Mr. Chokkapu NarayanaRao
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Mr. Nazeer Shaik
Address of Applicant :Asst. Professor, Dept.of.CSE, Srinivasa Ramanujan Institute of Technology, Autonomous-Anantapur, Andhra Pradesh, 515001, India ---------- ----------
2)J L. Sarwani Theeparthi
Address of Applicant :Associate Professor, Dept of CSE, Aditya College of Engineering and Technology, Surampalem, Kakinada-Dist., Andhra Pradesh-533 437, India. ---------- ----------
3)Mrs. Muddana.Rishitha Bhavani
Address of Applicant :Assistant Professor, Department of Cyber Security and Data Science, Bapatla Engineering College, Bapatla, Andhra Pradesh -522 102, India. ---------- ----------
4)Mrs. Inaganti Bhavana
Address of Applicant :Assistant Professor, Department of Cyber Security and Data Science, Bapatla Engineering College, Bapatla, Andhra Pradesh -522 102, India. ---------- ----------
5)Dr. Rahul Sharma
Address of Applicant :Assistant Professor, GDC KATHUA, 180001, KATHUA, Jammu and Kashmir, India. ---------- ----------
6)Abarna. S
Address of Applicant :Assistant Professor, Department of Chemistry, SNS College of Technology ---------- ----------
7)Mr. Rayavarapu Bhavani Sankar
Address of Applicant :Assistant Professor, Department of Computer Science and Engineering, Chirala Engineering College, Ramapuram Beach Road, Chirala, Bapatla District, Andhra Pradesh, 523157, India. ---------- ----------
8)Mr. Chokkapu NarayanaRao
Address of Applicant :Assistant Professor, Department of CSE, Vignan's Institute of Engineering for Women(A), Visakhapatnam, Andhra Pradesh -530046, India. ---------- ----------

(57) Abstract :
DETECTION OF MALICIOUS BLOCKCHAIN ATTACKS USING FEDERATED LEARNING A method for the development of the invention proposes a network flow intrusion detection technique based on a block chain and federal learning, which includes the processes listed below: Each device detects and labels the novel attack independently, so establishing a global model. After feeding a training sample set into the current local model and training it, the product of the weight matrix norm and the gradient norm of each network layer in the current local model satisfies the constraint condition of a Richest constant. A first bottom layer sub-model, an interaction layer sub-model, a top layer sub-model based on a Lipschitz neural network, and a second bottom layer sub-model in a second participant device comprise the longitudinal federated learning model. The block chain DDoS attack is efficiently recognized, and the communication overhead in the training process is considerably minimized. By using a two-stage detection mode, system resources are saved; by training each initial detection model using the federal learning method, each distributed malicious host that initiates a DDoS attack can be determined, the accuracy of DDoS detection is improved, and a user's privacy is protected. The approach can detect rogue nodes and strengthen the vertical federal learning system. FIG.1

No. of Pages : 17 No. of Claims : 1

FORM 1 THE PATENTS ACT 1970 (39 of 1970) and THE PATENTS RULES, 2003 **APPLICATION FOR GRANT OF PATENT** (See section 7, 54 and 135 and sub-rule (1) of rule 20)	(FOR OFFICE USE ONLY)

	Application No.	
	Filing date:	
	Amount of Fee paid:	
	CBR No:	
	Signature:	

1. APPLICANT'S REFERENCE / IDENTIFICATION NO. (AS ALLOTTED BY OFFICE)	

2. TYPE OF APPLICATION [Please tick (✓) at the appropriate category]

Ordinary (✓)		Convention ()		PCT-NP ()	
Divisional ( )	Patent of Addition ()	Divisional ( )	Patent of Addition ()	Divisional ( )	Patent of Addition ()

3A. APPLICANT(S)

Name in Full	Nationality	Country of Residence	Address of the Applicant
1. Mr. Nazeer Shaik	Indian	India	Asst. Professor, Dept.of.CSE, Srinivasa Ramanujan Institute of Technology, Autonomous-Anantapur, Andhra Pradesh, 515001, India.
2. J L. Sarwani Theeparthi	Indian	India	Associate Professor, Dept of CSE, Aditya College of Engineering and Technology, Surampalem, Kakinada-Dist., Andhra Pradesh-533 437, India.
3. Mrs. Muddana.Rishitha Bhavani	Indian	India	Assistant Professor, Department of Cyber Security and Data Science, Bapatla Engineering College, Bapatla, Andhra Pradesh -522 102, India.
4. Mrs. Inaganti Bhavana	Indian	India	Assistant Professor, Department of Cyber Security and Data Science, Bapatla Engineering College, Bapatla, Andhra Pradesh -522 102, India.

5. Dr. Rahul Sharma	Indian	India	Assistant Professor, GDC KATHUA, 180001, KATHUA, Jammu and Kashmir, India.
6. Abarna. S	Indian	India	Assistant Professor, Department of Chemistry, SNS College of Technology
7. Mr. Rayavarapu Bhavani Sankar	Indian	India	Assistant Professor, Department of Computer Science and Engineering, Chirala Engineering College, Ramapuram Beach Road, Chirala, Bapatla District, Andhra Pradesh, 523157, India.
8. Mr. Chokkapu NarayanaRao	Indian	India	Assistant Professor, Department of CSE, Vignan's Institute of Engineering for Women(A), Visakhapatnam, Andhra Pradesh -530046, India.

3B. CATEGORY OF APPLICANT [Please tick (✓) at the appropriate category]			
Natural Person (✓)	Other than Natural Person		
	Small Entity ()	Startup ()	Others ()

4. INVENTOR(S) [Please tick (✓) at the appropriate category]		
Are all the inventor(s) same as the applicant(s) named above?	Yes (✓)	No ()

If "No", furnish the details of the inventor(s)

Name in Full	Nationality	Country of Residence	Address of the Inventor
Same as Applicant			

5. TITLE OF THE INVENTION		
"DETECTION OF MALICIOUS BLOCKCHAIN ATTACKS USING FEDERATED LEARNING"		
6. AUTHORISED REGISTERED PATENT AGENT(S)	IN/PA No.	
	Name	
	Mobile No.	
7. ADDRESS FOR SERVICE OF	Name	

APPLICANT IN INDIA	Postal Address	Vadasithur, Kinathukadavu, Coimbatore - 641202, India
	Telephone No.	
	Mobile No.	
	Fax No.	
	E-mail ID	

~~8. IN CASE OF APPLICATION CLAIMING PRIORITY OF APPLICATION FILED IN CONVENTION~~
~~COUNTRY, PARTICULARS OF CONVENTION APPLICATION~~

~~Country~~	~~Application Number~~	~~Filing date~~	~~Name of the applicant~~	~~Title of the invention~~	~~IPC (as classified in the convention country)~~

~~9. IN CASE OF PCT NATIONAL PHASE APPLICATION, PARTICULARS OF INTERNATIONAL APPLICATION FILED UNDER PATENT CO-OPERATION TREATY (PCT)~~

~~International application number~~	~~International filing date~~

~~10. IN CASE OF DIVISIONAL APPLICATION FILED UNDER SECTION 16, PARTICULARS OF~~
~~ORIGINAL (FIRST) APPLICATION~~

~~Original (first) application No.~~	~~Date of filing of original (first) application~~

~~11. IN CASE OF PATENT OF ADDITION FILED UNDER SECTION 54, PARTICULARS OF MAIN~~
~~APPLICATION OR PATENT~~

~~Main application/patent No.~~	~~Date of filing of main application~~

12. DECLARATIONS

(i) Declaration by the inventor(s)

(**In case the applicant is an assignee**: the inventor(s) may sign herein below or the applicant may upload the assignment or enclose the assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period).

I/We, the above-named inventor(s) is/are the true & first inventor(s) for this Invention and declare that the applicant(s) herein is/are my/our assignee or legal representative.

(a) Date 09/11/2023

(b) Name	(c) Signature
1. Mr. Nazeer Shaik 2. J L. Sarwani Theeparthi 3. Mrs. Muddana.Rishitha Bhavani 4. Mrs. Inaganti Bhavana 5. Dr. Rahul Sharma 6. Abarna. S 7. Mr. Rayavarapu Bhavani Sankar 8. Mr. Chokkapu NarayanaRao	

~~**(ii) Declaration by the applicant(s) in the convention country**~~

~~**(In case the applicant in India is different than the applicant in the convention country:** the applicant in the convention country may sign herein below or applicant in India may upload the assignment from the applicant in the convention country or enclose the said assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period)~~

~~I/We, the applicant(s) in the convention country declare that the applicant(s) herein is/are my/our assignee or legal representative.~~

~~(a) Date~~

~~(b) Signature(s)~~

~~(c) Name(s) of the signatory~~

(iii) Declaration by the applicant(s)

I/We the applicant(s) hereby declare(s) that: -

- ~~I am/~~ We are in possession of the above-mentioned invention.
- The ~~provisional~~/complete specification relating to the invention is filed with this application.

- ☐ The invention as disclosed in the specification uses the biological material from India and the necessary permission from the competent authority shall be submitted by me/us before the grant of patent to me/us.
- ☐ There is no lawful ground of objection(s) to the grant of the Patent to me/us.
- ☐ I am/we are the true & first inventor(s).
- ☐ I am/we are the assignee or legal representative of true & first inventor(s).
- ☐ The application or each of the applications, particulars of which are given in Paragraph-8, was the first application in convention country/countries in respect of my/our invention(s).
- ☐ I/We claim the priority from the above mentioned application(s) filed in convention country/countries and state that no application for protection in respect of the invention had been made in a convention country before that date by me/us or by any person from which I/We derive the title.
- ☐ My/our application in India is based on international application under Patent Cooperation Treaty (PCT) as mentioned in Paragraph-9.
- ☐ The application is divided out of my /our application particulars of which is given inParagraph-10 and pray that this application may be treated as deemed to have been filed on DD/MM/YYYY under section 16 of the Act.
- ☐ The said invention is an improvement in or modification of the invention particulars of which are given in Paragraph-11.

13. FOLLOWING ARE THE ATTACHMENTS WITH THE APPLICATION

(a) Form 2

Item	Details	Fee	Remarks
Complete/ Provisional specification) #	No. of pages: 15		
No. of Claim(s)	No. of claims: 01 No. of pages: 01		
Abstract	No. of pages: 01		
No. of Drawing(s)	No. of drawings:02 No. of pages: 02		

In case of a complete specification, if the applicant desires to adopt the drawings filed with his provisional specification as the drawings or part of the drawings for the complete specification under rule 13(4), the number of such pages filed with the provisional specification are required to be mentioned here.

(b) Complete specification (in conformation with the international application)/as amended before the International Preliminary Examination Authority (IPEA), as applicable (2 copies).

(c) Sequence listing in electronic form

(d) Drawings (in conformation with the international application)/as amended before the International Preliminary Examination Authority (IPEA), as applicable (2 copies).

(e) Priority document(s) or a request to retrieve the priority document(s) from DAS (Digital Access Service) if the applicant had already requested the office of first filing to make the priority document(s) available to DAS.

(f) Translation of priority document/Specification/International Search Report/International Preliminary Report on Patentability.

(g) Statement and Undertaking on Form 3

(h) Declaration of Inventorship on Form 5

(i)Power of Authority

(j)**Total fee ₹…….in Cash/ Banker's Cheque /Bank Draft bearing No..... Date on ..... Bank.**

I/We hereby declare that to the best of my/our knowledge, information and belief the fact and matters slated herein are correct and I/We request that a patent may be granted to me/us for the said invention.

Dated this 09th day of November, 2023

Signature:

Name: Mr. Nazeer Shaik

To,

The Controller of Patents
The Patent Office, at
Chennai

Note: -

* Repeat boxes in case of more than one entry.
* To be signed by the applicant(s) or by authorized registered patent agent otherwise where mentioned.
* Tick ()/cross (x) whichever is applicable/not applicable in declaration in paragraph-12.
* Name of the inventor and applicant should be given in full, family name in the beginning.
* Strike out the portion which is/are not applicable.
* For fee: See First Schedule";

FORM 2

THE PATENTS ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003
COMPLETE SPECIFICATION
(See sections 10; rule 13)

TITLE OF THE INVENTION

DETECTION OF MALICIOUS BLOCKCHAIN ATTACKS USING FEDERATED LEARNING

APPLICANT

NAME: MR. NAZEER SHAIK, J L. SARWANI THEEPARTHI, MRS. MUDDANA.RISHITHA BHAVANI, MRS. INAGANTI BHAVANA, DR. RAHUL SHARMA, ABARNA. S, MR. RAYAVARAPU BHAVANI SANKAR, MR. CHOKKAPU NARAYANARAO

NATIONALITY: INDIA

ADDRESS: ASST. PROFESSOR, DEPT.OF.CSE, SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY, AUTONOMOUS-ANANTAPUR, ANDHRA PRADESH, 515001, INDIA.

DETECTION OF MALICIOUS BLOCKCHAIN ATTACKS USING FEDERATED LEARNING

Technical Field

[0001] The embodiments herein generally relate to a method for an detection of malicious blockchain attacks using federated learning.

Description of the Related Art

[0002] With the advancement of the internet era, attack behaviors such as internal threats, zero day vulnerabilities, and DoS attacks grow more prevalent, and intrusion detection becomes an important way of network attack detection. Federal Learning (Federal Learning) is a distributed machine Learning technology that breaks down data islands and unlocks the potential of artificial intelligence applications, and it can enable all Federal Learning participants to realize joint modelling by exchanging encrypted machine Learning intermediate results on the basis of not disclosing encryption forms of bottom data and bottom data. The goal is to develop machine learning models jointly, with no data being sent from one participant to the next. A blockchain is a distributed book in which data blocks sequentially build a chained data structure. Blockchains are widely employed in various sectors due to their decentralized, non-falsifiable, and non-forgeable characteristics. Because the points of attack are spread across numerous places, such attacks are known as distributed denial of service attacks, which can occur in multiples. Deep learning is a critical component of artificial intelligence technology, but its superior performance is frequently dependent on a significant amount of high-quality training data. Data is retained on client devices throughout training across mobile devices, and only model parameters are transferred to the server for aggregate. The federal

learning-based DDoS detection technique successfully tackles the problem of privacy disclosure, uses data mastered by all participants to train a local model and exchange model parameters to realize multi-party common modelling, and can complete joint training without uploading data. Current blockchain techniques have found widespread use in a variety of frontier fields.

[0003] Under the situation that data is not local, an industrial internet network traffic intrusion detection algorithm based on a federal learning architecture can construct a global detection model. In related art, most security privacy protection solutions in the longitudinal federated learning scene primarily handle a privacy leakage problem of participants in a process of intermediate result exchange in an iterative process. A flooding assault is the most prevalent type of DDoS attack, in which an attacker attacks a target server with scattered and large-flow malicious data packets, rendering the system unavailable. A machine learning approach is commonly employed in the related art to detect a data stream, that is, a detection model is trained on line, and then the data stream is detected on line to determine if the data stream is an attack data stream. Federal learning, like the general deep learning model, has various security vulnerabilities. Federal learning may experience counterattack during the system reasoning phase. This opens the door for a hostile client to control the training process. The previous art provides a credit evaluation method for evaluating a federal learning participant's credit, which alleviates the problem of multi-party trust to some extent, and primarily takes interactive credit as a primary component, and requires a block chain to evaluate a training model of each round. Data preparation is used to remove the impact of data irregularity, such as the elimination of irregular values and feature normalization.

[0004] In order to safeguard data privacy, building a worldwide network traffic intrusion detection model and detecting zero-day assaults becomes an urgent problem that must be tackled. The central server distributes the current combined model to randomly selected clients in each iteration of federal learning, and the clients independently calculate the gradient of the model based on local data from the clients and transmit the gradient to the central server to be aggregated to calculate a new global model. A data set is vertically segmented and held by different players in a longitudinal federated learning scene; that is, each participant possesses a separate attribute subset. It is difficult to find a trusted central node without failure in the block chain P2P network topology, and the entire training process generates a huge amount of communication overhead. The accuracy of the detection model in detecting the newly added data stream in order to realize correct classification of the newly added data stream is a challenge in the industry that has to be solved. If a hostile player attacks a central server in the vertical federal learning system, the other participants will be directed to incorrect reasoning findings. Backdoor attacks aim to ensure that the learnt model behaves differently on some target subtasks while still doing well on the major task. A number of local nodes have access to local data sets and processing resources, can meet the requirement for local model training, have model aggregation capacity, and can aggregate models sent by other nodes. To generate a trained target longitudinal federated learning model, propagate backwards the final mistake to update model parameters of a sub-model in each layer of the longitudinal federated learning model, and loop iterate until a pre-review stop condition is satisfied. Furthermore, in a one-to-one communication mode, the communication overhead generated by one round of training is significantly smaller than that generated by centralized federal learning, allowing resource-limited nodes in an actual blockchain scene to be greatly reduced.

SUMMARY

[0005] In view of the foregoing, an embodiment herein provides a method for detection of malicious blockchain attacks using federated learning. In some embodiments, wherein the data preparation module is used to remove the feature that the missing value in the data set exceeds a specific proportion, to transform the type of text data into numerical data, and to normalize the numerical data into a given numerical value range. The current local model deciding module is responsible for receiving training data sent by the server and determining a current local model based on the training data. The local data set of the local node is processed to obtain local node pretreatment data, which consists of a training set and a test set. To obtain an intermediate detection model corresponding to each initial detection model, perform incremental learning on each initial detection model depending on the data stream to be detected. The active computing node resists and trains the central server model by merging the resistance sample data supplied by the verification committee, so strengthening the central server model's ability to defend against attacks. Federated learning is combined with block chain, buffering time constraints are implemented, and clients who are unable to upload local models on time are excluded.

[0006] In some embodiments, wherein the mining nodes vote jointly on the local detection model parameters of a specific working node, and if the working node's marked legal number is greater than the illegal number, the working node is considered legal. The current federal model updating module is used to update the current federal model based on the most recent data. The Lipschitz neural network is a full connection layer in the first bottom layer sub-model and/or a full connection layer in the second bottom layer sub-model. Encrypting each gradient using the session key to produce an encrypted gradient for each intermediate

detection model. The created countermeasure sample is established as a countermeasure sample database by using the block chain's database function, and the countermeasure sample is offered for the active party's countermeasure training, so reinforcing the vertical federal system. The cutting condition is provided to the client in the federal learning process utilizing the features of block chain openness and non-falsification, so that the appropriate cutting rate is determined and the global model is protected from being attacked by a backdoor. The global model is a model that was created by using an aggregation algorithm to safely aggregate local models of other domains and performing multiple iterations. It has DDoS attack knowledge of multiple domains and can detect attack types of other domains in addition to identifying attacks in a local data set.

[0007] In some embodiments, wherein the block chain is added into the federal learning architecture to remove the interference of malicious nodes in the training process and to improve the training process's safety and privacy protection performance. A computer programmer product is given that includes a computer programmer that, when executed by a processor, implements the technique of generating a federated model described in any of the embodiments of the current disclosure. A Lipschitz constant constraint is applied to each layer of the Lipschitz neural network, and the Lipschitz constraint of the Lipschitz neural network is a product of the Lipschitz constant constraints of each layer of the Lipschitz neural network. In the second stage's fine granularity detection, based on the data flow to be detected, train an initial detection model on each edge node using federal learning, so that each distributed malicious site that launches a DDoS attack may be determined sensitively. The data uploaded to the block is used to build a sample detector, and the countermeasure sample uploaded by the malicious participant can be efficiently identified, allowing the participant to be evaluated

as a malicious node or not. A participant registration submodule, a participant administration submodule, and a participant credit calculation submodule compose the block chain credit evaluation module.

[0008] These and other aspects of the embodiments herein will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. It should be understood, however, that the following descriptions, while indicating preferred embodiments and numerous specific details thereof, are given by way of illustration and not of limitation. Many changes and modifications may be made within the scope of the embodiments herein without departing from the spirit thereof, and the embodiments herein include all such modifications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The embodiments herein will be better understood from the following detailed description with reference to the drawings, in which:

[0010] FIG. 1 illustrates a method for detection of malicious blockchain attacks using federated learning according to an embodiment herein; and

[0011] FIG. 2 illustrates a method for a schematic flow chart of a network traffic intrusion detection algorithm based on blockchain and federal learning according to an embodiment herein.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0012] The embodiments herein and the various features and advantageous details thereof are explained more fully with reference to the non-limiting embodiments that are

illustrated in the accompanying drawings and detailed in the following description. Descriptions of well-known components and processing techniques are omitted so as to not unnecessarily obscure the embodiments herein. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein may be practiced and to further enable those of skill in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

[0013] FIG. 1 illustrates a method for detection of malicious blockchain attacks using federated learning according to an embodiment herein. In some embodiment, to obtain a fine representation of data features, each equipment node collaboratively constructs a sparse automatic encoder based on a block chain and federal learning during the feature extraction stage. After obtaining a trained model, all parties utilize the model to jointly establish a model prediction for a new sample in the prediction data set. When each node learns its local model, independent training is performed using a random gradient descent method SGD based on the set learning rate lr, training round number M, and other parameter information. These packets are disguised and their source is unknown, and the services sought by these packets frequently demand a huge amount of system resources, preventing the target host from providing normal services to the user and even triggering a system crash. An active participant in a vertical federal system of a social network initiates a joint training task with the goal of training an interest and hobby prediction model for predicting a user's interest and hobby and achieving the goal of accurate recommendation by a downstream recommendation algorithm. These tunnels are private sub-networks that allow for the isolated communication of at least two peers. Only peers connected to the channel have access to read, submit, and validate transactions. Participants generate a local model by preprocessing a local data set and

executing local parameter adjustment training on machine learning or deep learning models such as a neural network and the like.

[0014] In some embodiment, the data pseudo tags with greater confidence coefficients are given during the pseudo tag creation stage by performing confidence coefficient evaluation on the network's last layer output. In federated learning, the server is a device that aggregates model data taught by numerous clients. The server and the client communicate. And the data to be trained is utilized by the client to train with the local sample data to create updated data, which is then communicated back to the server to be aggregated with the updated data of other clients to create a new model. The federal learning process may be more clearly described as follows: the client performs model training on the global model using local sample data, calculates gradient, updates model parameters, and sends the revised data to the server. To achieve Byzantine robustness, analyze the updated gradient with a hidden Markov model or a secure aggregation technique to identify the rogue user. During the training phase, each node can communicate the local model to other nodes via equipment such as a local mobile phone, a notebook computer, and so on, and each node's local model can be converged after numerous rounds of iterative updating. Fields such as IP address, port number, data packet number, and so on are used to calculate an entropy value, monitor the inflow traffic of the edge switch, and create an algorithm flow to detect malicious traffic. The generative countermeasure network is composed of two components: an attack generator network G and a discriminator network D. The private key is used for hash encryption when the client side encrypts the local area model, and the independent communication channel uses the public key to decrypt the encrypted local area model. The fully-connected neural network has three layers: an input layer, a hidden layer, and an output layer.

[0015] In some embodiment, the furthermore, based on the schematic design, the mining nodes in the block chain validate the validity of the local detection model parameters uploaded by the working nodes, and the mining nodes receive model verification rewards, while the legal working nodes receive model training rewards. Aggregating the update data entails, for example, conducting a weighted Average on the update data provided by each client using a federal Average method, and updating the data to be trained based on the calculation result. A longitudinal federated learning system's anti-attack capabilities can be strengthened, and dirty data and malicious update spread can be effectively limited to resist attacks. When each node trains its own local model, independent training is performed using a Stochastic Gradient Descent (SGD) approach based on parameter information set by each node such as the learning rate lr, training round number M, and so on. DDoS detection method with high efficiency and accuracy for DDoS detection and mixing machine learning. The approach can effectively protect SDN network controllers against DDoS attacks, allowing the controllers to function properly.

[0016] The generated countermeasure sample data is fed into a discriminator, where the probability of classification and the cross entropy of the positive sample label are used as the loss function of a generator, with the goal of making the generated countermeasure sample and the positive sample more similar. The first cutting occurs at a higher amplitude cutting rate, and when the model is cut, the central server adds the differential privacy noise to the cut model received after cutting. Identity information management, data management, and task management are the three components of participant information management.

[0017] FIG. 2 illustrates a method for a schematic flow chart of a network traffic intrusion detection algorithm based on blockchain and federal learning according to an

embodiment herein. In some embodiments, the voting mechanism can successfully eradicate malicious nodes as long as the malicious mining nodes participating in the vote verification process do not exceed one-third of the total voting nodes. The weight matrices of the network layers and/or the gradients of the network layers may be provided to the server as update data. The gradient propagates both forwards and backwards. The model training process can be separated into several model parameter updating stages. The first participant device inputs the first training data into the first bottom layer sub-model during a model parameter update procedure to get the first bottom layer output data. The experimental findings of the preceding methods show that the system can detect DDoS attacks in the block chain, is practicable and expandable, and can be used to real-world block chain situations. The cloud edge collaborative detection approach uses the entropy value measurement method to pick the optimum Self-organization map (SOM), classifies SOM neurons, and employs KD-trees to identify flows at a finer granularity, improving detection accuracy. Furthermore, an active party in the federal learning system can use the blockchain's database function to create an antagonistic sample database, and a source of the antagonistic sample is supplied for the antagonistic training of the central server model.

[0018] The central server can optimize the cutting rate to create an optimum cutting effect by repeating the model cutting and model verification operations, however at the time, the model is mainly erased by the injected backdoor features, so the effect is lost. Encrypting and uploading local model parameters to an aggregate server to produce a global model, then training iteratively to generate a final global model.

[0019] In some embodiments, after downloading the most recent block from the block chain, the working node updates the model parameters using the Federal aggregation process

after removing malicious model parameters depending on the vote results. To receive updated data, the client is used to train a neural network model that is not reliant on the constraint condition of the Leptochis constant, and the structure of the standard fully-connected neural network model is the same as that of the present local model. Lipschitz constant restrictions and neural network expression capabilities are sometimes thought to be mutually exclusive objectives. Meanwhile, when compared to a single node training approach, the result demonstrates the efficacy of collaborative training in the innovation. Second, a Snort intrusion detection system and an SAE deep learning model are installed on a control plane to improve detection precision. The non-tamper and accounting properties of block chain technology can record the historical contribution degree of each participant in the federal learning system, providing a foundation for discovering the malicious player. The processor could be a Central Processing Unit (CPU), a microprocessor unit (MPU), a Digital Signal Processor (DSP), or a Field Programmable Gate Array (FPGA), which could enable a block chain-based defense against federal learning backdoor assaults. A local training sub-module for performing data preprocessing and feature selection on the federated learning data set, as well as local training utilizing a machine learning or deep learning algorithm on the feature-selected data set.

[0020] In some embodiments, some or all of the modules may be chosen based on actual needs to fulfil the goal of this embodiment's solution. Without any imaginative effort, a person of ordinary proficiency in the art may grasp and implement it. Furthermore, the basic weighted average cannot prevent malicious updates made by attackers, and can even lead the model to collapse in the case of a multi-attacker combination attack. The longitudinal federated learning model contains a first bottom layer sub-model, an interaction layer sub-model, a top layer sub-model based on a Lipschitz neural network, and a second bottom layer sub-model in

a second participant device in the first participant device. The first baseline approach is a centralized learning-based DDoS detection method, while the second baseline method is a typical centralized joint learning technology-based DDoS detection method. The existing method has the problems of being inefficient, detecting the same attack flow multiple times, wasting resources, and being inefficient because the detection result is not shared across the nodes. In the vertical federal system, a malicious node detection and reinforcing mechanism is built, and the vertical federal model's safety and usability are improved. Following the completion of the aggregation, the central server provides the global model to the client over the separate communication channel and prepares for the next round of training.

CLAIMS

I/We Claim:

1. A method for detection of malicious blockchain attacks using federated learning, wherein the method comprises;

aiming for a local flow data set generated by each device in the industrial Internet during the manufacturing process, detecting and marking novel attacks independently using an unmarked attack type detection model to acquire local pseudo tag data and tagged data;

receiving training data given by a server and determining a current local model based on the training data;

acquiring second bottom layer output data received by the second participant device, where the second bottom layer output data is obtained utilizing the second training data and the second bottom layer sub-model;

inputting the training set of the local node pretreatment data into an LSTM model of the local node for training in order to generate the final model of the local node;

obtaining a target detection model, train an initial detection model on each edge node using federal learning based on the data stream to be detected under the constraint that the detection result is abnormal;

the active computing node resists and trains the central server model by merging resistance sample data supplied by the verification committee, so strengthening the central server model's ability to defend against attacks;

the client receives a pruning model added with disturbance corresponding to local data from the verification account book via an independent channel and submits a verification result to the central server;

each domain participant preprocesses a local federal learning data set and uses the preprocessed data set to train a neural network machine learning model or a deep learning model locally; and

the edge terminals participating in federal learning employ local data to perform model training in order to determine the gradient of the local model.

Dated this, 04th November, 2023.

Signature

ABSTRACT

DETECTION OF MALICIOUS BLOCKCHAIN ATTACKS USING FEDERATED LEARNING

A method for the development of the invention proposes a network flow intrusion detection technique based on a block chain and federal learning, which includes the processes listed below: Each device detects and labels the novel attack independently, so establishing a global model. After feeding a training sample set into the current local model and training it, the product of the weight matrix norm and the gradient norm of each network layer in the current local model satisfies the constraint condition of a Richest constant. A first bottom layer sub-model, an interaction layer sub-model, a top layer sub-model based on a Lipschitz neural network, and a second bottom layer sub-model in a second participant device comprise the longitudinal federated learning model. The block chain DDoS attack is efficiently recognized, and the communication overhead in the training process is considerably minimized. By using a two-stage detection mode, system resources are saved; by training each initial detection model using the federal learning method, each distributed malicious host that initiates a DDoS attack can be determined, the accuracy of DDoS detection is improved, and a user's privacy is protected. The approach can detect rogue nodes and strengthen the vertical federal learning system.

FIG.1

FORM 3

THE PATENTS ACT,
1970 (39 of 1970)
and
THE PATENTS RULES, 2003

STATEMENT AND UNDERTAKING UNDER SECTION 8

(See section 8; Rule 12)

1. Name of the applicant(s).	I/We Mr. Nazeer Shaik, J L. Sarwani Theeparthi, Mrs. Muddana.Rishitha Bhavani, Mrs. Inaganti Bhavana, Dr. Rahul Sharma, Abarna. S, Mr. Rayavarapu Bhavani Sankar, Mr. Chokkapu NarayanaRao, all are citizen of India, Address of one of the Applicant: Asst. Professor, Dept.of.CSE, Srinivasa Ramanujan Institute of Technology, Autonomous-Anantapur, Andhra Pradesh, 515001, India.
2. Name, address and nationality of the joint applicant.	(i) that I/We have not made any application for the same/substantially the same invention outside India Or (ii) ~~that I/We who have made this application No… dated alone/jointly with~~ ..... ~~, made for the same/ substantially same invention, application(s) for patent in the other countries, the particulars of which are given below:~~

Name of the Country	Date of Application	Application No.	Status of the Application	Date of Publication	Date of grant
-	-	-	-	-	-

3. Name and address of the assignee	(iii) that the rights in the application(s) has/have been assigned to …… none …… …… …… that I/We undertake that up to the date of grant of the patent by the Controller, I/We would keep him informed in writing the details regarding corresponding applications for patents filed outside India within six months from the date of filing of such application. **Dated this 09th day of November, 2023**

4. To be signed by the applicant or his authorized registered patent agent.	**Signature:**
5. Name of the natural person who has signed.	Mr. Nazeer Shaik **Name of the Applicant(s)**
	To The Controller of Patents, The Patent Office, at Chennai

FORM 9

THE PATENT ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003

REQUEST FOR PUBLICATION

[See section 11A (2) rule 24A]

I/We **MR. NAZEER SHAIK, J L. SARWANI THEEPARTHI, MRS. MUDDANA.RISHITHA BHAVANI, MRS. INAGANTI BHAVANA, DR. RAHUL SHARMA, ABARNA. S, MR. RAYAVARAPU BHAVANI SANKAR, MR. CHOKKAPU NARAYANARAO** hereby request for early publication of my/our Patent Application.

Dated **09/11/2023 00:00:00** under section 11A (2) of the Act.

Dated this (Final Payment Date): ----------
--

Signature

Name of the signatory

To,
The Controller of Patents,
The Patent Office,
At Chennai

APPLICANT: MR. NAZEER SHAIK, J L. SARWANI THEEPARTHI, MRS. MUDDANA.RISHITHA BHAVANI, MRS. INAGANTI BHAVANA, DR. RAHUL SHARMA, ABARNA. S, MR. RAYAVARAPU BHAVANI SANKAR, MR. CHOKKAPU NARAYANARAO

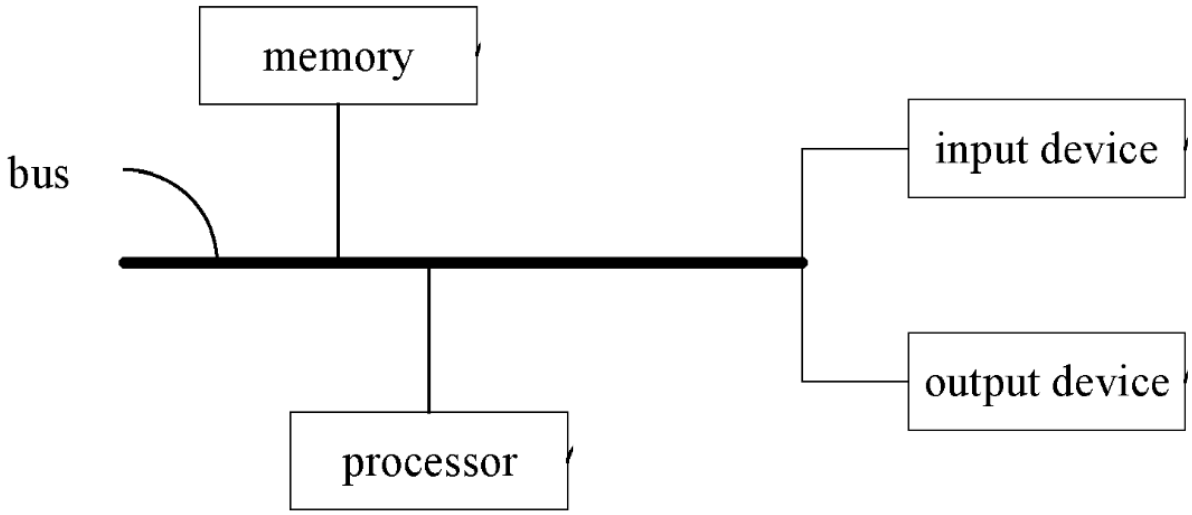

FIG.1.

APPLICANT: MR. NAZEER SHAIK, J L. SARWANI THEEPARTHI, MRS. MUDDANA.RISHITHA BHAVANI, MRS. INAGANTI BHAVANA, DR. RAHUL SHARMA, ABARNA. S, MR. RAYAVARAPU BHAVANI SANKAR, MR. CHOKKAPU NARAYANARAO

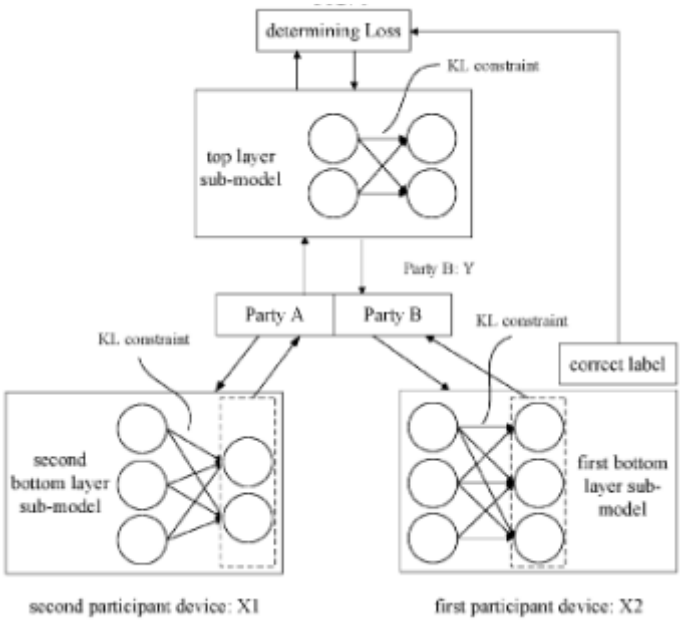

FIG.2.

Welcome Kalaimathi Sign out

Controller General of Patents, Designs & Trade Marks

सत्यमेव जयते

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

G.A.R.6
[See Rule 22(1)]
RECEIPT

Docket No 121125

Date/Time 2023/11/10 10:55:55

To
Kalaimathi

UserId: VIP.kalai

6/1, vadasithur post, kinathukadavu,
Coimbatore - 641202

CBR Detail:

Sr. No.	App. Number	Ref. No./Application No.	Amount Paid	C.B.R. No.	Form Name	Remarks
1	202341076807	TEMP/E-1/90836/2023-CHE	1600	51939	FORM 1	DETECTION OF MALICIOUS BLOCKCHAIN ATTACKS USING FEDERATED LEARNING
2	E-12/10729/2023/CHE	202341076807	2500	51939	FORM 9	----

TransactionID	Payment Mode	Challan Identification Number	Amount Paid	Head of A/C No
N-0001253207	Online Bank Transfer	1011230005281	4100.00	1475001020000001

Total Amount : ₹ 4100.00
Amount in Words: Rupees Four Thousand One Hundred Only

Received from Kalaimathi the sum of ₹ 4100.00 on account of Payment of fee for above mentioned Application/Forms.
* This is a computer generated receipt, hecnce no signature required.

Print

Home About Us Contact Us