

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202341011275 A

(19) INDIA

(22) Date of filing of Application :18/02/2023

(43) Publication Date : 17/03/2023

(54) Title of the invention : A MACHINE LEARNING BASED SYSTEM FOR CYBERATTACK DETECTION AND PREVENTION IN CLOUD-BASED, WIRELESS VIRTUAL ENVIRONMENTS

(51) International classification :C07K 161000, G06F 216000, G06N 030400, G06N 200000, H04L 671000
(86) International Application No :PCT//
Filing Date :01/01/1900
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)Name of Applicant :

1)Dr. P. Chitra

Address of Applicant :Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai -600026 -----

2)Dr. Shankar R.

3)Dr.Gandi Satyanarayana

4)Dr. Gogineni Krishna Chaitanya

5)Dr. K. Valarmathi

6)Mr. R. Sathishkannan

Name of Applicant : NA

Address of Applicant : NA

(72)Name of Inventor :

1)Dr. P. Chitra

Address of Applicant :Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai -600026 -----

2)Dr. Shankar R.

Address of Applicant :Professor, Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College (Autonomous), Meerpet, Hyderabad, Pincode: 500097 -----

3)Dr.Gandi Satyanarayana

Address of Applicant :Professor & Head, Department of Computer Science & Engineering, Avanthi Institute of Engineering and Technology, Cherukupally (Village) Near Thagarapuvalasa Bridge, Vizianagaram (Dist.), Pin-531162 -----

4)Dr. Gogineni Krishna Chaitanya

Address of Applicant :Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India -----

5)Dr. K. Valarmathi

Address of Applicant :Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Bangalore Trunk Road, Varadharajapuram, Poonamallee, Chennai - 600123 -----

6)Mr. R. Sathishkannan

Address of Applicant :Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathy - Bhavani State Highway, Alathukombai, Post, Sathyamangalam, Tamil Nadu 638401 -----

(57) Abstract :

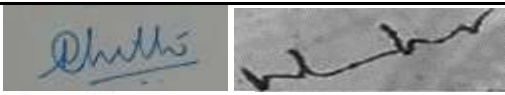
[025] The present invention discloses a machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments. In the present invention, one or more man-in-the-middle (MITM) detection tests initiated by a first node of a networked computing environment to determine whether communications between two other nodes of the same network have been intercepted or attempted to be intercepted by a third node; and it is determined by the first node that at least one of the tests indicates that the communications are likely to have been intercepted. Further, the first node is supplied with data defining the determinations; wherein at least one of the multiple types of MITM detection tests utilises at least one machine learning model trained by training data consisting of multiple samples that individually characterise network data traffic interception to a computer system received. Accompanied Drawing [FIGS. 1-2]

No. of Pages : 19 No. of Claims : 8

FORM 1 THE PATENTS ACT 1970 (39 of 1970) and THE PATENTS RULES, 2003 APPLICATION FOR GRANT OF PATENT (See section 7, 54 and 135 and sub-rule (1) of rule 20)				(FOR OFFICE USE ONLY)	
				Application No.	
				Filing date:	
				Amount of Fee paid:	
				CBR No:	
				Signature:	
1. APPLICANT'S REFERENCE / IDENTIFICATION NO. (AS ALLOTTED BY OFFICE)					
2. TYPE OF APPLICATION [Please tick (✓) at the appropriate category]					
Ordinary (✓)		Convention ()		PCT-NP ()	
Divisional ()	Patent of Addition ()	Divisional ()	Patent of Addition ()	Divisional ()	Patent of Addition ()
3A. APPLICANT(S)					
Name In Full		Nationality	Country of Residence	Address of the Applicant	
1. Dr. P. Chitra		Indian	India	Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai - 600026	
2. Dr. Shankar R.		Indian	India	Professor, Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College (Autonomous), Meerpet, Hyderabad, Pincode: 500097	
3. Dr.Gandi Satyanarayana		Indian	India	Professor & Head, Department of Computer Science & Engineering, Avanthi Institute of Engineering and Technology, Cherukupally (Village) Near Thagarapuvalasa Bridge, Vizianagaram (Dist.), Pin-531162	

4. Dr. Gogineni Krishna Chaitanya	Indian	India	Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India	
5. Dr. K. Valarmathi	Indian	India	Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Bangalore Trunk Road, Varadharajapuram, Poonamallee, Chennai - 600123	
6. Mr. R. Sathishkannan	Indian	India	Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathy - Bhavani State Highway, Alathukombai, Post, Sathyamangalam, Tamil Nadu 638401	
Natural Person (✓)	Other than Natural Person			
	Small Entity ()	Startup ()	Others ()	
4. INVENTOR(S) [Please tick (✓) at the appropriate category]				
Are all the inventor(s) same as the applicant(s) named above?	Yes (✓)		No ()	
If “No”, furnish the details of the inventor(s)				
Name in Full	Nationality	Country of Residence	Address of the Inventor	
Same as Applicant				
5. TITLE OF THE INVENTION				
“A MACHINE LEARNING BASED SYSTEM FOR CYBERATTACK DETECTION AND PREVENTION IN CLOUD-BASED, WIRELESS VIRTUAL ENVIRONMENTS”				
6. AUTHORISED REGISTERED PATENT AGENT(S)		IN/PA No.		
		Name		
		Mobile No.		
7. ADDRESS FOR SERVICE OF APPLICANT IN INDIA		Name	Dr. P. Chitra	
		Postal Address	Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai -	

				600026	
				Telephone No.	
				Mobile No. 9840167844	
				Fax No.	
				E-mail ID pchitra1111@gmail.com	
8. IN CASE OF APPLICATION CLAIMING PRIORITY OF APPLICATION FILED IN CONVENTION COUNTRY, PARTICULARS OF CONVENTION APPLICATION					
Country	Application Number	Filing date	Name of the applicant	Title of the invention	IPC (as classified in the convention country)
9. IN CASE OF PCT NATIONAL PHASE APPLICATION, PARTICULARS OF INTERNATIONAL APPLICATION FILED UNDER PATENT CO-OPERATION TREATY (PCT)					
International application number			International filing date		
10. IN CASE OF DIVISIONAL APPLICATION FILED UNDER SECTION 16, PARTICULARS OF ORIGINAL (FIRST) APPLICATION					
Original (first) application No.			Date of filing of original (first) application		
11. IN CASE OF PATENT OF ADDITION FILED UNDER SECTION 54, PARTICULARS OF MAIN APPLICATION OR PATENT					
Main application/patent No.			Date of filing of main application		
12. DECLARATIONS					
(i) Declaration by the inventor(s) (In case the applicant is an assignee: the inventor(s) may sign herein below or the applicant may upload the assignment or enclose the assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period). I/We, the above named inventor(s) is/are the true & first inventor(s) for this Invention and declare that the applicant(s) herein is/are my/our assignee or legal representative. (a) Date 18/02/2023					
(b) Name			(c) Signature		

1. Dr. P. Chitra 2. Dr. Shankar R. 3. Dr. Gandhi Satyanarayana 4. Dr. Gogineni Krishna Chaitanya 5. Dr. K. Valarmathi 6. Mr. R. Sathishkannan	 G. Satyanarayana K. Valarmathi 
(ii) Declaration by the applicant(s) in the convention country (In case the applicant in India is different than the applicant in the convention country: the applicant in the convention country may sign herein below or applicant in India may upload the assignment from the applicant in the convention country or enclose the said assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period) I/We, the applicant(s) in the convention country declare that the applicant(s) herein is/are my/our assignee or legal representative. (a) Date (b) Signature(s) (c) Name(s) of the signatory	
(iii) Declaration by the applicant(s) I/We the applicant(s) hereby declare(s) that: - € I am/ We are in possession of the above-mentioned invention. € The provisional/complete specification relating to the invention is filed with this application. € The invention as disclosed in the specification uses the biological material from India and the necessary permission from the competent authority shall be submitted by me/us before the grant of patent to me/us. € There is no lawful ground of objection(s) to the grant of the Patent to me/us. € I am/we are the true & first inventor(s). € I am/we are the assignee or legal representative of true & first inventor(s). € The application or each of the applications, particulars of which are given in Paragraph-8, was the first application in convention country/countries in respect of my/our invention(s). € I/We claim the priority from the above mentioned application(s) filed in convention country/countries and state that no application for protection in respect of the invention had been made in a convention country before that date by me/us or by any person from which I/We derive the title. € My/our application in India is based on international application under Patent Cooperation Treaty (PCT) as mentioned in Paragraph-9.	

€ ~~The application is divided out of my /our application particulars of which is given in Paragraph-10 and pray that this application may be treated as deemed to have been filed on DD/MM/YYYY under section 16 of the Act.~~

€ ~~The said invention is an improvement in or modification of the invention particulars of which are given in Paragraph-11.~~

13. FOLLOWING ARE THE ATTACHMENTS WITH THE APPLICATION

(a) Form 2

Item	Details	Fee	Remarks
Complete/ Provisional specification) #	No. of pages: 13		
No. of Claim(s)	No. of claims: 08 No. of pages: 03		
Abstract	No. of pages: 01		
No. of Drawing(s)	No. of drawings: 02 No. of pages: 02		

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

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

(c) Sequence listing in electronic form

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

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

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

(g) Statement and Undertaking on Form 3

(h) Declaration of Inventorship on Form 5

(i) Power of Authority

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

I/We hereby declare that to the best of my/our knowledge, information and belief

the fact and matters slated herein are correct and I/We request that a patent may be granted to me/us for the said invention.

Dated this 18th day of February 2023

Signature:



Name: Dr. P. Chitra et. al.

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

Note: -

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

FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

The Patent Rules, 2003

COMPLETE SPECIFICATION

(See section 10 and rule 13)

TITLE OF THE INVENTION

“A MACHINE LEARNING BASED SYSTEM FOR CYBERATTACK DETECTION
AND PREVENTION IN CLOUD-BASED, WIRELESS VIRTUAL ENVIRONMENTS”

Applicant

NAME	NATIONALITY	ADDRESS
1. Dr. P. Chitra	Indian	Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai - 600026
2. Dr. Shankar R.	Indian	Professor, Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College (Autonomous), Meerpet, Hyderabad, Pincode: 500097
3. Dr.Gandi Satyanarayana	Indian	Professor & Head, Department of Computer Science & Engineering, Avanthi Institute of Engineering and Technology, Cherukupally (Village) Near Thagarapuvalasa Bridge, Vizianagaram (Dist.), Pin-531162
4. Dr. Gogineni Krishna Chaitanya	Indian	Associate Professor, Department of Computer Science and Engineering,

		Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India
5. Dr. K. Valarmathi	Indian	Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Bangalore Trunk Road, Varadharajapuram, Poonamallee, Chennai - 600123
6. Mr. R. Sathishkannan	Indian	Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathy - Bhavani State Highway, Alathukombai, Post, Sathyamangalam, Tamil Nadu 638401

The following specification particularly describes the nature of the invention and the manner in which it is performed:

FIELD OF THE INVENTION

[001] The present invention relates to the field of the AI and ML based advanced system for cyberattack detection and prevention in cloud-based with novel techniques, methods, devices and apparatus. The invention more particularly relates to a machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments.

BACKGROUND OF THE INVENTION

[002] The following description provides the information that may be useful in understanding the present invention. It is not an admission that any of the information provided herein is prior art or relevant to the presently claimed invention, or that any publication specifically or implicitly referenced is prior art.

[003] Further, the approaches described in this section are approaches that could be pursued, but not necessarily approaches that have been previously conceived or pursued. Therefore, unless otherwise indicated, it should not be assumed that any of the approaches described in this section qualify as prior art merely by virtue of their inclusion in this section.

[004] As cloud network exchange data mechanism among a vast number of nodes (such as clients, mobile computing devices, servers, etc.) via a variety of gateways (such as routers, etc.) and communications protocols, the complexity of computing environments rises. This level of complexity renders the network vulnerable to hacking and other forms of espionage. Man in the middle attacks are a form of unwanted access in which a node or other agent in the computer environment reroutes or otherwise intercepts communications between two other nodes. Such Man in the Middle assaults sometimes go

undetected for extended periods of time, allowing the attackers to steal valuable information like payment passwords.

[005] Accordingly, on the basis of aforesaid facts, there remains a need in the prior art to provide a machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments. Therefore, it would be useful and desirable to have a system, method, apparatus and interfaces to meet the above-mentioned needs.

SUMMARY OF THE PRESENT INVENTION

[006] In view of the foregoing disadvantages inherent in the known types of conventional cyberattack detection and prevention in cloud-based systems, methods and techniques, are now present in the prior art, the present invention provides a machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments, which has all the advantages of the prior art and none of the disadvantages.

[007] It is an object of the present invention, wherein a first node in a networked computing environment performs one or more man-in-the-middle (MITM) detection tests to determine whether communications between two other nodes in the same network have been intercepted or attempted to be intercepted by a third node; and first node concludes that at least one of the tests indicates that the communications are likely to have been intercepted.

[008] Furthermore, first node is given information defining the determinations; at least one of the various MITM detection tests makes use of a machine learning model educated using training data including numerous samples that characterise network data traffic interception to a computer system.

[009] In this respect, before explaining at least one object of the invention in detail, it is to be understood that the invention is not limited in its application to the details of set of rules and to the arrangements of the various models set forth in the following description or illustrated in the drawings. The invention is capable of other objects and of being practiced and carried out in various ways, according to the need of that industry. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[010] These together with other objects of the invention, along with the various features of novelty which characterize the invention, are pointed out with particularity in the disclosure. For a better understanding of the invention, its operating advantages and the specific objects attained by its uses, reference should be made to the accompanying drawings and descriptive matter in which there are illustrated preferred embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[011] When considering the following thorough explanation of the present invention, it will be easier to understand it and other objects than those mentioned above will become evident. Such description refers to the illustrations in the annex, wherein:

[012] **FIG. 1**, illustrates a conventional machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments, in accordance with an embodiment of the present invention.

[013] **FIG. 2**, illustrates another conventional schematic diagram of the machine learning based system for cyberattack detection and prevention in

cloud-based, wireless virtual environments, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[014] The following sections of this article will provide various embodiments of the current invention with references to the accompanying drawings, whereby the reference numbers utilised in the picture correspond to like elements throughout the description. However, this invention is not limited to the embodiment described here and may be embodied in several other ways. Instead, the embodiment is included to ensure that this disclosure is extensive and complete and that individuals of ordinary skill in the art are properly informed of the extent of the invention. Numerical values and ranges are given for many parts of the implementations discussed in the following thorough discussion. These numbers and ranges are merely to be used as examples and are not meant to restrict the claims' applicability. A variety of materials are also recognised as fitting for certain aspects of the implementations. These materials should only be used as examples and are not meant to restrict the application of the innovation.

[015] Referring now to the drawings, these are illustrated in FIG. **1 & 2**, the present invention discloses a machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments. The system is comprised of, but not limited to, one or more man-in-the-middle (MITM) detection tests initiated by a first node of a networked computing environment to determine whether communications between two other nodes of the same network have been intercepted or attempted to be intercepted by

a third node; and it is determined by the first node that at least one of the tests indicates that the communications are likely to have been intercepted.

[016] In accordance with another embodiment of the present invention, the first node is supplied with data defining the determinations; wherein at least one of the multiple types of MITM detection tests utilises at least one machine learning model trained by training data consisting of multiple samples that individually characterise network data traffic interception to a computer system received.

[017] In accordance with another embodiment of the present invention, labelling at least some of the samples to describe a likelihood of each such sample as relating to an unauthorised interception of data traffic; categorising the samples into clusters based on their shared characteristics.

[018] In accordance with another embodiment of the present invention, training the at least one machine learning model using the assigned labelled clusters, which, once trained, determines a likelihood of future samples as relating to an unauthorised interception of data traffic to a corresponding computing device; and assigning each cluster with a label corresponding to the majority of samples within such cluster.

[019] In accordance with another embodiment of the present invention, a method for detecting a cyber-attack on a plant managed by a Supervisory Control and Data Acquisition (SCADA) system, wherein the attacker's goal is to cause physical damage or harm the functionality of the plant, includes equipping the plant with one or more dedicated industrial computerised devices, passively connected to the SCADA system, wherein each of said

industrial computerised devices comprises a processor that is configured with a data validation module.

[020] Further, one or more specialised industrial computerised device to passively monitor in parallel all data transferred between each of the controllers and the SCADA system, including the outputted data, at points closest to each of the controllers by using the one or more specialised industrial computers to look for discrepancies between the actual plant state and the physical operation model.

[021] In accordance with another embodiment of the present invention, a communication protocol test is one sort of MITM detection test; it compares the cypher suite used in cryptographic communications between the first and third nodes to a known cypher suite, and any disparities between the two indicate interception or attempted eavesdropping by the third node.

[022] The above-mentioned invention is provided with the preciseness in its real-world applications to provide a machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments. Further, a means of determining whether or not an app is harmful, including the training phase, a server programme accesses a database containing information on a collection of software applications; from this data, the server application derives a classification algorithm that may be used to determine whether an application is likely to be benign or harmful.

[023] The benefits and advantages that the present invention may offer have been discussed above with reference to particular embodiments. These benefits and advantages are not to be interpreted as critical, necessary, or essential features of any or all of the embodiments, nor are they to be read as

any elements or constraints that might contribute to their occurring or becoming more evident.

[024] Although specific embodiments have been used to describe the current invention, it should be recognized that these embodiments are merely illustrative and that the invention is not limited to them. The aforementioned
5 embodiments are open to numerous alterations, additions, and improvements. These adaptations, changes, additions, and enhancements are considered to be within the purview of the invention.

We Claim:

1. A machine learning based system for cyberattack detection and prevention in cloud-based, wireless virtual environments, comprising:

one or more man-in-the-middle (MITM) detection tests initiated by a first node of a networked computing environment to determine whether communications between two other nodes of the same network have been intercepted or attempted to be intercepted by a third node; and it is determined by the first node that at least one of the tests indicates that the communications are likely to have been intercepted.

2. The system as claimed in claim 1, wherein the first node is supplied with data defining the determinations; wherein at least one of the multiple types of MITM detection tests utilises at least one machine learning model trained by training data consisting of multiple samples that individually characterise network data traffic interception to a computer system received.

3. The system as claimed in claim 1, wherein labelling at least some of the samples to describe a likelihood of each such sample as relating to an unauthorised interception of data traffic; categorising the samples into clusters based on their shared characteristics.

4. The system as claimed in claim 1, wherein training the at least one machine learning model using the assigned labelled clusters, which, once trained,

determines a likelihood of future samples as relating to an unauthorised interception of data traffic to a corresponding computing device; and assigning each cluster with a label corresponding to the majority of samples within such cluster.

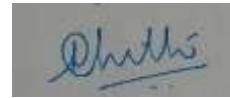
- 5 **5.** The system as claimed in claim **1**, wherein a method for detecting a cyber-attack on a plant managed by a Supervisory Control and Data Acquisition (SCADA) system, wherein the attacker's goal is to cause physical damage or harm the functionaUty of the plant, includes equipping the plant with one or more dedicated industrial computerised devices, passively connected to the
- 10 SCADA system, wherein each of said industrial computerised devices comprises a processor that is configured with a data validation module.
- 6.** The system as claimed in claim **1**, wherein one or more specialised industrial computerised device to passively monitor in parallel all data transferred between each of the controllers and the SCADA system, including the outputted
- 15 data, at points closest to each of the controllers by using the one or more specialised industrial computers to look for discrepancies between the actual plant state and the physical operation model.
- 7.** The system as claimed in claim **1**, wherein a communication protocol test is one sort of MITM detection test; it compares the cypher suite used in
- 20 cryptographic communications between the first and third nodes to a known

cypher suite, and any disparities between the two indicate interception or attempted eavesdropping by the third node.

8. The system as claimed in claim 1, wherein a means of determining whether or not an app is harmful, including the training phase, a server programme
5 accesses a database containing information on a collection of software applications; from this data, the server application derives a classification algorithm that may be used to determine whether an application is likely to be benign or harmful.

10 **Dated this 18th day of February 2023**

Signature:



Applicant(s)

Dr. P. Chitra et. al.

ABSTRACT

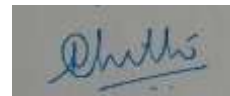
A MACHINE LEARNING BASED SYSTEM FOR CYBERATTACK DETECTION AND PREVENTION IN CLOUD-BASED, WIRELESS VIRTUAL ENVIRONMENTS

[025] The present invention discloses a machine learning based system for
5 cyberattack detection and prevention in cloud-based, wireless virtual environments. In
the present invention, one or more man-in-the-middle (MITM) detection tests initiated
by a first node of a networked computing environment to determine whether
communications between two other nodes of the same network have been intercepted
or attempted to be intercepted by a third node; and it is determined by the first node
10 that at least one of the tests indicates that the communications are likely to have been
intercepted. Further, the first node is supplied with data defining the determinations;
wherein at least one of the multiple types of MITM detection tests utilises at least one
machine learning model trained by training data consisting of multiple samples that
individually characterise network data traffic interception to a computer system
15 received.

Accompanied Drawing [FIGS. 1-2]

Dated this 18th day of February 2023

Signature:



Applicant(s)

Dr. P. Chitra et. al.

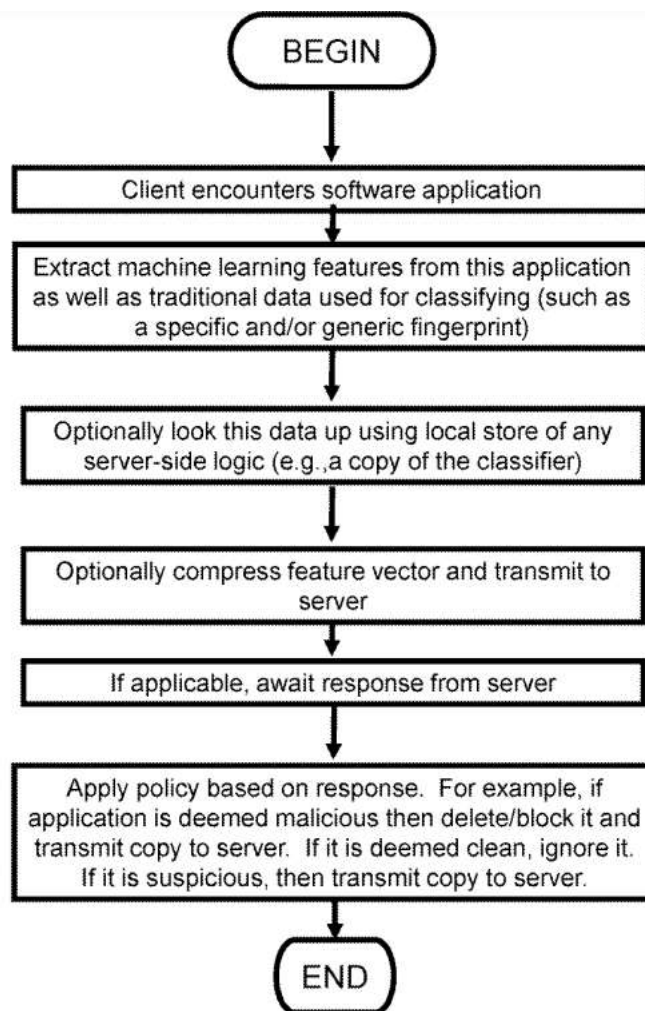
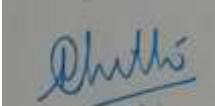


Figure 1

Signature:



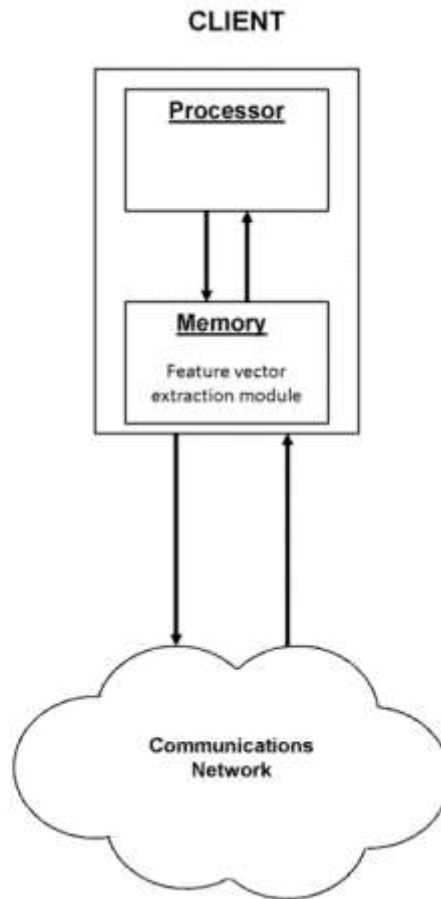


Figure 2

Dated this 18th day of February 2023

Signature:

A handwritten signature in blue ink, appearing to read "Dr. P. Chitra et. al.", is shown within a grey rectangular box.

Applicant(s) Name: Dr. P. Chitra et. al.

FORM 3 THE PATENTS ACT, 1970 (39 of 1970) and THE PATENTS RULES, 2003 STATEMENT AND UNDERTAKING UNDER SECTION 8 (See section 8; Rule 12)					
1. Name of the applicant(s).		I/We. Dr. P. Chitra et. al., all are citizen of India, Address of one of the Applicant: Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai -600026.			
2. Name, address and nationality of the joint applicant.		(i) that I/We have not made any application for the same/substantially the same invention outside India Or (ii) that I/We who have made this application No... dated alone/jointly with ; made for the same/ substantially same invention, application(s) for patent in the other countries, the particulars of which are given below:			
Name of the Country	Date of Application	Application No.	Status of the Application	Date of Publication	Date of grant
-	-	-	-	-	-
3. Name and address of the assignee		(iii) that the rights in the application(s) has/have been assigned to none that I/We undertake that upto the date of grant of the patent by the Controller, I/We would keep him informed in writing the details regarding corresponding applications for patents filed outside India within six months from the date of filing of such application. Dated this 18th day of February 2023			

4. To be signed by the applicant or his authorized registered patent agent.	Signature: 
5. Name of the natural person who has signed.	Dr. P. Chitra et. al. Name of the Applicant(s)
	To The Controller of Patents, The Patent Office, at Chennai
Note.- Strike out whichever is not applicable;	

FORM- 5
THE PATENTS ACT, 1970
(39 of 1970)
&
The Patents Rules, 2003
DECLARATION AS TO INVENTORSHIP
[See Section 10(6) and Rule 13(6)]

1. NAME OF THE APPLICANT

I/We. Dr. P. Chitra et. al., all are citizen of India, Address of one of the Applicant: Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai -600026.

hereby declare that the true and first inventor(s) of the invention disclosed in the complete specification filed in pursuance of ~~my~~/ our application numbered _____ dated 18-02-2023 is/are

2. INVENTOR(S)

(a) NAME	(b) NATIONALITY	(c) ADDRESS
1. Dr. P. Chitra	Indian	Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai - 600026
2. Dr. Shankar R.	Indian	Professor, Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College (Autonomous), Meerpet, Hyderabad, Pincode: 500097
3. Dr.Gandi Satyanarayana	Indian	Professor & Head, Department of Computer Science & Engineering, Avanthi Institute of Engineering and Technology, Cherukupally (Village) Near Thagarapuvalasa Bridge, Vizianagaram (Dist.), Pin-531162
4. Dr. Gogineni Krishna Chaitanya	Indian	Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

5. Dr. K. Valarmathi	Indian	Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Bangalore Trunk Road, Varadharajapuram, Poonamallee, Chennai - 600123
6. Mr. R. Sathishkannan	Indian	Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathy - Bhavani State Highway, Alathukombai, Post, Sathyamangalam, Tamil Nadu 638401
3. DECLARATION TO BE GIVEN WHEN THE APPLICATION IN INDIA IS FILED BY THE APPLICANT(S) IN THE CONVENTION COUNTRY:— N.A. We the applicant(s) in the convention country hereby declare that our right to apply for a patent in India is by way of assignment from the true and first inventor(s).		
Dated this 18th day of February 2023 Dr. P. Chitra et. al. Applicant(s) To, The Controller of Patents The Patent Office, Chennai		

FORM 9

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

REQUEST FOR PUBLICATION

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

I/We **Dr. P. Chitra, Dr. Shankar R., Dr. Gandhi Satyanarayana, Dr. Gogineni Krishna Chaitanya, Dr. K. Valarmathi, Mr. R. Sathishkannan** hereby request for early publication of my/our [Patent Application No.]
TEMP/E-1/12986/2023-CHE

Dated **18/02/2023 00:00:00** under section 11A(2) of the Act.

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

Signature

Name of the signatory

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

This form is electronically generated.