



Office of the Controller General of Patents, Designs & Trade Marks
Department of Industrial Policy & Promotion,
Ministry of Commerce & Industry,
Government of India

सत्यमेव जयते

(<http://ipindia.nic.in/index.htm>)



(<http://ipindia.nic.in/index.htm>)

Application Details

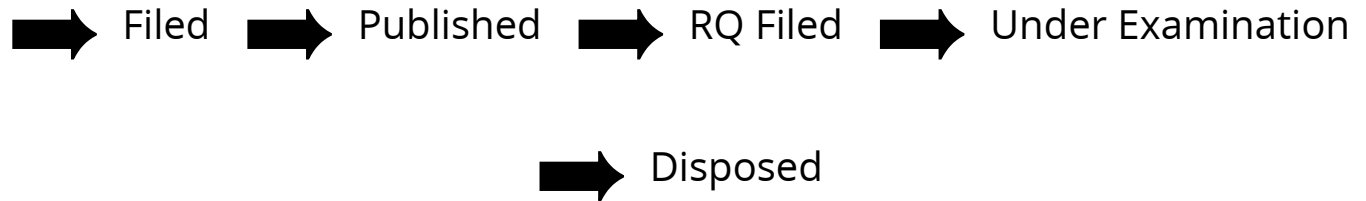
APPLICATION NUMBER	202141000707
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	07/01/2021
APPLICANT NAME	1 . Mohana S. D 2 . Nitish A 3 . Dr. S.P. Shiva Prakash 4 . Bhavya D 5 . Santhosh Kumar K. S 6 . Dr. J. Hanumanthappa 7 . Dr. D.S. Vinod 8 . Chethan Raj C
TITLE OF INVENTION	ROOT CAUSE ANALYSIS, THREAT INTERPRETATION, AND NETWORK SURVIVABILITY PREDICTION DEVICE FOR HETEROGENEOUS NETWORKS
FIELD OF INVENTION	COMMUNICATION
E-MAIL (As Per Record)	nitish.anantha@acm.org
ADDITIONAL-EMAIL (As Per Record)	
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	--
PUBLICATION DATE (U/S 11A)	19/02/2021

Application Status

APPLICATION STATUS

Awaiting Request for Examination

[View Documents](#)



In case of any discrepancy in status, kindly contact ipo-helpdesk@nic.in

FORM 1				(FOR OFFICE USE ONLY)	
<p align="center">THE PATENTS ACT 1970 (39 of 1970) and THE PATENTS RULES, 2003</p> <p align="center">APPLICATION FOR GRANT OF PATENT</p> <p>(See section 7, 54 and 135 and sub-rule (1) of rule 20)</p>				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 (<input checked="" type="checkbox"/>)		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	
Dr. J. Hanumanthappa		INDIAN	INDIA	Designation	Associate Professor, Dept. of Studies in Computer Science, University of Mysore
				Street	Manasagangothri
				City	Mysuru
				State	Karnataka
				Country	India
Nitish A		INDIAN	INDIA	Designation	Research Scholar, Dept. of Studies in Computer Science, University of Mysore
				Street	Manasagangothri
				City	Mysuru
				State	Karnataka
				Country	India
Dr. S.P. Shiva Prakash		INDIAN	INDIA	Designation	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University
				Street	JSS Technical Institution Campus,
				City	Mysuru
				State	Karnataka
				Country	India
Dr. D.S. Vinod		INDIAN	INDIA	Designation	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University
				Street	JSS Technical Institution Campus,
				City	Mysuru
				State	Karnataka
				Country	India

			State	Karnataka
			Country	India
			Pin code	570006
Bhavya D	INDIAN	INDIA	Designation	Assistant Professor, Dept. of Computer Science and Engineering, PES College of Engineering
			Street	PES Engineering College Rd, PES College Campus
			City	Mandya
			State	Karnataka
			Country	India
			Pin code	571401
Santhosh Kumar K. S	INDIAN	INDIA	Designation	Research Scholar, Dept. of Studies in Computer Science, University of Mysore
			Street	Manasagangothri
			City	Mysuru
			State	Karnataka
			Country	India
			Pin code	570006
Chethan Raj C	INDIAN	INDIA	Designation	Associate Professor, Dept. of Computer Science and Engineering, Mysuru Royal Institute of Technology
			Street	Palahally village, Laxmi Pura Road, S R Patna-Q
			City	Mandya
			State	Karnataka
			Country	India
			Pin code	571438
Mohana S. D	INDIAN	INDIA	Designation	Research Scholar, Dept. of Information Science and Engineering, JSS Science and Technology University
			Street	JSS Technical Institution Campus,
			City	Mysuru
			State	Karnataka
			Country	India
			Pin code	570006

3B. CATEGORY OF APPLICANT [Please tick (✓) at the appropriate category]

Natural Person (✓)	Other than Natural Person		
	Small Entity ()	Startup ()	Others ()

4. INVENTOR(S) [Please tick () at the appropriate category]

Are all the inventor(s) same as the applicant(s) named above?	Yes (✓)	No ()
---	-----------	--------

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

Name in Full	Nationality	Country of Residence	Address of the Inventor	
Dr. J. Hanumanthappa	INDIAN	INDIA	Designation	Associate Professor, Dept. of Studies in Computer Science, University of Mysore
			Street	Manasagangothri
			City	Mysuru
			State	Karnataka
			Country	India
Nitish A	INDIAN	INDIA	Designation	Research Scholar, Dept. of Studies in Computer Science, University of Mysore
			Street	Manasagangothri
			City	Mysuru
			State	Karnataka
			Country	India
Dr. S.P. Shiva Prakash	INDIAN	INDIA	Designation	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University
			Street	JSS Technical Institution Campus,
			City	Mysuru
			State	Karnataka
			Country	India
Dr. D.S. Vinod	INDIAN	INDIA	Designation	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University
			Street	JSS Technical Institution Campus,
			City	Mysuru
			State	Karnataka
			Country	India
Bhavya D	INDIAN	INDIA	Designation	Assistant Professor, Dept. of Computer Science and Engineering, PES College of Engineering
			Street	PES Engineering College Rd, PES College Campus
			City	Mandya
			State	Karnataka
			Country	India
Santhosh Kumar K. S	INDIAN	INDIA	Designation	Research Scholar, Dept. of Studies in Computer Science, University of Mysore
			Street	Manasagangothri
			City	Mysuru
			State	Karnataka
			Country	India
Chethan Raj C	INDIAN	INDIA	Designation	Associate Professor, Dept. of Computer Science and Engineering, Mysuru Royal Institute of Technology
			Street	Palahally village, Laxmi Pura Road, S R Patna-Q

			City	Mandya
			State	Karnataka
			Country	India
			Pin code	571438
Mohana S. D	INDIAN	INDIA	Designation	Research Scholar, Dept. of Information Science and Engineering, JSS Science and Technology University
			Street	JSS Technical Institution Campus,
			City	Mysuru
			State	Karnataka
			Country	India
			Pin code	570006

5. TITLE OF THE INVENTION

ROOT CAUSE ANALYSIS, THREAT INTERPRETATION, AND NETWORK SURVIVABILITY PREDICTION DEVICE FOR HETEROGENEOUS NETWORKS

6. AUTHORISED REGISTERED PATENT AGENT(S)

IN/ PA No.	Nil
Name	Nil
Mobile No.	Nil

7. ADDRESS FOR SERVICE OF APPLICANT IN INDIA

Name	Mr. Nitish A
Postal Address	Research Scholar, Dept. of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka 570006
Telephone No.	
Mobile No.	+91 9480390007
Fax No.	-
E-mail ID	nitish.anantha@acm.org

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)
Nil					

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
Nil	

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
Nil	

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
-----------------------------	------------------------------------

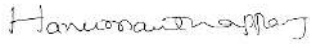
12. DECLARATIONS

(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: **06th Day of January 2021**



Dr. J. Hanumanthappa



Nitish A



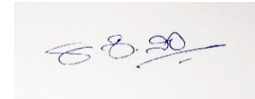
Dr. S.P. Shiva Prakash



Dr. D.S. Vinod

Bhavya - D

Bhavya D



Santhosh Kumar K. S



Chethan Raj C



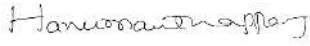
Mohana S. D

(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.

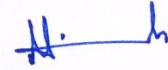
(a) Date: **06th Day of January 2021**



Dr. J. Hanumanthappa




Nitish A



Dr. S.P. Shiva Prakash



Dr. D.S. Vinod



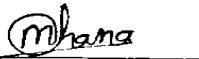
Bhavya D



Santhosh Kumar K. S



Chethan Raj C



Mohana S. D

(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).

13. FOLLOWING ARE THE ATTACHMENTS WITH THE APPLICATION

(a) Form 2

Item	Details	Fee	Remarks
Complete/provisional specification) #	No. of pages		
No. of Claim(s)	No. of claims and No. of pages		
Abstract	No. of pages		
No. of Drawing(s)	No. of drawings and No. of pages		

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

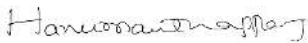
(h) Declaration of Inventor-ship on Form 5

Total fee in Cash/ Banker's Cheque /Bank Draft Bearing No.....

Date.....onBank.

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.

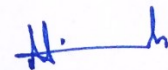
Dated this **06th Day of January 2021**



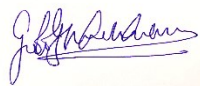
Dr. J. Hanumanthappa



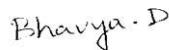
Nitish A



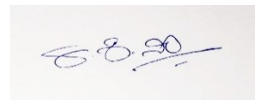
Dr. S.P. Shiva Prakash



Dr. D.S. Vinod



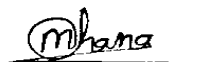
Bhavya D



Santhosh Kumar K. S



Chethan Raj C



Mohana S. D

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

FORM - 2
THE PATENTS ACT, 1970
(39 OF 1970)
THE PATENTS RULES, 2003
COMPLETE SPECIFICATION
(Section 10; rule 13)

1. TITLE OF THE INVENTION

ROOT CAUSE ANALYSIS, THREAT INTERPRETATION, AND NETWORK SURVIVABILITY PREDICTION DEVICE FOR HETEROGENEOUS NETWORKS
--

2. APPLICANTS

Applicants Name	Nationality	Address
Dr. J. Hanumanthappa	INDIAN	Associate Professor, Department of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka, India, 570006
Nitish A	INDIAN	Research Scholar, Department of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka, India, 570006
Dr. S.P. Shiva Prakash	INDIAN	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University, JSS Technical Institution Campus, Mysuru, Karnataka, India, 570006
Dr. D.S. Vinod	INDIAN	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University, JSS Technical Institution

		Campus, Mysuru, Karnataka, India, 570006
Bhavya D	INDIAN	Assistant Professor, Department of Computer Science and Engineering, PES College of Engineering, PES Engineering College Rd, PES College Campus, Mandya, Karnataka, 571401
Santhosh Kumar K. S	INDIAN	Research Scholar, Department of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka, India, 570006
Chethan Raj C	INDIAN	Associate Professor, Dept. of Computer Science and Engineering, Mysuru Royal Institute of Technology, Palahally village, Laxmi Pura Road, S R Patna-Q, Mandya, Karnataka, India, 571438
Mohana S. D	INDIAN	Research Scholar, Dept. of Information Science and Engineering, JSS Science and Technology University, JSS Technical Institution Campus, Mysuru, Karnataka, India, 570006

3. The following specification particularly describes the invention and the manner in which it is to be performed.

ROOT CAUSE ANALYSIS, THREAT INTERPRETATION, AND NETWORK SURVIVABILITY PREDICTION DEVICE FOR HETEROGENEOUS NETWORKS

FIELD OF INVENTION

[001] The present invention generally relates to Heterogenous Network Security Systems. More specifically, the invention describes a distributed Intrusion Detection and Prevention System (IDPS) for heterogenous (Hetlot-based) networks, that is implementable on a System-on-chip (SoC) that houses the IDPS facilitating units, wherein the proposed IDPS system has an impact on the heterogeneity, real-time traffic processing, energy-efficiency, and changing network contexts due to constituent ad hoc devices with varied specifications. The invention further extends by correlating expert knowledge with data-driven detection techniques, root cause analysis of detected threats, and network survivability prediction based on threat severity.

BACKGROUND OF THE INVENTION

[002] A network intrusion detection and prevention system is a system that monitors and scans traffic over a network to identify suspicious activity and proceeds to issue alerts to a Security Information and Event Management (SIEM) system or to an administrator. As much as it is important to detect threats that emerge from outside, there are a growing anomaly of threats that originate from within the network. According to an Intel Security Report titled 'Grand Theft Data', around 43 percent of network security breaches happened due to internal contributors.

[003] In a heterogenous network built over networking technologies such as Internet-of-things (IoT), billions of devices come together with diverse protocols and varied specifications. There will be more than 50 billion

internet-of-things (IoT) powered devices by 2020, according to a Juniper research report. It is not the sheer volume of devices that come together in a typical HetIoT network, it is the sheer diversity that makes managing HetIoT devices challenging. For instance, a heterogenous network may comprise of devices that comply with various IoT-based protocols such as MQTT, XMPP-IoT, 6LoWPAN, etc., WSN-based protocols like LEACH, PEGASIS, SL-QoS-MS, etc., including the most common TCP/IP-based protocols such as UDP, SNMP, ARP, etc. A heterogeneous network can house devices that work on various infrastructure protocols, communication protocols, data protocols, identification protocols, etc. Ensuring security with heterogeneity and energy-efficiency in HetIoT-like networks would be a herculean challenge to manage.

[004] The growing need for information and process ubiquity, coupled with the reduced hardware costs have resulted in a rampant increase in the number of unconventional and non-conforming devices being connected to the Internet—facilitating networking technologies like the internet of things (industrial and social IoTs), cyber-physical systems (CPS), SCADA (smart grids), wireless sensor networks (WSN), etc.—consisting of heterogeneous devices.

[005] It is no secret now that the security of such heterogenous networks could be compromised through any of these many devices or modes that will open-up additional threat vectors. A holistic network and upstream threat detection and prevention system becomes the key overlying a layer of device-by-device or case-by-case threat management strategy. Developing an intrusion detection system that maintains the status quo of the network devices with respect to the confidentiality, integrity, authentication, privacy and physical security of devices is no mean task.

[006] With the exponential increase in the cyber threat landscape, a heterogeneous network built for handling time-critical and mission-critical

applications, is highly susceptible to the attacks associated with network degradation and data loss, resulting in high recovery costs. The solution to providing efficient security for such a network scenario involves having the ability to analyse voluminous data (both, spatial and temporal) collected from various heterogeneous sources to detect and prevent the existing attacks, predict the possible attacks in the future, and estimate their impacts on the devices of the network for better threat interpretation and survivability—necessitating a distributed, adaptive network-based IDPS.

[007] The real challenge lies in addressing the Zero-day attacks, resulting from the undiscovered network vulnerabilities, characterized by the non-existence of suitable knowledgebase and the exhibition of variations from the existing attack signatures. Those, with lower variance scores from the baseline, are predictable and the others with high variance are challenging to predict.

[008] The recent capabilities of HetIoT with the advancements in hardware and software technologies, reduction in costs, and ease of access to the information resources have resulted in a rampant increase in the number of devices being connected to the Internet, leading to the frequent generation of humongous amounts of heterogeneous network traffic that requires processing in real-time. Adversaries that tend to gain intellectual or monetary benefits from the critical information dealt in HetIoT, resort to launching attacks that can result in network infiltration, information system compromise, and data breaches—essentially rendering the network defenseless, necessitating redesign—resulting in very high recovery costs.

[009] A Microsoft US patent document US009560068B2, titled “Network Intrusion Detection with Distributed Correlation” describes a network security framework with multi-level processing to identify security threats. The monitoring agents are deployed in each node in the network to obtain threats by analysing the network traffic locally. The authors consider an

enterprise network consisting of high-power devices where a specific host identifies suspicious traffic and summarizes the activity. The summary is then transmitted to the other devices to correlate with the respective traffic. The work neither offers a description of the usage of low-power devices and their challenges nor considers the case of context-change that is common in ad hoc networks.

[010] Another US patent US007062683B2, assigned to BMC Software, titled “Two-Phase Root Cause Analysis” proposes a two-phase approach, starting from the upstream analysis to identify the failed nodes in the enterprise-specific network, followed by the downstream analysis to determine the impact of failure. The work offers no information on context-change.

[011] A US patent document US010511620B2 titled “Detection of Vulnerable Devices in Wireless Networks” describes a detection system for vulnerable devices in wireless networking environment through profiling. The vulnerable devices detected upon investigation trigger alerts and facilitate mitigating actions. Each device is profiled into fifteen attributes and is assessed for vulnerability based on the values. The device-specific profiling presented in the work is not suitable for a network involving dynamic contexts.

[012] The previous works highlighted, address either enterprise-specific or network-specific vulnerabilities and offer no information about their applicability either on heterogeneous networks or on encrypted traffic. Therefore, there exists a need for an Intrusion Detection and Prevention System (IDPS) that works effectively on complex heterogeneous networks.

SUMMARY OF THE INVENTION

[013] The objective of the present invention is to design an Intrusion Detection and Prevention System (IDPS) to provide security to

heterogeneous networks through automated learning-based techniques correlated with expert knowledge to reduce false alarms, a means to determine threat severity and predict the survivability of the network in a given threat context.

[014] The aforementioned aspects along with the objectives and the advantages can be achieved as described herein.

[015] The proposed Intrusion Detection and Prevention System (IDPS) is designed to be executed in 2 phases viz., Network Initialization and Anomaly Detection. Network Initialization Phase comprises of collection of datasets of heterogeneous network traffic instances from various sources, thereby constituting a knowledgebase. The knowledgebase comprises of datasets with Normal Network Traffic Instances (baseline) and Known Attack Traces which constitute the Data-driven information (as outlined in Para [036]), to facilitate distributed data-driven misuse detection.

[016] The knowledgebase constituted in the Network Initialization Phase also comprise of a high-level expert knowledge-driven network profile to generate Knowledge-driven information (as outlined in Para [037]) in the forms of root cause analysis (RCA) and threat severity analysis (TSA) tables to identify network faults and threat severity, correlated with the alerts from the automated low-level data-driven learning-based techniques.

[017] The second phase outlined in the Intrusion Detection and Prevention System (IDPS) is the Anomaly Detection phase which is performed by setting up the network according to context defined during Initialization phase and monitoring the inbound and outbound traffic from the constituent devices within the network to identify anomalies.

[018] The knowledge-driven information about the network gathered via the knowledgebase is correlated with the detected anomalies to filter-out false and unimportant alerts, thereby facilitating better context-awareness.

[019] New attack traffic is generated from the correlated anomalies to interpret threats involving signatures with high variance from the baseline and predict network survivability in a given threat context by facilitating predictive network maintenance in defense against Zero-day attacks.

[020] The aforementioned procedures for efficient IDPS which are realized as a SoC-based distributed architecture deployed at switch or access point (AP) levels, offer protection against both insider and outsider attacks with reduced traffic processing (including encapsulation and decapsulation of packets, normalization of packets into session records, etc.), resulting in reduced latency.

[021] Proposed security solution based on device and attack categories scale well with the changes in context and size of the network.

[022] The proposed SoC device performs firewall-like traffic monitoring in addition to providing IDPS for context-changing distributed Hetlot-like networks—essentially replacing dedicated firewalls.

BRIEF DESCRIPTION OF FIGURES

[023] Other features and advantages of the present invention will become apparent from the detailed description of the invention which follows, when considered in light of the accompanying drawings in which:

[024] FIG. 1 depicts the design of a hardware-based SoC device with the computing capabilities of the overall procedure described in FIG. 2.

[025] FIG. 2 depicts an overall flow of the proposed invention, including the network initialization and anomaly detection phases.

[026] FIG. 3 describes the intended real-time network setup based on the specifications in Phase 1.

[027] FIG. 4 depicts the process of network initialization, as a result of correlation between data-driven and knowledge-driven techniques.

[028] FIG. 5 provides a depiction of the anomaly detection phase, performed on real-time network traffic.

[029] FIG. 6 describes the construction of knowledge-driven information from the metadata collected from the datasets, used to predict network survivability.

[030] FIG. 7 describes the proposed correlation module, employed to reduce false alarms.

[031] FIG. 8 depicts the flow involved in high-level knowledge correlated attack traffic generation to improve the performance of anomaly detection.

[032] FIG. 9 depicts the attack data generation technique, followed by a validation technique employed in the proposal.

DETAILED DESCRIPTION

[033] The present IDPS process involves two phases namely Network Initialization wherein the existing knowledgebase is utilized to detect known attacks and Anomaly detection wherein the initialized (trained) network is deployed in real-time and monitored for anomalies, leading to new attacks.

[034] The distributed Network-based Intrusion Detection and Prevention System (IDPS) for heterogenous networks that is desired to be implemented on a System-on-chip (SoC). The SoC is configured to house the processor module that comprises of the Network Initialization Module and the Anomaly Detection module as outlined in [030] and presented in **FIG. 1**.

[035] **FIG. 1** depicts the proposed hardware-based SoC model **35**, which encompasses the proposed network-based IDPS components realized as firmware, deployed at the level of a switch or AP **39**. The SoC consists of a volatile memory module which facilitates temporary data storage during the detection process, and a Gigabit or 10-Gigabit Ethernet port **36** which enables faster traffic capture **21** and data transfer to the local storage device

13. The invention which is powered by the IDPS processing module are described in full detail in the subsequent sections.

[036] The present invention and its full process is depicted in **FIG. 2**. The proposed network model **10** is trained with the available data-driven knowledgebase **14**, resulting in an initialized network with prior intrusion detection and prevention measures, before it can be deployed in real-time.

[037] Anomalies detected upon network deployment are filtered for seemingly malicious traces, which are used to generate new attack traffic signatures. The generated signatures are correlated **19** with the expert knowledge **15** to obtain predictions **36** regarding the survivability of the network. The predictions offer information regarding the network status and its behaviour for a given context, which are reinforced for improved network redesign and the corresponding signatures are stored in the knowledgebase **13**.

[038] The present network IDPS is deployed on a sample network model **10**, built to emulate an enterprise network setup on a much smaller scale, as depicted in **FIG. 3**. It consists of heterogeneous devices, employed for specific purposes, and are ad hoc in nature, obeying different underlying protocols. An edge router **2** connects a trusted enterprise network to the untrusted Internet **1**. The enterprise network is typically equipped with a firewall **3** that monitors and blocks suspicious inbound and outbound traffic based on the predefined policies, which cannot offer a secured environment against more sophisticated, targeted and insider attacks.

[039] Network **10** may contain one or more workstations **4** with high computational power, utilized for heavy workloads. It houses various combinations of high power **4, 5, 6, 7** and low power **8**, wired **5, 6, 7**, and wireless **9** devices that are vulnerable to a large spectrum of attacks.

[040] In **FIG. 4**, the propounded network IDPS model is initialized by collecting the network traffic traces from several heterogeneous datasets **11**, pre-processed **12**, and stored in the knowledgebase **13** for further use, which constitutes the data-driven information **14** which contain the traces of normal network profile (acting as a baseline for anomaly detection) and known network attacks.

[041] The knowledgebase **13** also contains high-level knowledge-driven information **15** about the known network faults **17**. The inferences from data-driven **16** and knowledge-driven **18** decisions upon correlation reveal the network vulnerabilities **20**, that help initialize the network **10** thereby improving its survivability.

[042] Most of the traffic on the Internet is encrypted to offer privacy which requires the IDPS to analyse the traffic at the application-level. Doing so involves dealing with heterogeneous applications and their protocols. This is one of the advantages of the proposed invention over the prior-arts (as outlined in the background Para [012]), as most network-based IDPS implementations tend to ignore encrypted traffic.

[043] The initialized network can protect itself from the known attacks and faults that conform to the baseline. However, it is not equipped to detect new attacks that exhibit variations from the baseline. The anomaly detection phase detects the deviations (from the baseline) in the network traffic when deployed in real-time, as depicted in **FIG. 5**.

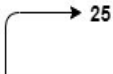
[044] The incoming stream of raw network packets **21** are subjected to inspection **22** to extract the flow-based session records that contain metadata like source and destination IP and port addresses, underlying protocols, duration of a session, etc.—constituting a signature. The learning-based anomaly detection module **23** detects the incoming deviations from the baseline, offered by the data-driven information **13**.

[045] However, not all deviations are intrusions, and hence anomaly detection is prone to high false positives. Hence, the detections are correlated **19** with the knowledge-driven information **18** to reduce false alarms.

[046] Both the phases of intrusion detection discuss correlating the expert knowledge-driven information **15** with the statistical inferences offered by the data-driven decisions. In **FIG. 6**, we describe the approach to building high-level expert knowledge.

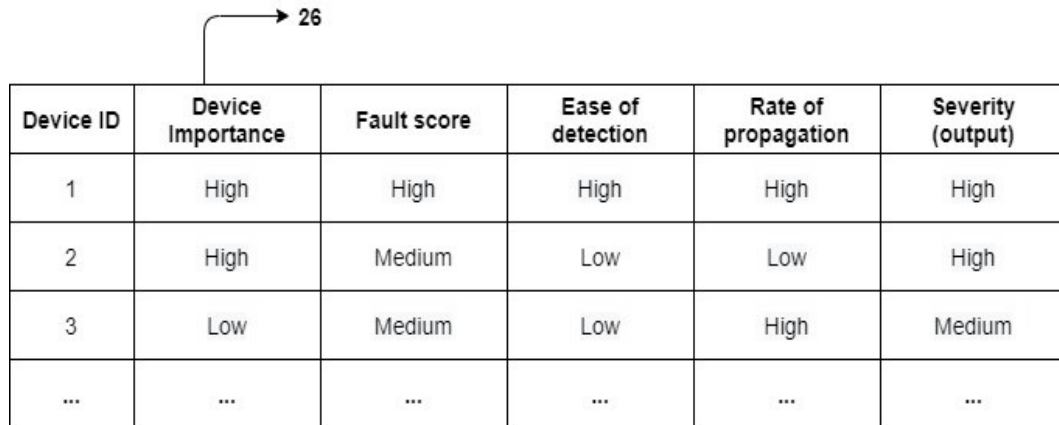
[047] The experts collect the metadata in natural language behavioural descriptions **24** from the dataset sources for each attack type and map them into six categories that constitute an RCA table **25**, a sample as presented in **Table 1**; this offers insights into the root cause of the network status that resulted in an attack. Based on the information from the RCA table, the threats are assessed to determine their severity from the expert-curated rules **26** that help predict network survivability **27** for a given attack context, a sample as presented in **Table 2**.

Table 1



Device ID	Unexpected device behavior	Device Category	Attack Category	Fault possibilities	Probable cause(s)
1	Repeating loss of network connectivity and re-initiating authentication procedure.	Wireless high power	Denial of Service (DoS)	1. Compromised access point (AP). 2. Compromised client.	De-authentication packets are transmitted unprotected, prone to spoofing.
2	Station is apparently in sleep mode. No inbound or outbound traffic from the sensor.	Wireless low power	Denial of Service (DoS)	1. Compromised AP or sensor. 2. Power consumption mechanism.	Sensor notifying AP about going to sleep through null data frame with power-save bit set.
...

Table 2



Device ID	Device Importance	Fault score	Ease of detection	Rate of propagation	Severity (output)
1	High	High	High	High	High
2	High	Medium	Low	Low	High
3	Low	Medium	Low	High	Medium
...

CORELATION MODULE

[048] **FIG. 7** depicts the correlation process **19** employed in the design. The alerts **28** generated from the data-driven detection approaches undergo validation with the knowledge-driven expert information **15** to classify the incoming traffic instances (signatures); this helps to identify the false alarms, and the network administrator or SIEM system **30** is alerted accordingly.

[049] In **FIG. 8**, the correlated alerts **28** generated upon anomaly detection (true positives and false negatives) essentially provide attack instances and their characteristics in terms of their statistical distributions. This feature is utilized to generate new attack instances that can capture degenerate distributions characterized by high variance from the baseline thereby predicting the Zero-day attacks, their behaviour, and the corresponding network vulnerabilities, which are updated in the knowledgebase **13** (as depicted in **FIG. 2**).

[050] The propounded invention highlights the importance of correlating the high-level expert knowledge with the low-level statistical inferences for improved context-awareness, resulting in reduced false alarm rates that are common in intrusion detection.

[051] The invention provides an automated learning-based model for misuse and anomaly detection techniques that provide efficient IDPS capabilities to a network. The proposition addresses the heterogeneity issues that are common in ad hoc and IoT-based networks, adhering to the current reality.

[052] The proposed knowledge-driven techniques such as the root cause analysis (RCA) and the threat severity analysis (TSA) tables provide a unique and easy way to analyse the network for faults and vulnerabilities. The distributed nature of the proposed invention enables it to provide cost-effective security solutions, based on the criticality of each device category within the network, as the devices in the same category are prone to same or similar network-level attacks.

[053] The attack traffic generation module embodied in the proposed invention facilitates predicting future attacks that the network may be prone to, depending on the current network status. The invention also embodies the technique of classifying encrypted traffic.

[054] The present invention of network-based IDPS realized as a hardware-based SoC offers updatable logical components, thereby enabling easier system maintenance. The current SoC-based invention eliminates the need for a dedicated network firewall.

CLAIMS:

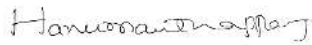
We claim:

1. A network-based intrusion detection and prevention system (NIDPS) for heterogeneous networks consisting of a plurality of devices with varied capabilities, compliance protocols, and a distributed architecture that is designed for each device category. The said NIDPS is implementable on a System-on-Chip (SoC) that houses the below-listed processing components, comprising of:
 - a. The network initialization module comprising of a collection of datasets of heterogeneous network traffic instances from various sources, constituting a data-driven knowledgebase, followed by a high-level expert knowledge-driven network profile in the form of root cause analysis (RCA) and threat severity analysis (TSA) tables—used in identifying network faults and threat severity assessment.
 - b. The anomaly detection module, which is performed by setting up the network according to the context defined during network initialization and collecting the inbound and outbound traffic to identify anomalies, correlated with the expert knowledge to filter out unimportant alerts.
 - c. The correlation module, which correlates the data-driven and knowledge-driven information to achieve reduced false alarm rates.
 - d. The attack traffic generation and validation modules comprising of an automated traffic generator to determine the traffic characteristics of the network, followed by the validator with signature validation capability to compare those characteristics with the data-driven attack signatures from the knowledgebase to make predictions on the network survivability.

2. The method as claimed in claim 1, wherein the proposed distributed approach involves identifying the subnets within the network with the corresponding device categories to speculate possible attacks and faults at a higher level, which helps to choose suitable IDP techniques.
3. The method as claimed in claim 1, wherein the SoC-based hardware architecture propounded, comprises of the computing capabilities of the aforementioned modules of the proposed NIDPS that is deployed at the access point (AP) or router level, corresponding to the subnets identified by the proposed distributed approach.
4. The method as claimed in claim 1a, wherein the proposed data-driven knowledgebase comprises of the existing datasets that are carefully selected to address specific issues in heterogeneous networks.
5. The method as claimed in claim 1a, wherein a format for constructing a root cause analysis (RCA) table, comprising of six high-level (natural language-based) descriptors from the metadata of the datasets, is proposed.
6. The method as claimed in claim 1a, wherein a format is put forth for constructing a threat severity analysis (TSA) table, comprising of six high-level (natural language-based) descriptors.
7. The method as claimed in claim 1c, wherein a technique for correlating the data-driven and knowledge-driven information during network initialization and anomaly detection phases is propounded; this helps reduce false alarms that are common in IDPS. The proposed technique also performs decision-making in allowing or blocking traffic and alerting the SIEM or administrator.
8. The method as claimed in claim 1d, wherein a network traffic generator module is propounded that determines the distributional characteristics of anomalous traffic from the constituent devices.

9. The method as claimed in claim 1d, wherein the proposed validator module compares the incoming traffic distributions with the distributions of the attack signatures from the knowledgebase to make predictions on network survivability.

Dated: 06th Day of January 2021



Dr. J. Hanumanthappa



Nitish A



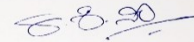
Dr. S.P. Shiva Prakash



Dr. D.S. Vinod

Bhavya D

Bhavya D



Santhosh Kumar K. S



Chethan Raj C

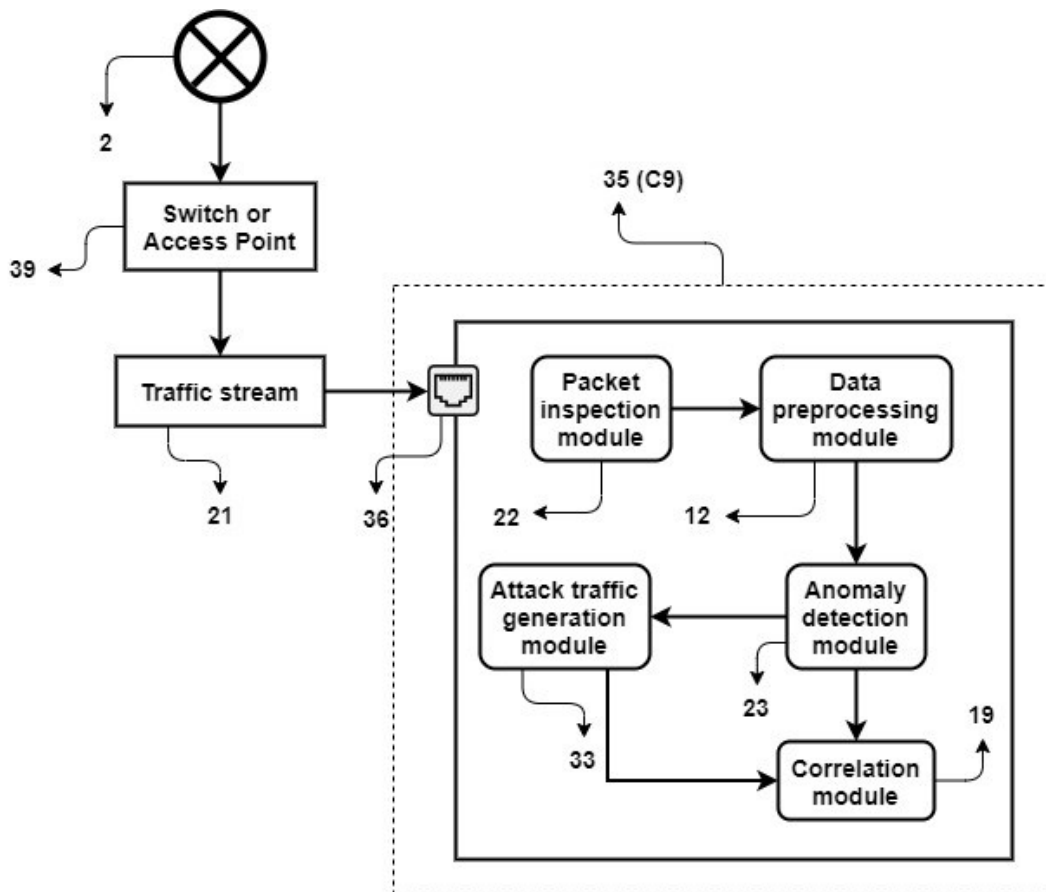


Mohana S. D

ABSTRACT

System, Method and Hardware for Network Intrusion Detection and Prevention is described. The embodiments of the invention presented, provide a framework to design and develop a network-based distributed, cost-effective intrusion detection and prevention system for heterogeneous networks. The proposed approach addresses common issues associated with such networks and provide a way to correlate low-level data-driven inferences with the high-level expert knowledge-driven information to minimize false alarms and provide better context-awareness. The invention offers a way to predict future threats based on the current network threat status and new attack traffic generation by facilitating predictive network maintenance. Doing so is beneficial in detecting the Zero-day attacks, that exhibit large variations from the baseline. The proposed network-based IDPS invention is realized as a hardware-based SoC including a firewall-like packet monitoring capability, eliminating the need for a dedicated firewall.

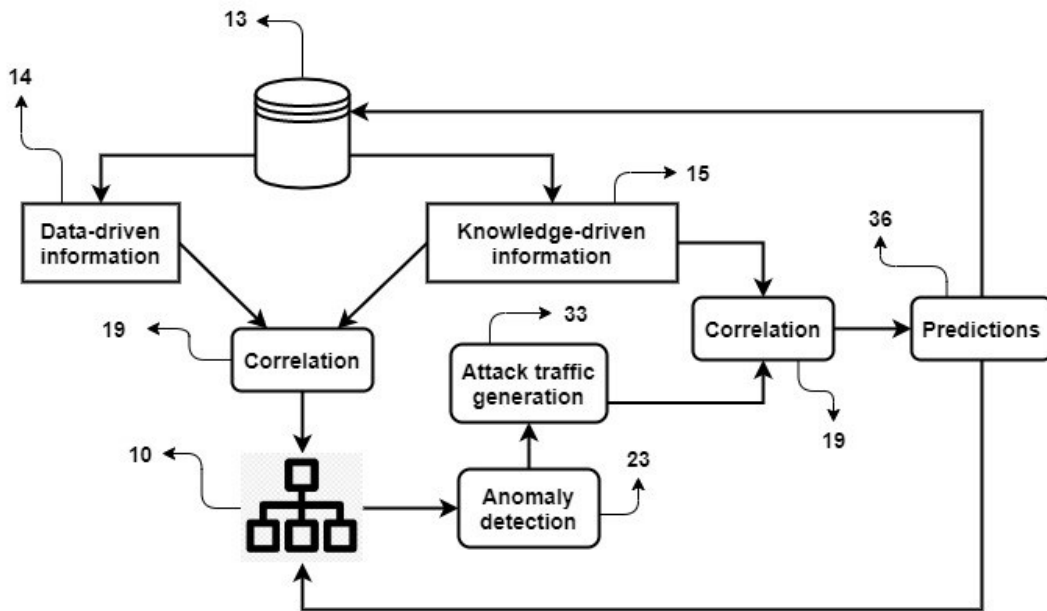
Fig. 1



Hanumanthappa

Dr. J. Hanumanthappa

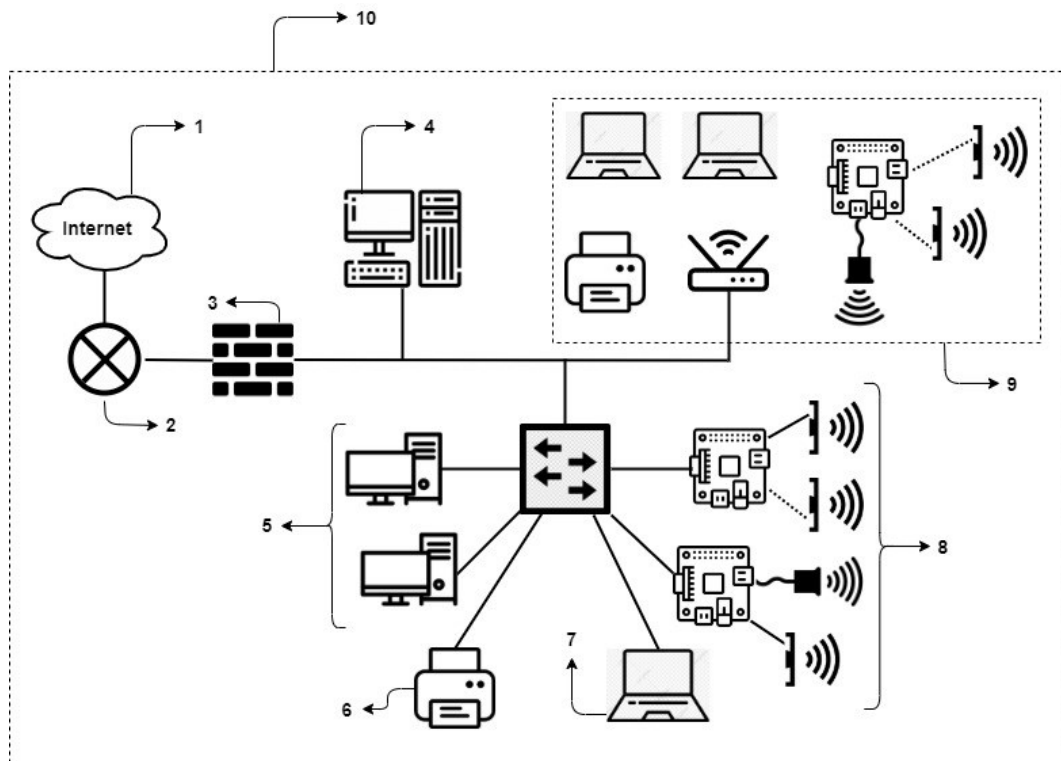
Fig. 2



Hanumanthappa

Dr. J. Hanumanthappa

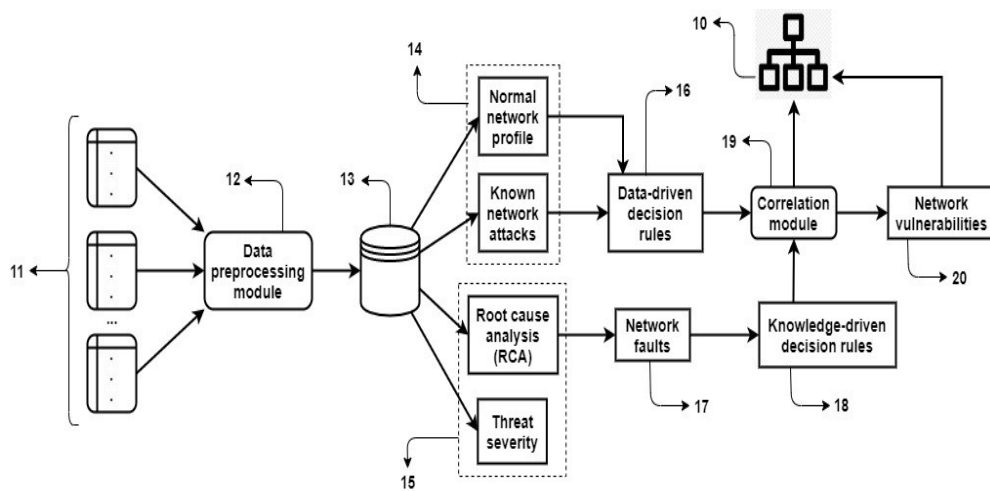
Fig. 3



Hanumanthappa

Dr. J. Hanumanthappa

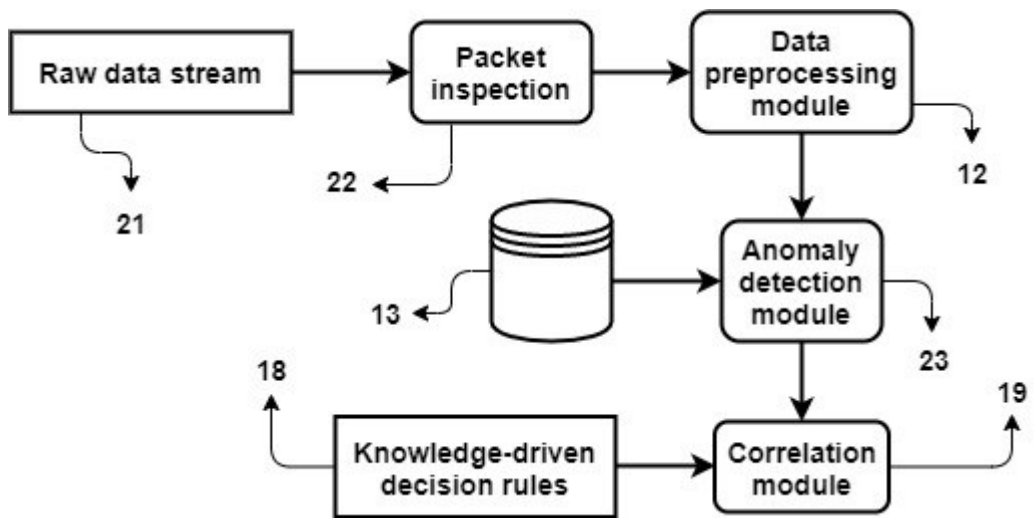
Fig. 4



Hanumanthappa

Dr. J. Hanumanthappa

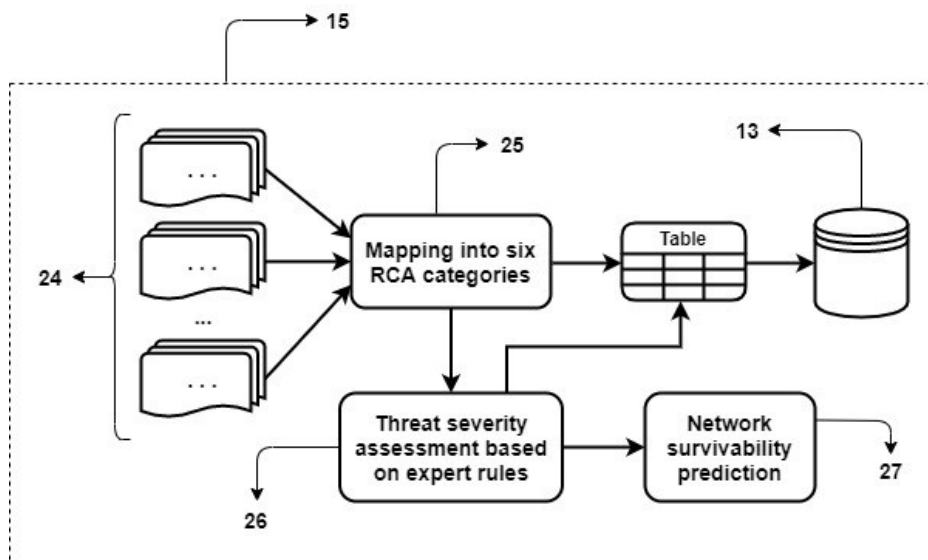
Fig. 5



Hanumanthappa

Dr. J. Hanumanthappa

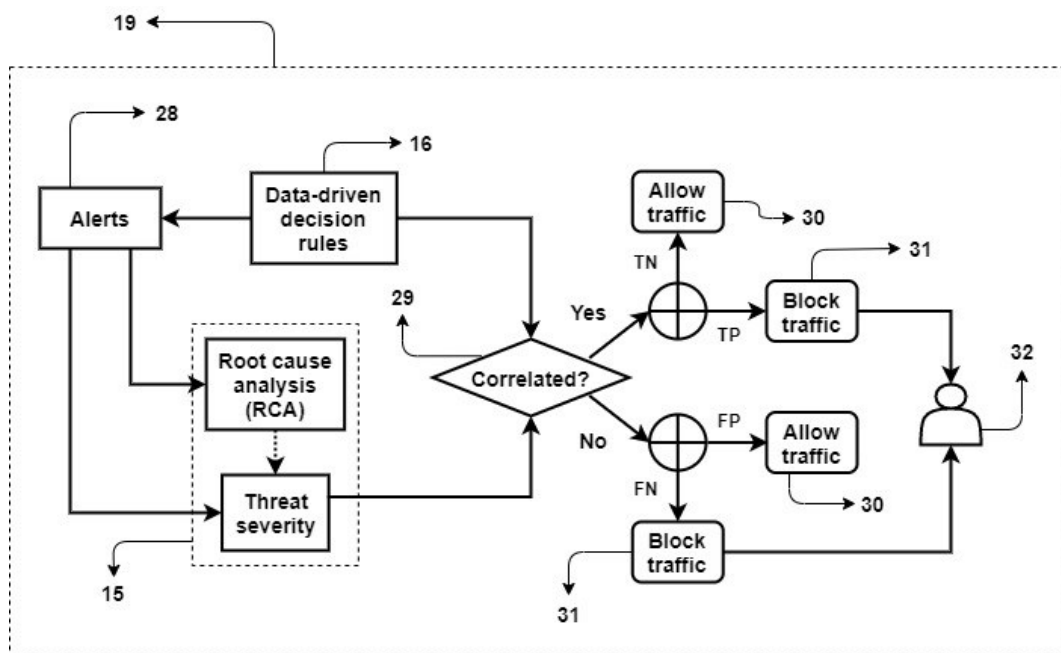
Fig. 6



Hanumanthappa

Dr. J. Hanumanthappa

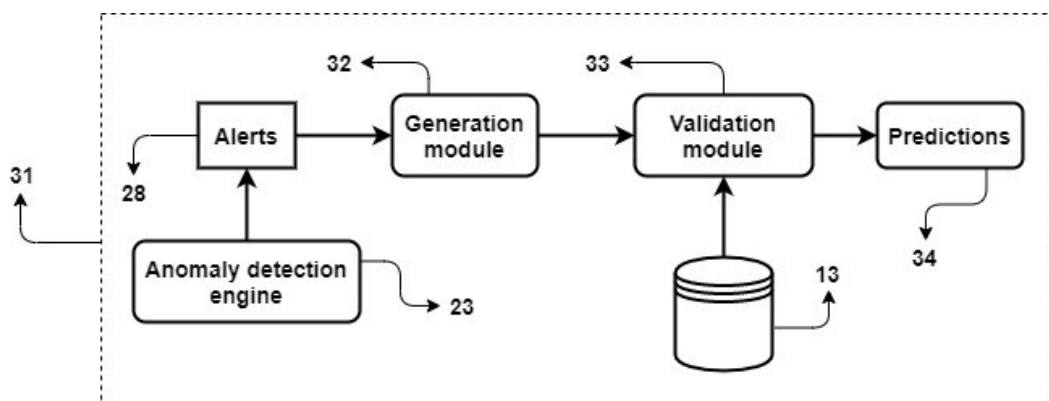
Fig. 7



Hanumanthappa

Dr. J. Hanumanthappa

Fig. 9



Hanumanthappa

Dr. J. Hanumanthappa

FORM - 5
THE PATENTS ACT, 1970
(39 OF 1970)
THE PATENTS RULES, 2003
DECLARATION AS TO INVENTORSHIP
[Section 10(6) and rule 13(6)]

1. NAME OF THE APPLICANTS

- | |
|---------------------------|
| 1. Dr. J. Hanumanthappa |
| 2. Nitish A |
| 3. Dr. S.P. Shiva Prakash |
| 4. Dr. D.S. Vinod |
| 5. Bhavya D |
| 6. Santhosh Kumar K.S |
| 7. Chethan Raj C |
| 8. Mohana S. D |

We hereby declare that the true and first inventors disclosed in the complete specification are:

NAME	Dr. J. Hanumanthappa
NATIONALITY	INDIAN
ADDRESS	Associate Professor, Department of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka, India - 570006.

Dated this 06th Day of January 2021

Hanumanthappa

Dr. J. Hanumanthappa

NAME	Nitish A
NATIONALITY	INDIAN

ADDRESS	Research Scholar, Department of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka, India - 570006.
---------	--

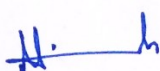
Dated this 06th Day of January 2021



Nitish A

NAME	Dr. S.P. Shiva Prakash
NATIONALITY	INDIAN
ADDRESS	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University, JSS Technical Institution Campus, Mysuru, Karnataka, India – 570006.

Dated this 06th Day of January 2021



Dr. S.P. Shiva Prakash

NAME	Dr. D.S. Vinod
NATIONALITY	INDIAN
ADDRESS	Associate Professor, Dept. of Information Science and Engineering, JSS Science and Technology University, JSS Technical Institution Campus, Mysuru, Karnataka, India – 570006.

Dated this 06th Day of January 2021



Dr. D.S. Vinod

NAME	Bhavya D
NATIONALITY	INDIAN
ADDRESS	Assistant Professor, Department of Computer Science and Engineering, PES College of Engineering, PES Engineering College Rd, PES College Campus, Mandya, Karnataka – 571401.

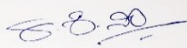
Dated this 06th Day of January 2021

Bhavya D

Bhavya D

NAME	Santhosh Kumar K. S
NATIONALITY	INDIAN
ADDRESS	Research Scholar, Department of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka, India, 570006

Dated this 06th Day of January 2021



Santhosh Kumar K. S

NAME	Chethan Raj C
NATIONALITY	INDIAN
ADDRESS	Associate Professor, Dept. of Computer Science and Engineering, Mysuru Royal Institute of Technology, Palahally village, Laxmi Pura Road, S R Patna-Q, Mandya, Karnataka, India – 571438.


Dated this 06th Day of January 2021



Chethan Raj C

NAME	Mohana S. D
NATIONALITY	INDIAN
ADDRESS	Research Scholar, Dept. of Information Science and Engineering, JSS Science and Technology University, JSS Technical Institution Campus, Mysuru, Karnataka, India – 570006.

Dated this 06th Day of January 2021



Mohana S. D

To

The Controller of Patents

The Patent Office at Chennai.



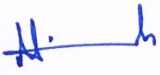
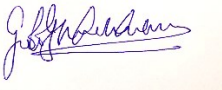
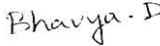
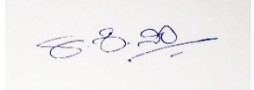

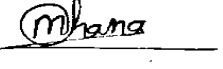
FORM 3
THE PATENTS ACT, 1970
(39 of 1970)
&
The Patents Rules, 2003
STATEMENT AND UNDERTAKING UNDER SECTION 8
(see section 8, rule 12)

1. Name of the Applicants	We, Dr. J. Hanumanthappa, Nitish A, Dr. S.P. Shiva Prakash, Dr. D.S. Vinod, Bhavya D, Santhosh Kumar K.S, Chethan Raj C and Mohana S.D, having our communication address at, Dept. of Studies in Computer Science, University of Mysore, Manasagangothri, Mysuru, Karnataka 570006 (address of the correspondence inventor), hereby declare
2. Name, address and Nationality of Joint applicant	(i) that We have not made any application for the same/substantially the same invention outside India.

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

NIL

Dated this 06th Day of January 2021

 Dr. J. Hanumanthappa	 Nitish A	 Dr. S.P. Shiva Prakash
 Dr. D.S. Vinod	 Bhavya D	 Santhosh Kumar K. S
 Chethan Raj C	 Mohana S. D	

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