Electronic Acknowledgement Receipt

EFS ID:	43815238
Application Number:	17480070
International Application Number:	
Confirmation Number:	1068
Title of Invention:	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT
First Named Inventor/Applicant Name:	Won Ki HONG
Customer Number:	157354
Filer:	Soyeon P. Laub
Filer Authorized By:	
Attorney Docket Number:	122326-5011
Receipt Date:	20-SEP-2021
Filing Date:	
Time Stamp:	21:15:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$830
RAM confirmation Number	E20219JL16092344
Deposit Account	500310
Authorized User	Soyeon Laub

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.16 (National application filing, search, and examination fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	122326-5011_ADS.pdf	1256327 acd9c3c983e9ffde640a14cc14341e83392aa8aa	no	9
Warnings:					
Information:					
2		122326-5011_Application.pdf	420092 762d6d0cd3f318597199a21061b89d54d7ce7c37	yes	35

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	25
	Claims	26	30
	Abstract	31	31
	Drawings-only black and white line drawings	32	35

Warnings:					
Information:					
3	Oath or Declaration filed	122326-5011_Declarations.pdf	204472 e844cdcd6b408d43bdaeacbb9bcf045c789fc1d4	no	4
Warnings:					
Information:					
4	Power of Attorney	122326-5011_POA.pdf	953592 4881ff3169125fb9bd337415ab58f6b7666aaaa3	no	2
Warnings:					
Information:					

5	Request for USPTO to retrieve priority docs	122326-5011_SB38.pdf	204449 14cf51d4a09a8f89001cbb3ce34fca496fe09ad4	no	1
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	44097 85bc6dde4d347576843813112b8bdda80994260b	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	3083029	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT
First Named Inventor/Applicant Name:	Won Ki HONG
Filer:	Soyeon P. Laub
Attorney Docket Number:	122326-5011

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**830**

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Won Ki		HONG	

Residence Information (Select One) US Residency ● Non US Residency Active US Military Service

City	Country of Residence [i]
Pohang-si	KR

Mailing Address of Inventor:

Address 1	328-304, 319, Jigok-ro, Nam-gu
Address 2	Gyeongsangbuk-do
City	Pohang-si
State/Province	
Postal Code	37671
Country [i]	KR

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jae Hyoung		YOO	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Country of Residence [i]
Seoul	KR

Mailing Address of Inventor:

Address 1	211-1303, 135, Olympic-ro, Songpa-gu
Address 2	
City	Seoul
State/Province	
Postal Code	05502
Country [i]	KR

Inventor 3 Remove

Legal Name

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Ji Bum		HONG	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Seoul	Country of Residence [i]	KR

Mailing Address of Inventor:

Address 1	612-1801, 28, Dobong-ro 136-gil, Dobong-gu
Address 2	

City	Seoul	State/Province	
Postal Code	01398	**Country** [i]	KR

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Su Hyun		PARK	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Seoul	Country of Residence [i]	KR

Mailing Address of Inventor:

Address 1	101-1003, 20, World Cup buk-ro 38ga-gil, Mapo-gu
Address 2	

City	Seoul	State/Province	
Postal Code	03941	**Country** [i]	KR

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	157354		
Email Address		Add Email	Remove Email

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

Application Information:

Title of the Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT		
Attorney Docket Number	122326-5011	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	**Suggested Figure for Publication (if any)**	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	157354		

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
10-2021-0018674	KR	2021-02-09	6AF1

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 — Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	POSTECH Research and Business Development Foundation		
Mailing Address Information For Applicant:			
Address 1	77, Cheongam-ro, Nam-gu		
Address 2	Gyeongsangbuk-do		
City	Pohang-si,	**State/Province**	
Country	KR	Postal Code	37673
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Soyeon P. Laub/			Date (YYYY-MM-DD)	2021-09-20
First Name	Soyeon P.	Last Name	Laub	Registration Number	39,266

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	122326-5011
	Application Number	
Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT	

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
WON KI HONG	09/06/2021
JAE HYOUNG YOO	09/06/2021
JI BUM HONG	09/06/2021
SU HYUN PARK	09/06/2021

RECEIVING PARTY DATA

Name:	POSTECH RESEARCH AND BUSINESS DEVELOPMENT FOUNDATION
Street Address:	77, CHEONGAM-RO, NAM-GU
Internal Address:	GYEONGSANGBUK-DO
City:	POHANG-SI
State/Country:	KOREA, REPUBLIC OF
Postal Code:	37673

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	17480070

CORRESPONDENCE DATA

Fax Number: (714)830-0700
Phone: 714-830-0600
Email: lori.tillman@morganlewis.com, OCIPDocketing@morganlewis.com
Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.
Correspondent Name: MORGAN, LEWIS & BOCKIUS LLP
Address Line 1: 600 ANTON BOULEVARD
Address Line 2: SUITE 1800
Address Line 4: COSTA MESA, CALIFORNIA 92626-7653

ATTORNEY DOCKET NUMBER:	122326-5011
NAME OF SUBMITTER:	SOYEON P. LAUB, REG. # 39,266
Signature:	/Soyeon P. Laub/

Date:	09/23/2021

Total Attachments: 3
source=122326-5011_Assignment#page1.tif
source=122326-5011_Assignment#page2.tif
source=122326-5011_Assignment#page3.tif

RECEIPT INFORMATION

EPAS ID:	PAT6933263
Receipt Date:	09/23/2021

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT

As the below named inventor, I hereby declare that:

This declaration is directed to:

☒ The attached application, or

☐ United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

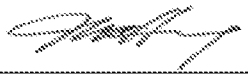
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Won Ki HONG Date (Optional): September 6, 2021

Signature: 

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT

As the below named inventor, I hereby declare that:

This declaration is directed to:

☒ The attached application, or

☐ United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

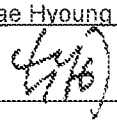
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Jae Hyoung YOO Date (Optional): September 6, 2021

Signature: 

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT

As the below named inventor, I hereby declare that:

This declaration is directed to:

☒ The attached application, or

☐ United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Ji Bum HONG Date (Optional): September 6, 2021

Signature: 홍지범

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT

As the below named inventor, I hereby declare that:

This declaration is directed to:

☒ The attached application, or

☐ United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

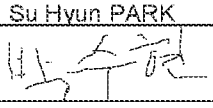
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Su Hyun PARK Date (Optional): September 6, 2021

Signature: 

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

Doc Code: PD.REQ.RETR
Document Description: Request for USPTO to retrieve priority docs

PTO/SB/38 (02-20)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Request to Retrieve Electronic Priority Application(s)

Send completed form to: Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

COMPLETE IF KNOWN	
Application Number	Not yet assigned
Filing Date	Concurrently herewith
First Named Inventor	Won Ki HONG
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	122326-5011

Pursuant to 37 CFR 1.55(i), the undersigned hereby requests that the USPTO retrieve an electronic copy of each of the following foreign applications for which priority has been claimed under 35 U.S.C. 119(a)-(d) from a foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement. This Request must be submitted:

- within the later of sixteen months from the filing date of the prior foreign application or four months from the actual filing date of an application under 35 U.S.C. 111(a),
- within four months from the later of the date of commencement (37 CFR 1.491(a)) or the date of the initial submission under 35 U.S.C. 371 of an application entering the national stage under 35 U.S.C. 371, or
- with a petition under 37 CFR 1.55(e) or (f).

☐ **OPTION A**

Please retrieve the priority application identified in Column C, a certified copy of which is contained in the EP or JP application identified in Columns A and B:

	A	B			C	
	Code for Participating Office (EP or JP only)	Application containing the non-participating priority application			Non-participating priority application to be retrieved	
		App. No.	Filing Date	Access Code (for JP only)	Country Code	App. No.
1						

☑ **OPTION B**

This Request may be used for the infrequent circumstance when a claim for priority to an application filed in a participating foreign intellectual property office was made prior to that foreign intellectual property office becoming a participating foreign intellectual property office.

Please retrieve the priority application identified in Columns A and B:

	A	B		
	Code for Participating Office (e.g., EP) or WIPO DAS Depositing Office (e.g., AU, BR, CN, DK, EA, EE, ES, FI, GB, IB, IN, JP, KR, MA, NL, NZ, SE)	Application to be retrieved		
		App. No.	Filing Date	Access Code (for WIPO DAS Depositing Office)
1	KR	10-2021-0018674	February 9, 2021	6AF1
2				

The USPTO will not attempt to retrieve the identified priority application(s) unless an identical claim for foreign priority to the application identified above is made pursuant to 37 CFR 1.55(d) or a petition is granted under 37 CFR 1.55(e) or (f). Applicants are advised to consult Private PAIR (accessed through www.uspto.gov) to assure that the retrieval has been successful. The applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period set forth in 37 CFR 1.55(g)(1).

I hereby declare that I have the authority to grant access to the above-identified foreign application(s).

/Soyeon P. Laub/	September 20, 2021
Signature	Date
Soyeon P. Laub	714-830-8600
Printed or Typed Name	Telephone Number
Attorney for Applicant	39,266
Title	Registration Number, if applicable

This collection of information is required by 37 CFR 1.55(d). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	Not yet assigned
Filing Date	Concurrently herewith
First Named Inventor	Won Ki HONG
Title	MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	122326-5011

SIGNATURE of Applicant or Patent Practitioner

Signature	/Soyeon P. Laub/	Date (Optional)	September 20, 2021
Name	Soyeon P. Laub	Registration Number	39,266
Title (if Applicant is a juristic entity)	Attorney for Applicant		
Applicant Name (if Applicant is a juristic entity)	POSTECH Research and Business Development Foundation		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 157354

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

POSTECH Research and Business Development Foundation

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	Nov 19, 2019
Name	Sang Woo Kim		
Title	Executive Director		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

U.S. PATENT APPLICATION FOR

MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT

Inventors: Won Ki HONG, residing in
Pohang-si, REPUBLIC OF KOREA

Jae Hyoung YOO, residing in
Seoul, REPUBLIC OF KOREA

Ji Bum HONG, residing in
Seoul, REPUBLIC OF KOREA

Su Hyun PARK, residing in
Seoul, REPUBLIC OF KOREA

Applicant: POSTECH Research and Business Development Foundation
77, Cheongam-ro, Nam-gu
Pohang-si, Gyeongsangbuk-do 37673
Republic of Korea

Entity: Small

MORGAN, LEWIS & BOCKIUS LLP
600 Anton Boulevard, Suite 1800
Costa Mesa, CA 92626-7653
714.830.0600

MACHINE LEARNING-BASED VNF ANOMALY DETECTION SYSTEM AND METHOD FOR VIRTUAL NETWORK MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to Korean Patent Application No. 10-2021-0018674, filed on February 9, 2021, with the Korean Intellectual Property Office (KIPO), the entire content of which is hereby incorporated by reference.

BACKGROUND

1. Technical Field

[0002] Exemplary embodiments of the present disclosure relate to a virtual network management-specific machine learning-based virtualized network function (VNF) anomaly detection system and method.

2. Related Art

[0003] With the rapid development of Software-Defined Networking (SDN)/Network Function Virtualization (NFV) technology, telecommunication operators and cloud data center operators are introducing and operating Virtualized Network Function (VNF) in which network functions are virtualized. As the scale is gradually increasing, new management issues, such as resource allocation and performance management of VNFs and fault management of a virtual network connecting VNFs, are increasing. In order to solve overall management issues related to SDN/NFV, it is necessary to check and analyze, in real time, resources used by VNF operating on a server inside a data center and abnormal states of a virtual network. In the past, abnormal states were detected based on a threshold in order to check the resources of the virtual network and the abnormal states of the network. Recently, along with an increase of attempts to manage networks without human intervention utilizing machine learning technology, an abnormal-state detection method based on machine learning technology is also emerging.

[0004] However, the conventional threshold-based detection method or machine learning-based detection method, which is for detecting abnormal states on the basis of relatively simple metrics such as the CPU utilization or memory usage of a server, has a problem in that it is highly likely to cause a false alarm. The present disclosure proposes a method of detecting an abnormal state of VNF based on a service state (anomaly detection). The proposing method includes a method of analyzing a network state and VNF resources through machine learning technology.

[0005] Anomaly detection is an important element of management and security of a virtual network and virtual resources that operate in an NFV environment such as a virtual machine (VM) and VNF, including a physical server operating inside a data center. Network managers use an abnormal-state detection method in order to check whether their services provided in a virtualized environment operate normally, whether the use state of allocated resources is appropriate, etc. and execute a policy appropriate to the situation.

[0006] There are two anomaly detection methods, i.e., a method of detecting an abnormal state of system resources and a method of detecting an abnormal state of network traffic. The method of detecting an abnormal state of system resources is a method of checking whether a CPU is being used excessively or whether a memory is insufficient by monitoring measurements such as CPU utilization, memory usage, and disk I/O access status. The method of detecting an abnormal state of network traffic uses a method of checking whether a sudden increase in traffic or a traffic attack such as a Denial of Service (DoS) occurs on the basis of the normal operating situation of the network traffic. Recently, many studies have been conducted to detect abnormal states by applying machine learning technology to the above two detection methods.

[0007] As the system resource-based detection method, which is one of the above two methods for detecting abnormal states of VNF in order to manage NFV environments, a method of utilizing a statistic approach to determine abnormal states on the basis of a threshold was widely

used in the past. Conventional detection methods set thresholds by utilizing statistical approaches such as a Seasonal Trend decomposition using LOESS (STL) algorithm that considers seasonality factors that change according to a fixed period in time-series data or 3-sigma rule that classifies a point apart from the mean of data distribution by three times the standard deviation as an exceptional situation. This statistical approach is efficient when the anomaly is defined as a single value, but has a limitation in that it cannot detect anomalies caused by complex conditions.

[0008] To this end, recently, studies are being conducted on detecting abnormal states of VNF using machine learning technology. Most of these studies are for detecting abnormal states utilizing supervised learning-based algorithms (Random Forest, Support Vector Machine, Neural Network, etc.) among three categories of machine learning such as supervised learning, unsupervised learning, and reinforcement learning. However, since most of the machine learning-based studies define abnormal states based on simple measurements such as CPU utilization and memory usage, it is necessary to define abnormal states in consideration of a resource usage state and whether Service Level Agreement (SLA) is violated in terms of services in operation.

[0009] In addition, conventional statistical-based and machine learning-based abnormal-state detection methods define abnormal states on the basis of measurement thresholds such as CPU, memory, and disk access. Also, with the machine learning-based abnormal-state detection method, it is possible to learn abnormal states through data correlations. However, the definition of the abnormal states has a limitation in that when a measurement for resource use temporarily rises for a short time, this causes false alarms and does not consider aspects of services provided through VNFs.

SUMMARY

[0010] Accordingly, exemplary embodiments of the present disclosure are provided to substantially obviate one or more problems due to limitations and disadvantages of the related art.

[0011] Exemplary embodiments of the present disclosure provide a more accurate anomaly detection method by defining an abnormal state in consideration of a service aspect such as an SLA violation when an abnormal state of a VNF is detected to manage an NFV environment.

[0012] To this end, data collected by monitoring resource usage, network states, and SLA violation information in a virtual network is applied to machine learning. The collected data undergoes a labeling process that extracts meaningful features from the collected data and classifies the data into normal and abnormal states so that the data can be used for learning based on a supervised learning-based machine learning algorithm.

[0013] The proposed method uses eXtreme Gradient Boosting (XGBoost), which is known to have the best performance among tree-based algorithms, for more accurate classification accuracy and faster training. Thus, an anomaly detection model is generated, and then the classification accuracy of the model is verified and used in an anomaly detection system.

[0014] Ultimately, the present disclosure aims to implement an anomaly detection system that overcomes the limitations of conventional methods by achieving high classification accuracy with little error.

[0015] According to an exemplary embodiment of the present disclosure for achieving the above-described objective, a virtual network management-specific machine learning-based virtualized network function (VNF) anomaly detection system, which is related to an abnormal-state detection apparatus for detecting an abnormal state of a VNF operating in a virtual network of a network function virtualization (NFV) infrastructure formed in a physical network through virtualization, may comprise: a data collection unit configured to collect normal state

data generated when a service is normally provided and abnormal state data generated through a fault injection method through a monitoring agent and a monitoring module in real time, store the collected data in a time-series database, and transmit the monitoring data to determine whether there is an abnormal state; and a data analysis unit configured to extract a feature necessary for detecting an abnormal state by pre-processing monitoring data received from the data collection unit and send data on the extracted data to an abnormal-state detection model so that the abnormal-state detection model analyzes data that is input in real time to determine whether there is an abnormal state and notifies a network manager when an abnormal state occurs.

[0016] The data collection unit may comprise a monitoring agent configured to periodically collect a resource usage state of each virtual machine operating in the virtual network and send collected monitoring data to the monitoring module; and a dashboard configured to provide the monitoring data stored in the database in time-series in a visualized form.

[0017] According to another exemplary embodiment of the present disclosure for achieving the above-described objective, a virtual network management-specific machine learning-based virtualized network function (VNF) anomaly detection method may comprise: an NFVI monitoring operation for monitoring a network function virtualization infrastructure (NFVI) in order to train an abnormal-state detection model; a fault injection operation for generating an abnormal state of a virtualized network function (VNF); a pre-processing operation for converting monitoring data collected in a previous operation into a form suitable for training the abnormal-state detection model; and an abnormal-state detection model training performance evaluation operation for training the abnormal-state detection model through an abnormal-state detection algorithm and deriving an optimal abnormal-state detection model through comparison of a result of verifying the trained abnormal state detection model.

[0018] The virtual network management-specific machine learning-based VNF anomaly detection method may further comprise a feedback operation for re-training the abnormal-state

detection model through the abnormal-state detection algorithm on the basis of the optimal abnormal-state detection model derived in the abnormal-state detection model training performance evaluation operation.

[0019] The NFVI monitoring operation may be an operation in which: a monitoring agent periodically collects monitoring measurements, which indicate a resource usage state of each virtual machine operating in a virtual network, a monitoring module receives data on the collected monitoring measurements from the monitoring agent and collects the data on the collected monitoring measurements in a time-series database, and a dashboard receives, in a visualized form desired by a user, data converted into a dataset for learning and stored in the database after the data is pre-processed.

[0020] The fault injection operation may be an operation of generating, through a fault injection technique, an abnormal state in software and hardware that is likely to occur in a virtual network in which a VNF operates using a technique used to control the frequency of occurrence of an abnormal state occurring in an actual operating environment.

[0021] The fault injection operation may be an operation of generating an abnormal state through a fault injection technique that causes an abnormal state in a virtual machine in which a VNF operates or causes overload to the extent that normal service cannot be guaranteed by transmitting a large amount of traffic.

[0022] The fault injection operation may be: an operation of directly injecting a fault such as CPU load, memory shortage, disk I/O access failure, network latency, and network packet loss into a virtual machine where a VNF operates; or an operation of generating a situation that exceeds an allowable range of access to and request for traffic or service, resulting in packet processing latency and packet drop by kernel.

[0023] The pre-processing operation may comprise a feature selection operation for distinguishing and selecting values that are criteria for determining normal and abnormal states among measurements collected through the monitoring, removing items with features that are

similar to or overlapping with each other from the collected measurements, extracting features for distinguishing normal and abnormal states of a VNF, and using data on the extracted features to perform model training.

[0024] The pre-processing operation may comprise a data labeling operation for classifying data at each time into normal and abnormal states to use extracted feature data in a supervised learning-based machine learning algorithm.

[0025] The pre-processing operation may be an operation of: defining an abnormal state on the basis of a request state of service and information for determining an SLA violation that occurs inside a VNF due to system and traffic overload generated by fault injection; and generating a dataset by labeling a case in which an SLA violation and a service request failure occurs as an abnormal state and a case other than the abnormal state as a normal state.

[0026] The abnormal-state detection model training performance evaluation operation may comprise an operation of generating an anomaly detection model through learning using a supervised learning-based eXtreme Gradient Boosting (XGBoost) algorithm through a labeled dataset generated in the pre-processing operation.

[0027] The abnormal-state detection model training performance evaluation operation may comprise an operation of generating an anomaly detection model using XGBoost algorithm-based learning through a dataset labeled based on SLA violation information and an application service provision state in the fault injection operation and the pre-processing operation, verifying classification accuracy of the generated anomaly detection model, and evaluating performance of the model.

[0028] A model training operation may include, as a list of features selected for abnormal state detection training, a measurement time, a VNF instance name, CPU - idle time, CPU - time spent in interrupt processing, CPU - time spent in executing a process with nice value, CPU – time spent in softirq processing, CPU - CPU standby time by hypervisor, CPU - time spent in kernel mode, CPU - time spent in user mode, CPU - I/O standby time, Rx traffic bandwidth for

a network interface, Tx traffic bandwidth for a network interface, the number of Rx packets in a network interface, the number of Tx packets in a network interface, Disk - free space, Disk - reserved space, Disk – space in use, Disk - read I/O, Disk - write I/O, Disk - I/O execution time, Memory - free space, Memory - buffered space, Memory - cached space, Memory – space in use, and network packet latency.

[0029] A model training operation may include, as a hyperparameter value of an XGBoost algorithm used by a VNF anomaly detection model, the number of trees, the maximum depth of a tree, the minimum number of observations in a leaf, a column sampling rate, a column sampling rate per tree, a metric to be used in early stopping, a value used for early stopping, L2 regularization, and L1 regularization.

[0030] In order to overcome these limitations, the present disclosure solves the problems by defining abnormal states corresponding to a service request and an SLA violation, and thus conventional studies show a classification accuracy between 80% and 90%, but an eXtreme Gradient Boosting (XGBoost) algorithm model used in the present disclosure is more suitable for preventing false alarms because it shows a high classification accuracy of 95% or more even in an abnormal-state definition method similar to conventional methods. When an abnormal state is defined in terms of a service, such as an SLA violation and service request failure that is more complicated than the threshold-based abnormal-state defining method, the present disclosure shows classification accuracy higher than or equal to that of the conventional method even if it is taken into account that actual verification is necessary.

[0031] Also, according to the present disclosure, various causes of abnormal states that may occur in real situations are included by generating abnormal states using various fault injection methods related to SLA violations as well as resource usage.

[0032] As a result, according to the present disclosure, it is possible to build a more precise VNF abnormal-state detection system by detecting abnormal states in consideration of service aspects and providing higher classification accuracy than before.

BRIEF DESCRIPTION OF DRAWINGS

[0033] Exemplary embodiments of the present disclosure will become more apparent by describing the exemplary embodiments of the present disclosure in detail with reference to the accompanying drawings, in which:

[0034] FIG. 1 is a configuration diagram illustrating an example of a machine learning-based virtualized network function (VNF) abnormal-state detection system according to the present disclosure;

[0035] FIG. 2 is a flowchart illustrating an approximate algorithm of eXtreme Gradient Boosting (XGBoost) used by an abnormal-state detection model according to the present disclosure; and

[0036] FIGS. 3 and 4 are flowcharts illustrating the learning of a machine learning-based abnormal-state detection method according to the present disclosure.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0037] Exemplary embodiments of the present disclosure are disclosed herein. However, specific structural and functional details disclosed herein are merely representative for purposes of describing embodiments of the present disclosure. Thus, embodiments of the present disclosure may be embodied in many alternate forms and should not be construed as limited to embodiments of the present disclosure set forth herein.

[0038] Accordingly, while the present disclosure is capable of various modifications and alternative forms, specific embodiments thereof are shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that there is no intent to limit the present disclosure to the particular forms disclosed, but on the contrary, the present disclosure is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the present disclosure. Like numbers refer to like elements throughout the description of the figures.

[0039] It will be understood that, although the terms first, second, etc. may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another. For example, a first element could be termed a second element, and, similarly, a second element could be termed a first element, without departing from the scope of the present disclosure. As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items.

[0040] In exemplary embodiments of the present disclosure, "at least one of A and B" may refer to "at least one A or B" or "at least one of one or more combinations of A and B". In addition, "one or more of A and B" may refer to "one or more of A or B" or "one or more of one or more combinations of A and B".

[0041] It will be understood that when an element is referred to as being "connected" or "coupled" to another element, it can be directly connected or coupled to the other element or intervening elements may be present. In contrast, when an element is referred to as being "directly connected" or "directly coupled" to another element, there are no intervening elements present. Other words used to describe the relationship between elements should be interpreted in a like fashion (i.e., "between" versus "directly between," "adjacent" versus "directly adjacent," etc.).

[0042] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the present disclosure. As used herein, the singular forms "a," "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises," "comprising," "includes" and/or "including," when used herein, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0043] Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this present disclosure belongs. It will be further understood that terms, such as those defined in commonly used dictionaries, should be interpreted as having a meaning that is consistent with their meaning in the context of the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein.

[0044] Hereinafter, preferred exemplary embodiments of the present disclosure will be described in more detail with reference to the accompanying drawings. In describing the present disclosure, in order to facilitate an overall understanding, the same reference numerals are used for the same elements in the drawings, and duplicate descriptions for the same elements are omitted.

[0045] FIG. 1 is a configuration diagram illustrating an example of a virtual network management-specific machine learning-based virtualized network function (VNF) anomaly detection system 100 according to the present disclosure.

[0046] Referring to FIG. 1, there is disclosed a virtual network management-specific machine learning-based VNF anomaly detection system 100 that is applied to a virtual network 50 in a Network Functions Virtualization Infrastructure (NFVI) environment configured through virtualization in a physical network 10 proposed by the present disclosure.

[0047] The abnormal-state detection system 100 which is for detecting an abnormal state of the VNF according to the present disclosure and which operates in the virtual network 50 of the NFVI environment configured through virtualization in the physical network 10 includes a data collection unit 110 and a data analysis unit 150.

[0048] The data collection unit 110, which is a part that collects data from the virtual network 50 to train an abnormal-state detection model, collects data which has a state indicating that a service is normally provided and abnormal data which occurs through a fault injection method, such as resource shortage, network anomaly, and SLA violation, through a monitoring module

111 and a collect, which is a monitoring agent. The collected data is stored in a time-series database 113 and transmitted to the data analysis unit 150 in order to determine abnormal states.

[0049] The data collection unit 110 may further include a monitoring agent and a dashboard.

[0050] Monitoring measurements collected by the monitoring agent are stored in the database 113 through the monitoring module 111 and are visualized as a dashboard.

[0051] The monitoring agent periodically collects a resource usage state of each virtual machine operating in a virtual network. The monitoring measurements collected by the monitoring agent include a total of 73 items, including sub-items such as CPU utilization, memory usage, and network traffic load. The monitoring agent sends time-series monitoring data, which includes the collected measures, to the monitoring module 111.

[0052] The monitoring module 111 stores the collected time-series monitoring data in the database 113.

[0053] The database 113 stores the time-series monitoring data collected by the monitoring module 111.

[0054] The dashboard provides the time-series monitoring data stored in the database 113 in a visualized form desired by a user, such as a graph, a table, etc.

[0055] The data analysis unit 150 extracts features required to detect abnormal states as shown in Table 1 through data pre-processing 151 of the monitoring data received from the data collection unit 110 and sends the extracted feature data to an abnormal-state detection model 153.

[0056] Through the data pre-processing 151, the monitoring data stored in the database 113 is converted into dataset for learning.

[0057] By analyzing data that is input in real time, the abnormal-state detection model 153 determines whether there is an abnormal state and notifies a network manager 5 when an abnormal state occurs.

[0058] Table 1 is a list of features selected for abnormal-state detection learning.

[Table 1]

Feature	Description
Time	Measurement time
instance	VNF instance name
cpu_idle	CPU – idle time
cpu_interrupt	CPU – time spent in interrupt processing
cpu_nice	CPU - time spent in executing process with nice value
cpu_softirq	CPU - time spent in softirq processing
cpu_steal	CPU - CPU standby time by hypervisor
cpu_system	CPU - time spent in kernel mode
cpu_user	CPU - time spent in user mode
cpu_wait	CPU - I/O standby time
network_rx_bytes	Rx traffic bandwidth for network interface
network_tx_bytes	Tx traffic bandwidth for network interface
network_rx_packets	number of Rx packets in network interface
network_tx_packets	number of Tx packets in network interface
disk_free	Disk - free space
disk_reserved	Disk - reserved space
disk_used	Disk – space in use
disk_read	Disk - read I/O
disk_write	Disk - write I/O
disk_Io_time	Disk - I/O execution time
mem_free	Memory - free space
mem_buffered	Memory - buffered space
mem_cashed	Memory - cached space
mem_used	Memory - space in use
hop-by-hop latency	Network packet latency

[0059] The labeling of the dataset used to train the VNF anomaly detection model 153 through the method proposed by the present disclosure as normal data and abnormal data is achieved as follows. First, the dataset is generated by converting the collected monitoring data into a

form suitable for model training as described above. To this end, a metric most relevant to a criterion for identifying abnormal states is selected from among metrics collected during the monitoring process. This process is performed in consideration of correlations between the metrics. Subsequently, in the case of labeling of normal and abnormal states of data, many fault alarms are caused when a metric such as CPU utilization is determined as a criterion for the labeling. Therefore, in the present disclosure, a case in which the performance degradation (performance bottleneck) of VNF occurs or an SLA violation occurs is defined as an abnormal state.

[0060] The performance degradation of VNF causes a shortage of available system resources due to the overload of the VNF or the injection of faults, which causes packet loss in the VNF. Accordingly, in the present disclosure, a packet loss rate being greater than or equal to 1% is defined as an abnormal state, and VNF having an anomaly (root cause localization) is detected. In the case of SLA violation, a criteria is different for each service, but an average response time and a service request failure rate are generally included. Thus, an abnormal state is defined as such an index, and also, an SLA violation criterion for each service is defined as an abnormal state. For example, for a web hosting service, a case in which an average response time is 0.5 seconds, one second, two seconds or more and a service request failure rate is 0.1%, 1%, 2% or more is defined as an SLA violation (based on GFD-R. 192-Web Service Agreement Specification).

[0061] Also, the eXtreme Gradient Boosting (XGBoost) algorithm used in the present disclosure is based on an ensemble learning technique that obtains a model with better performance than when training is performed through a single model by training and combining multiple models. XGBoost is an algorithm that corresponds to a boosting technique among ensemble learning techniques. The boosting technique increases classification accuracy in the next model training by increasing the weight of data with a classification error in the previously

trained model. Unlike GBM, which is generally widely used among boosting-technique-based algorithms, XGBoost has an advantage.

[0062] FIG. 2 is a flowchart illustrating an approximate algorithm of XGBoost used by an abnormal-state detection model according to the present disclosure.

[0063] Referring to FIG. 2, the algorithm of XGBoost used by an anomaly detection model according to the present disclosure will be described using Equations 1 to 4 below.

[0064] First, XGBoost prevents overfitting through an objective function to which regularization is applied as in Equation 1 to solve an overfitting issue of GBM.

[0065] [Equation 1]

$$L(\phi) = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{i=1}^{n} \Omega(f_i)$$

l : Loss Function ($\hat{y}_i$: Predicted Value, y_i : Actual Result Value)

[0066] In Equation 1, the first term l is a loss function (differentiable convex loss function), which represents the difference between the predicted value $\hat{y}_i$ of an i^{th} instance and the actual result value y_i. The second term Ω, which is a regularization technique that indicates the complexity of each tree, solves the fitting issue by controlling the complexity of the model in the process of minimizing the objective function by adding the number T of leaves of a tree and the norm $\|w\|^2$ of a weight vector of the leaves to the loss function for each tree as shown in Equation 2.

[0067] [Equation 2]

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda\|w\|^2$$

γT : Number of leaves of tree

$\|w\|^2$: Norm of weight vector of leaves

[0068] In addition to the above-described objective function, XGBoost uses shrinkage scaling and column sub-sampling to solve the overfitting issue. The shrinkage scaling reduces the influence of existing trees or leaves on new trees in the stochastic optimization process by applying scaling to weights newly added at each stage of a boosting-based tree. The column sub-sampling increases a training speed by preventing overfitting compared to a conventional row-based sub-sampling.

[0069] Also, since the existing GBM uses a greedy algorithm in the process of searching for optimization points for all split points for each feature, high classification accuracy is provided, but there is a limitation in that the training time is long. In contrast, XGBoost uses an approximate algorithm as shown in FIG. 2 to search for an optimized split point. The approximate algorithm sets a candidate split point for each feature (S30) and sums gradient vectors of the loss function for split sections according to the quantiles of the feature distribution (S40). Based on the sum, the approximate algorithm computes a score for the splitting optimization and determines whether to finally confirm split point settings (S50).

[0070] In order to properly set a candidate split point for each feature, the approximate algorithm of XGBoost applies a weighted quantile sketch method (S10) and a sparsity-aware split finding method (S20) to search for a candidate split point. The quantile sketch method finds split points $\{s_{k,1}, s_{k,2}, \ldots, s_{k,l}\}$ that are obtained by uniformly dividing data through an approximation factor ε for dividing data for feature k by 1/ε as shown in Equation 3.

[0071] [Equation 3]

$$\left|r_k(s_{k,j}) - r_k(s_{k,j+1})\right| < \epsilon$$

E: Approximation factor

$s_{k,j}$: j^{th} split point for feature k

[0072] In order to uniformly split data, a function r_k representing the proportion of data smaller than each split point is defined as in Equation 4 and used for data splitting. In this case, D_k denotes a dataset in which a weight is applied to the feature k, and h denotes a data weight. XGBoost finds a split point while maintaining accuracy for weighted data through the quantile sketch method.

[0073] [Equation 4]

$$r_k(z) = \frac{1}{\sum_{(x,h)\in D_k} h} \sum_{(x,h)\in D_k, x<z} h$$

D_k: Dataset for feature k

h: Weight of data

[0074] The sparsity-aware split finding method (S20) finds a split point in consideration of missing data and sparsity data when a missing value is generated due to omission of values in the data collection process or data is sparse. For example, by setting a default classification direction for each tree node, missing values are classified in the default classification direction when values are missing in the data.

[0075] Table 2 includes hyper-parameter values of the XGBoost algorithm used by a proposed VNF anomaly detection model.

[Table 2]

Hyper-parameter	Value	Description
ntrees	111	Number of trees
max_depth	5	Maximum depth of tree
min_rows	3	Minimum number of observations in leaf
col_sample_rate	0.8	Column sampling rate
col_sample_rate_per_tree	0.8	Column sampling rate per tree
stopping_metric	Logloss	Metric to be used in early stopping

stopping_tolerance	0.0045469579205	Value used for early stopping
reg_lambda	0.001	L2 regularization
reg_alpha	1	L1 regularization

[0076] In order to train the anomaly detection model based on the XGBoost algorithm and the dataset generated through the fault injection method in the NFV environment, the present disclosure optimizes the performance of the anomaly detection model using the hyper-parameters as shown in Table 2.

[0077] Data is labeled in order to verify the performance of the abnormal-state detection model generated based on this (S400). The labeled data is split into a training dataset of 75% and a test dataset of 25%, and then the abnormal-state detection model is trained. The performance of the abnormal-state detection model trained through the training dataset is evaluated through the 5-fold cross validation method. Accuracy, precision, reproduction rate (recall), F-measure (F1 score), and the like are used as items for evaluation of the abnormal-state detection model. Subsequently, the performance of the abnormal-state detection model is finally evaluated through test dataset that is not involved in training the abnormal-state detection model.

[0078] FIGS. 3 and 4 are flowcharts illustrating the training of a machine learning-based abnormal-state detection method according to the present disclosure.

[0079] Referring to FIGS. 3 and 4, the virtual network management-specific machine learning-based VNF anomaly detection method according to the present disclosure includes an NFVI monitoring operation (S100) for monitoring a network function virtualization infrastructure (NFVI) in order to train an abnormal-state detection model, a fault injection operation (S200) for generating an abnormal state of a VNF, a preprocessing operation (S300) for converting monitoring data collected in the previous operation into a form suitable for training the abnormal-state detection model, and an abnormal-state detection model training performance evaluation operation (S400) for training the abnormal-state detection model through an

abnormal-state detection algorithm and deriving an optimal abnormal-state detection model through comparison of a result of verifying the trained abnormal-state detection model.

[0080] Here, the preprocessing operation (S300) includes a feature selection operation (S310) and a data labeling operation (S350), and the abnormal-state detection model training performance evaluation operation (S400) includes a model training operation (S410) and a model performance evaluation operation (S450).

[0081] Here, the abnormal-state detection model training performance evaluation operation (S400) further includes a feedback operation (S470) for re-training the abnormal-state detection model (S410) through an abnormal-state detection algorithm on the basis of the optimal abnormal-state detection model derived in the model performance evaluation operation (S450).

[0082] In describing the virtual network management-specific machine learning-based VNF anomaly detection method using the above-described virtual network management-specific machine learning-based VNF anomaly detection system according to the present disclosure, an anomaly detection model generation method according to the present disclosure is largely composed of four operations. In a first operation, which is the NFVI monitoring operation (S100), an NFVI environment is monitored to train an abnormal-state detection model. In a second operation, which is the fault injection operation (S200), an abnormal state of a VNF is generated. In a third operation, which is the preprocessing operation (S300), the feature selection operation (S310) and the data labeling operation (S350) are performed to convert monitoring data collected in the previous operation into a form suitable for training a machine learning model. Last, in the anomaly detection model training performance evaluation operation (S400), the abnormal-state detection model is trained through XGBoost algorithm (S410), and the model performance evaluation operation (S450) for deriving an optimal model through comparison of a result of verifying each model is performed.

[0083] In the NFVI monitoring operation (S100), monitoring measurements collected by a monitoring agent are stored in the database 113 through the monitoring module 111 and are

visualized as a dashboard. The monitoring agent periodically collects a resource usage state of each virtual machine operating in a virtual network. The monitoring measurements collected by the monitoring agent include a total of 73 items, including sub-items such as CPU utilization, memory usage, and network traffic load. The monitoring agent sends the data to the monitoring module 111, and the monitoring module 111 stores the collected data in the time-series database 113. The stored data is pre-processed and then is converted into a dataset for learning. Through the dashboard, the data stored in the database 113 is provided in a visualized form desired by a user, such as a graph, a table, etc.

[0084] The fault injection operation (S200) is a technique used to control the frequency of occurrence of an abnormal state that occurs very rarely in an actual operating environment. Various abnormal states in software and hardware that can occur in the virtual network in which the VNF operates are generated through fault injection technology. There are two main methods to generate an abnormal state through the fault injection technology. The first method is to generate an abnormal state in the VM where the VNF operates, and the second method is to cause an overload to the extent that proper service cannot be guaranteed by transmitting a large amount of traffic. The first method injects faults directly into the VM where the VNF operates. This causes CPU load and memory shortage, disk I/O access failure, network latency, network packet loss, and the like. The second method causes network overload through a large amount of traffic, which makes the VNF consume a great deal of system resources and time to process incoming packets. For example, the second method causes a situation in which access to and requests for traffic or services are excessively input, resulting in packet processing latency and packet drop by kernel.

[0085] The preprocessing operation (S300) includes the feature selection operation (S310) and the data labeling operation (S350). First, the feature selection operation (S310) is an operation of identifying and selecting values that are criteria for determining normal and abnormal states of measurements collected through monitoring. In operation S310, items with features that are

similar to or overlapping with each other are removed from the collected measurements. Through this process, features for determining the normal and abnormal states of the VNF are extracted, and the data is used for learning. The data labeling operation (S350) is an operation of classifying data for each time into a normal state and an abnormal state in order to allow the extracted feature data to be used in a supervised learning-based machine learning algorithm. The abnormal state is defined based on a request state of service and information that may determine an SLA violation occurring in the VNF due to system and traffic overload caused by fault injection. That is, cases in which an SLA violation and a service request failure occur are labeled as an abnormal state, and the other cases are labeled as a normal state to create a dataset.

[0086] Last, in the anomaly detection model training performance evaluation operation (S400), an anomaly detection model is trained using a supervised learning-based XGBoost algorithm through the labeled dataset generated in the preprocessing operation (S300) (S410). XGBoost is a decision tree-based machine learning algorithm which exhibits better performance in classifying and predicting typical data, unlike a neural network-based algorithm that exhibits good performance in predicting atypical data such as images or text. In particular, XGBoost utilizes a method of iteratively training an independent tree like Gradient Boosting Machine (GBM), which is a commonly used boosting technique-based algorithm, but solves the overfitting issue of the GBM and exhibits better performance than the GBM in terms of resource usage and training speed. In the anomaly detection model training performance evaluation operation (S400), an anomaly detection system 100 of a VNF operating in a series of processes, which include generating an anomaly detection model using XGBoost algorithm-based training through a labeled dataset on the basis of application service provision statuses and SLA violation information in the fault injection operation (S200) and the pre-processing operation (S300) (S410), verifying the classification accuracy of the generated anomaly detection model and evaluating the performance of the anomaly detection model (S450), and

feeding an optimal anomaly detection model generated as a result of the anomaly detection model performance evaluation operation (S450) back to the abnormal-state detection model training operation (S410) (S470), is built and utilized to manage an NFV environment.

[0087] With the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure, it is possible to learn abnormal states through data correlations. However, a conventional machine learning-based abnormal-state detection method defines abnormal states on the basis of thresholds of measurements such as CPU and memory in defining the abnormal states and thus has a limitation in that many false alarms are induced and the state of an actually provided service is not considered.

[0088] Therefore, the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure solve the issues by defining an abnormal state corresponding to a service request and an SLA violation in order to overcome the limitation. Conventional studies exhibit a classification accuracy of 80 to 90%, but the XGBoost algorithm model used in the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure has a high classification accuracy of more than 95% even in an anomaly state definition method similar to that of the conventional method and thus is more suitable for preventing false alarms. When an abnormal state is defined in terms of a service, such as a more complicated SLA violation and service request failure than the threshold-based abnormal-state defining method, the present disclosure is expected to exhibit classification accuracy higher than or equal to that of the conventional method even if it is taken into account that actual verification is necessary.

[0089] Also, in the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure, various causes of abnormal states that may occur in real situations are included by generating abnormal states using various fault injection methods related to SLA violations as well as resource usage. As

a result, with the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure, it is possible to build a more precise VNF abnormal-state detection system by considering a service aspect that detects an abnormal state and provides higher classification accuracy than before.

[0090] In the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure, a method of generating a machine learning-based VNF abnormal-state detection model is defined in order to solve NFV environment management issues that arise along with the advancement and complexity of the current NFV environment, and a method of detecting an abnormal state of an actually operating VNF by applying the generated model to the NFV environment is proposed.

[0091] An anomaly detection model training method used in the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure may generate an optimal model with the best accuracy through new machine-learning algorithms that are not used in the conventional methods, such as XGBoost.

[0092] In addition, with the virtual network management-specific machine learning-based VNF anomaly detection system and method according to the present disclosure, which are obtained by improving a method in which a conventional system detects an abnormal state on the basis of simple measurements such as CPU and memory, it is possible to realize a more precise anomaly detection system by defining an abnormal state in consideration of the state of a service including an SLA violation.

[0093] The operations of the method according to an embodiment of the present disclosure can also be embodied as computer-readable programs or codes on a computer-readable recording medium. The computer-readable recording medium includes any type of recording apparatus in which data readable by a computer system is stored. The computer-readable recording medium can also be distributed over network-coupled computer systems so that computer-readable programs or codes are stored and executed in a distributed fashion.

[0094] Also, examples of the computer-readable recording medium may include a hardware device such as ROM, RAM, and flash memory, which are specifically configured to store and execute program commands. The program commands may include high-level language codes executable by a computer using an interpreter as well as machine codes made by a compiler.

[0095] Although some aspects of the disclosure have been described in the context of an apparatus, it is clear that these aspects also represent a description of the corresponding method, where a block or apparatus corresponds to a method step or a feature of a method step. Analogously, aspects described in the context of a method step may also represent a description of a corresponding block or item or feature of a corresponding apparatus. Some or all of the method steps may be performed by means of (or by using) a hardware device such as, for example, a microprocessor, a programmable computer, or an electronic circuit. In some embodiments, one or more of the most important method steps may be performed by such a device.

[0096] In some embodiments, a programmable logic device (for example, a field-programmable gate array) may be used to perform some or all of the functionalities of the methods described herein. In some embodiments, a field-programmable gate array may cooperate with a microprocessor in order to perform one of the methods described herein. Generally, the methods are performed by any hardware device.

[0097] While the exemplary embodiments of the present disclosure and their advantages have been described in detail, it should be understood that various changes, substitutions and alterations may be made herein without departing from the scope of the present disclosure.

WHAT IS CLAIMED IS:

1. A virtual network management-specific machine learning-based virtualized network function (VNF) anomaly detection system, which is related to an abnormal-state detection apparatus for detecting an abnormal state of a VNF operating in a virtual network of a network function virtualization (NFV) infrastructure formed in a physical network through virtualization, the virtual network management-specific machine learning-based VNF anomaly detection system comprising:

a data collection unit configured to collect normal state data generated when a service is normally provided and abnormal state data generated through a fault injection method through a monitoring agent and a monitoring module in real time, store the collected data in a time-series database, and transmit the monitoring data to determine whether there is an abnormal state; and

a data analysis unit configured to extract a feature necessary for detecting an abnormal state by pre-processing monitoring data received from the data collection unit and send data on the extracted data to an abnormal-state detection model so that the abnormal-state detection model analyzes data that is input in real time to determine whether there is an abnormal state and notifies a network manager when an abnormal state occurs.

2. The virtual network management-specific machine learning-based VNF anomaly detection system of claim 1, wherein the data collection unit comprises a monitoring agent configured to periodically collect a resource usage state of each virtual machine operating in the virtual network and send collected monitoring data to the monitoring module; and a dashboard configured to provide the monitoring data stored in the database in time-series in a visualized form.

3. A virtual network management-specific machine learning-based virtualized network function (VNF) anomaly detection method comprising:

an NFVI monitoring operation for monitoring a network function virtualization infrastructure (NFVI) in order to train an abnormal-state detection model;

a fault injection operation for generating an abnormal state of a virtualized network function (VNF);

a pre-processing operation for converting monitoring data collected in a previous operation into a form suitable for training the abnormal-state detection model; and

an abnormal-state detection model training performance evaluation operation for training the abnormal-state detection model through an abnormal-state detection algorithm and deriving an optimal abnormal-state detection model through comparison of a result of verifying the trained abnormal state detection model.

4. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, further comprising a feedback operation for re-training the abnormal-state detection model through the abnormal-state detection algorithm on the basis of the optimal abnormal-state detection model derived in the abnormal-state detection model training performance evaluation operation.

5. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the NFVI monitoring operation is an operation in which:

a monitoring agent periodically collects monitoring measurements, which indicate a resource usage state of each virtual machine operating in a virtual network,

a monitoring module receives data on the collected monitoring measurements from the monitoring agent and collects the data on the collected monitoring measurements in a time-series database, and

a dashboard receives, in a visualized form desired by a user, data converted into a dataset for learning and stored in the database after the data is pre-processed.

6. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the fault injection operation is an operation of generating, through a fault injection technique, an abnormal state in software and hardware that is likely to occur in a virtual network in which a VNF operates using a technique used to control the frequency of occurrence of an abnormal state occurring in an actual operating environment.

7. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the fault injection operation is an operation of generating an abnormal state through a fault injection technique that causes an abnormal state in a virtual machine in which a VNF operates or causes overload to the extent that normal service cannot be guaranteed by transmitting a large amount of traffic.

8. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the fault injection operation is:

an operation of directly injecting a fault such as CPU load, memory shortage, disk I/O access failure, network latency, and network packet loss into a virtual machine where a VNF operates; or

an operation of generating a situation that exceeds an allowable range of access to and request for traffic or service, resulting in packet processing latency and packet drop by kernel.

9. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the pre-processing operation comprises a feature selection operation for distinguishing and selecting values that are criteria for determining

normal and abnormal states among measurements collected through the monitoring, removing items with features that are similar to or overlapping with each other from the collected measurements, extracting features for distinguishing normal and abnormal states of a VNF, and using data on the extracted features to perform model training.

10. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the pre-processing operation comprises a data labeling operation for classifying data at each time into normal and abnormal states to use extracted feature data in a supervised learning-based machine learning algorithm.

11. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the pre-processing operation is an operation of:

defining an abnormal state on the basis of a request state of service and information for determining an SLA violation that occurs inside a VNF due to system and traffic overload generated by fault injection; and

generating a dataset by labeling a case in which an SLA violation and a service request failure occurs as an abnormal state and a case other than the abnormal state as a normal state.

12. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the abnormal-state detection model training performance evaluation operation comprises an operation of generating an anomaly detection model through learning using a supervised learning-based eXtreme Gradient Boosting (XGBoost) algorithm through a labeled dataset generated in the pre-processing operation.

13. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein the abnormal-state detection model training performance

evaluation operation comprises an operation of generating an anomaly detection model using XGBoost algorithm-based learning through a dataset labeled based on SLA violation information and an application service provision state in the fault injection operation and the pre-processing operation, verifying classification accuracy of the generated anomaly detection model, and evaluating performance of the model.

14. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein a model training operation comprises, as a list of features selected for abnormal state detection training, a measurement time, a VNF instance name, CPU - idle time, CPU - time spent in interrupt processing, CPU - time spent in executing a process with nice value, CPU – time spent in softirq processing, CPU - CPU standby time by hypervisor, CPU - time spent in kernel mode, CPU - time spent in user mode, CPU - I/O standby time, Rx traffic bandwidth for a network interface, Tx traffic bandwidth for a network interface, the number of Rx packets in a network interface, the number of Tx packets in a network interface, Disk - free space, Disk - reserved space, Disk – space in use, Disk - read I/O, Disk - write I/O, Disk - I/O execution time, Memory - free space, Memory - buffered space, Memory - cached space, Memory – space in use, and network packet latency.

15. The virtual network management-specific machine learning-based VNF anomaly detection method of claim 3, wherein a model training operation comprises, as a hyperparameter value of an XGBoost algorithm used by a VNF anomaly detection model, the number of trees, the maximum depth of a tree, the minimum number of observations in a leaf, a column sampling rate, a column sampling rate per tree, a metric to be used in early stopping, a value used for early stopping, L2 regularization, and L1 regularization.

ABSTRACT

A virtual network management-specific machine learning-based VNF anomaly detection system may comprise: a data collection unit configured to collect normal state data generated when a service is normally provided and abnormal state data generated through a fault injection method through a monitoring agent and a monitoring module in real time, store the collected data in a time-series database, and transmit the monitoring data to determine whether there is an abnormal state; and a data analysis unit configured to extract a feature necessary for detecting an abnormal state by pre-processing monitoring data received from the data collection unit and send data on the extracted data to an abnormal-state detection model so that the abnormal-state detection model analyzes data that is input in real time to determine whether there is an abnormal state and notifies a network manager when an abnormal state occurs.

DRAWINGS

FIG. 1

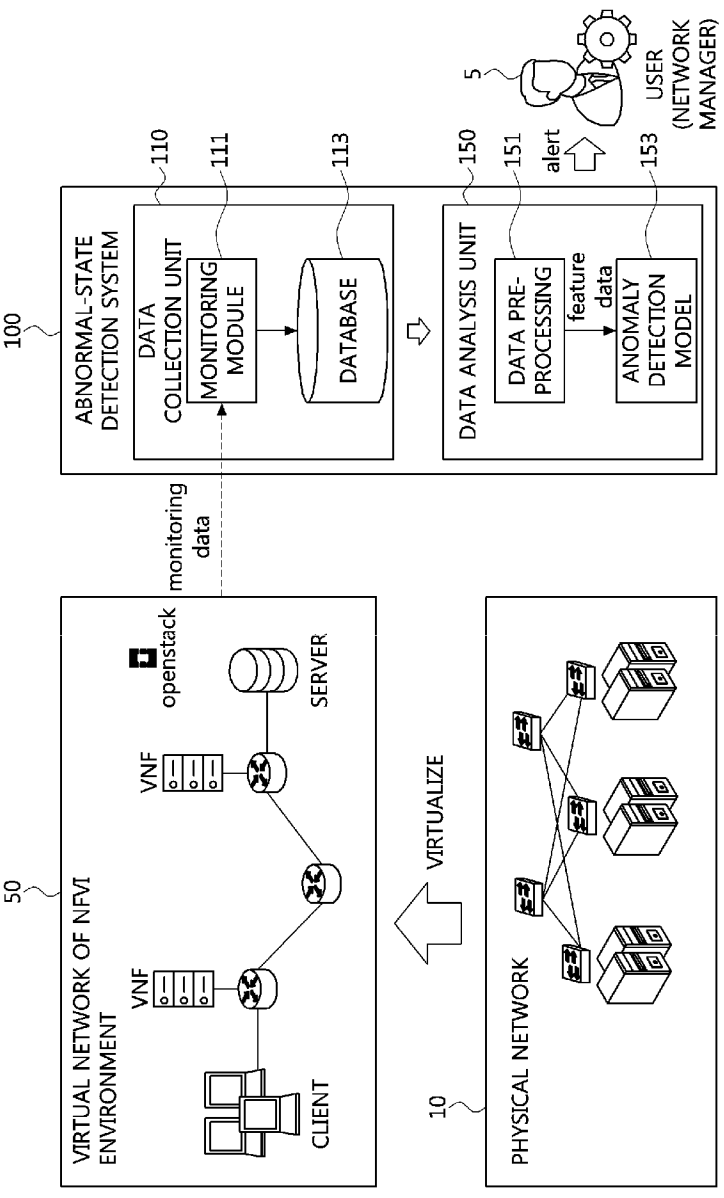


FIG. 2

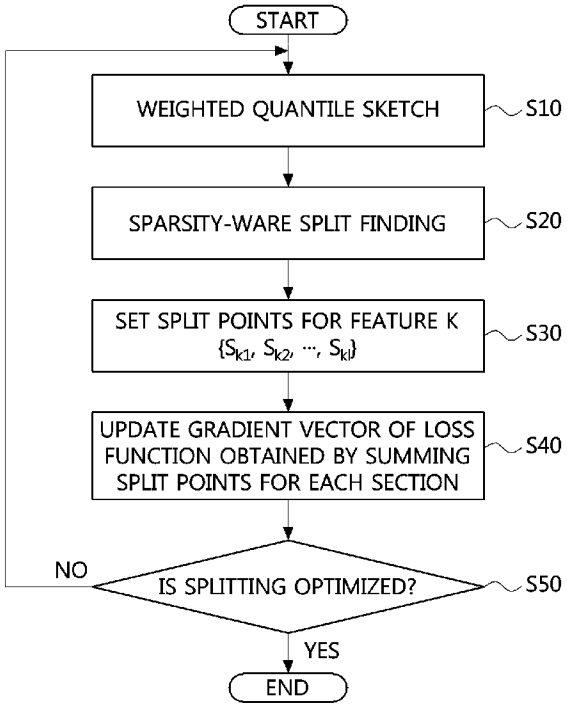

START
WEIGHTED QUANTILE SKETCH
S10
SPARSITY-WARE SPLIT FINDING
S20
SET SPLIT POINTS FOR FEATURE K
{Sk1, Sk2, ···, Skl}
S30
UPDATE GRADIENT VECTOR OF LOSS FUNCTION OBTAINED BY SUMMING SPLIT POINTS FOR EACH SECTION
S40
NO
IS SPLITTING OPTIMIZED?
S50
YES
END

FIG. 3

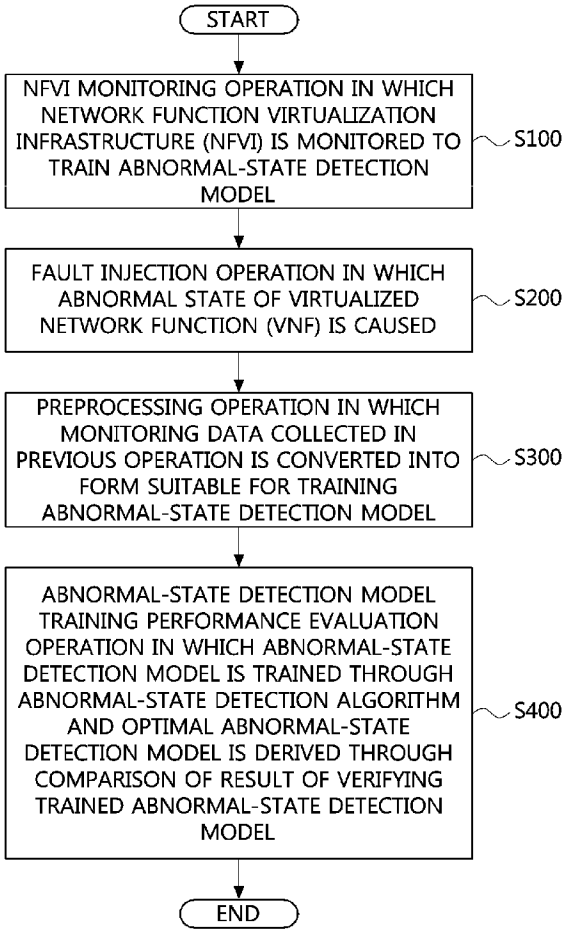
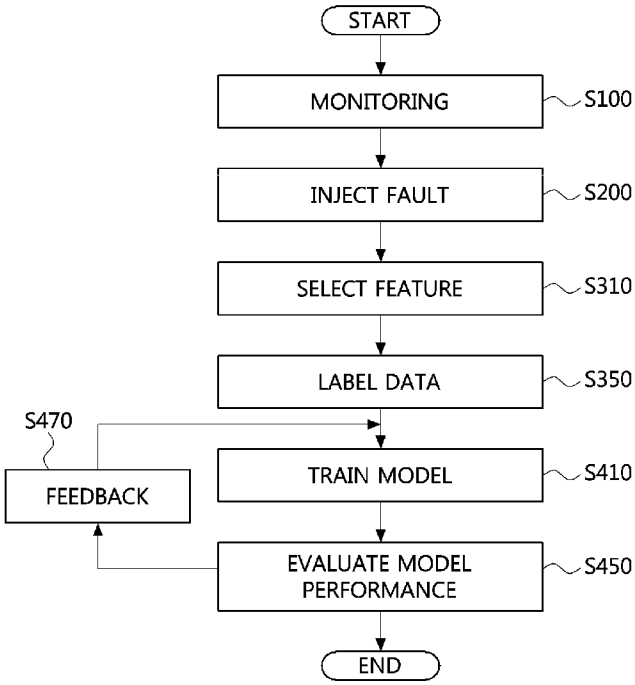

START
NFVI MONITORING OPERATION IN WHICH NETWORK FUNCTION VIRTUALIZATION INFRASTRUCTURE (NFVI) IS MONITORED TO TRAIN ABNORMAL-STATE DETECTION MODEL
S100
FAULT INJECTION OPERATION IN WHICH ABNORMAL STATE OF VIRTUALIZED NETWORK FUNCTION (VNF) IS CAUSED
S200
PREPROCESSING OPERATION IN WHICH MONITORING DATA COLLECTED IN PREVIOUS OPERATION IS CONVERTED INTO FORM SUITABLE FOR TRAINING ABNORMAL-STATE DETECTION MODEL
S300
ABNORMAL-STATE DETECTION MODEL TRAINING PERFORMANCE EVALUATION OPERATION IN WHICH ABNORMAL-STATE DETECTION MODEL IS TRAINED THROUGH ABNORMAL-STATE DETECTION ALGORITHM AND OPTIMAL ABNORMAL-STATE DETECTION MODEL IS DERIVED THROUGH COMPARISON OF RESULT OF VERIFYING TRAINED ABNORMAL-STATE DETECTION MODEL
S400
END

FIG. 4


START
MONITORING
S100
INJECT FAULT
S200
SELECT FEATURE
S310
LABEL DATA
S350
S470
FEEDBACK
TRAIN MODEL
S410
EVALUATE MODEL PERFORMANCE
S450
END