Home (http://ipindia.nic.in/index.htm) About Us (http://ipindia.nic.in/about-us.htm) Who's Who (http://ipindia.nic.in/whos-who-page.htm)
Policy & Programs (http://ipindia.nic.in/policy-pages.htm) Achievements (http://ipindia.nic.in/achievements-page.htm)
RTI (http://ipindia.nic.in/right-to-information.htm) Feedback (https://ipindiaonline.gov.in/feedback) Sitemap (shttp://ipindia.nic.in/itemap.htm)
Contact Us (http://ipindia.nic.in/contact-us.htm) Help Line (http://ipindia.nic.in/helpline-page.htm)
Skip to Main Content Screen Reader Access (screen-reader-access.htm)

inPASS
Indian Patent Advanced Search System
(http://ipindia.nic.in/index.htm)
INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS
(http://ipindia.nic

Patent Search

Invention Title	A SYSTEM AND METHOD FOR DETECTING MALICIOUS ACTIVITIES IN COMPUTING NETWORK
Publication Number	23/2020
Publication Date	05/06/2020
Publication Type	INA
Application Number	202021016998
Application Filing Date	20/04/2020
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0029060000, G06F0021550000, G06F0021560000, G08B0021100000, G06F0021570000

Inventor

Name	Address	Country	N
Mr. Ashish Kumar Jain	18 MR-4 Mahalaxmi Nagar, Indore, Madhya Pradesh - 452010	India	I
Mr. Manjeet Kumar Soni	4/6 block no 4 SGSITS staff quarter Y N Road Indore, Madhya Pradesh	India	I
Mr. Chandra Prakash Patidar	CG 1 IET DAVV Campus Khandwa Road Indore	India	I
Mr. Mukul Shukla	Block no.-7, Quarter no.-1, SGSITS Staff Quarter Y.N. Road Indore, Madhya Pradesh - 452003	India	I
Mr. Upendra Singh	1 Rehuta, gram-Rehuta Tehsil – Rampur Baghelan, Dist. Satna, Madhya Pradesh-485001	India	I

Applicant

Name	Address	Country	N
Mr. Ashish Kumar Jain	18 MR-4 Mahalaxmi Nagar, Indore, Madhya Pradesh - 452010	India	I
Mr. Manjeet Kumar Soni	4/6 block no 4 SGSITS staff quarter Y N Road Indore, Madhya Pradesh	India	I
Mr. Chandra Prakash Patidar	CG 1 IET DAVV Campus Khandwa Road Indore	India	I
Mr. Mukul Shukla	Block no.-7, Quarter no.-1, SGSITS Staff Quarter Y.N. Road Indore, Madhya Pradesh - 452003	India	I
Mr. Upendra Singh	1 Rehuta, gram-Rehuta Tehsil – Rampur Baghelan, Dist. Satna, Madhya Pradesh-485001	India	I

Abstract:

A SYSTEM AND METHOD FOR DETECTING MALICIOUS ACTIVITIES IN COMPUTING NETWORK The present invention is a system (100) for detecting malicious activities
computing network (120, 116n). The system (100) comprises one or more data filter modules (102), a security management module (104) and one or more monitorin
(122). The one or more data filter modules (102) is configured to filter incoming and outgoing network data packets and packet's header according to a predetermine
security management module (104) comprises an event tracker module (110), a vulnerabilities test module (106), an event analyzer module (108), an alarm analyzing
(112), an alert manager module (114). The management module (104) is configured to examine and scan the filtered network data packets and packet's header accor
predetermined rule and patterns. The alarm analyzing module (112) is configured to classify alarm and analyze the classified alarm. The alert manager module (114)
to generate one or more malicious activities detecting alert signals and send the detected alert signal to the one or more monitoring modules (122). The one or more
modules (122) is configured to display detected alert signal to one or more users. Figure 1

Complete Specification

Claims:1. A system (100) for detecting malicious activities in a computing network (120, 116n), the system (100) comprising:

one or more data filter modules (102) configured to filter incoming and outgoing network data packets and respective packet header according to a predetermined

a security management module (104) connected to the one or more data filter modules (102), the security management module (104) comprising:

an event tracker module (110) configured to examine the filtered network data packets and respective packet header;

a vulnerabilities test module (106) configured to scan the filtered network data packets and respective packet header;

an event analyzer module (108) operatively connected with the event tracker module (110) and the vulnerabilities test module (106) wherein the event analyzer mo (108) is configured to analyze the network data packets and packet's header patterns and classify the received network data packet and packet's header patterns by event tracker module (110) and vulnerabilities test module (106) according to the predetermined rule and packet's header pattern;

an alarm analyzing module (112) configured to classify an alarm and analyze the classified alarm;

an alert manager module (114) connected to the alarm analyzing module (112), wherein the alert manager module (114) is configured to receive the analyzed alarm generate one or more malicious activities detecting alert signals; and

one or more monitoring modules (122) communicatively connected with the security management module (104) and the computing network (120, 116n), wherein t or more monitoring modules (122) are configured to receive one or more malicious activities detecting alert signals and to display detected alert signal to one or m users.

2. The system (100) as claimed in claim 1, wherein the one or more data filter modules (102) are selected from the group comprising a packet filter, a stateful insp

View Application Status

Department of Industrial Policy and Promotion
Government of India

Terms & conditions (http://ipindia.gov.in/terms-conditions.htm) Privacy Policy (http://ipindia.gov.in/privacy-policy.htm)
Copyright (http://ipindia.gov.in/copyright.htm) Hyperlinking Policy (http://ipindia.gov.in/hyperlinking-policy.htm)
Accessibility (http://ipindia.gov.in/accessibility.htm) Archive (http://ipindia.gov.in/archive.htm) Contact Us (http://ipindia.gov.in/contact-us.htm)
Help (http://ipindia.gov.in/help.htm)