

FORM 2 THE PATENTS ACT, 1970 (39 of 1970) & The Patent Rules, 2003 COMPLETE SPECIFICATION (See sections 10 & rule 13)		
1. TITLE OF THE INVENTION FLAGGING USER HARDWARE BASED ON VIRTUAL PRIVATE NETWORK CONNECTION TIME		
2. APPLICANT (S)		
NAME	NATIONALITY	ADDRESS
VIT-AP University	IN	Inavolu, Amaravati, Andhra Pradesh - 522237, India.
3. PREAMBLE TO THE DESCRIPTION		
COMPLETE SPECIFICATION The following specification particularly describes the invention and the manner in which it is to be performed.		

TECHNICAL FIELD

[0001] The present disclosure relates to the field of network security system. More particularly, the present disclosure relates to a system where a website administrator can decide about giving the appropriate access to a user
5 based on the pre allotted flag or rating for the hardware using proposed algorithms.

BACKGROUND

[0002] Background description includes information that may be useful in
10 understanding the present disclosure. It is not an admission that any of the information provided herein is prior art or relevant to the presently claimed disclosure, or that any publication specifically or implicitly referenced is prior art.

[0003] When a user requests some data from the server, the website can ask for cookies at maximum, from a user and maintain sessions with the same
15 browser. Also, the website can get to know about the geographical location and other interests of the user. This data also depends on the browser but when it comes to the case of a Virtual Private Network (VPN) user all the data is hidden or manipulated by the VPN servers this manipulation includes geographical location, Internet Protocol (IP) address, and other crucial data which is considered
20 by websites to provide suitable data to a user. The crucial information websites banned by a country's government can be accessed by citizens. Also, anonymity on the Internet still exists. Existing models have multiple drawbacks in the case of monitoring the VPN-related traffic and control over VPN usage by user of the Internet.

25 [0004] Many people use virtual private networks (VPN) daily to get around constraints like geographically restricted content, explicitly blocked services, and many other situations. This prompted people to conceal their identity when using a website or any other online service. This will be soon creating uncertainty about the threat to a website or service.

30 [0005] Deploying a system to control VPN usage is, therefore, highly necessary. This issue can be avoided by modifying and implementing one or more

security features generated using VPN usage time and important metrics. The website administrator should decide which data on the website should be accessible to the user based on his/her hardware's rating provided by the model discussed in the current work.

- 5 **[0006]** There is, therefore a need to provide a simple, efficient, reliable, and cost-efficient system and methodology for a better understanding of how users utilize VPNs, and how a website administrator can decide which data on the website should be accessible to the user.

10 **OBJECTS OF THE PRESENT DISCLOSURE**

[0007] It is an object of the present disclosure is to provide a system and methodology for a better understanding of how users utilize VPNs, and how newly proposed algorithms rate hardware of users in the network.

- 15 **[0008]** It is an object of the present disclosure is to provide a simple, efficient, reliable, and cost-efficient system and methodology that can address security issues related with VPN communication.

[0009] Another object of the present disclosure is to provide checking of VPN connection time to rate every user on timed basis for rating the hardware connected.

- 20 **[0010]** Another object of the present disclosure is to identify more dangerous hardware in a network and rating them appropriately to prevent the websites from anonymous attacks.

SUMMARY

- 25 **[0011]** The present disclosure relates to the field of network security system. More particularly, the present disclosure relates to a system where proposed algorithms rate user hardware based on the virtual private network usage time and website administrator can decide about giving the appropriate access to a user based on the pre allotted flag or rating for the hardware using proposed algorithms.
- 30

[0012] In an aspect, the present disclosure is about a system to monitor

and control over virtual private network includes a server in communication with the plurality of devices such that at least one device is held by a user in at least one internet service provider in a network. The server is configured with a plurality of modules, one or more processors operatively coupled with memory
5 storing instructions executable by one or more processors, the one or more processors are configured to request, by the user through a domain name system (DNS) to provide access to a website for procuring data; monitor user by checking their VPN connection time using a first algorithm to work with a second algorithm as per pre-defined instructions; generate a watch list based on the rating
10 of the user group that controls access to a new resource by the user, based at least in part on the domain name for sharing to external servers; evaluate the viability evolution algorithm-rating (VIE-rating) of the user and redirects the user to access appropriate pages of website; restrict by flagging one or more flag that caution user as per user's rating; and connect the user through the at least one route based
15 on categorisation of the user based on VIE rating and flagging instruction.

[0013] In an embodiment, the domain name server (DNS) is application layer protocol for message exchange between user and the server required for the functioning of the Internet and to change domain name into Internet Protocol address number.

20 **[0014]** In an embodiment, the first algorithm is a Rating Algorithm Child (RAC) and the second algorithm is Rating Algorithm Parent (RAP).

[0015] In an embodiment, the RAC is deployed at router topological level, the RAP is deployed in own server with a software client working at internet service provider (ISP), and wherein both working together to make the system
25 robust that identify the threat to the internet.

[0016] In an embodiment, the Rating Algorithm Child (RAC) detects user's connection with the VPN and starts counting the time of connection for the VIE rating.

[0017] In an embodiment, the system rates each user's hardware using
30 virtual private network to make the rating public for website administrators for providing access to websites as per the user's rating.

[0018] In an embodiment, the router and the ISP are not able to read data of the user's activity, but ISP able to know the time connected to the VPN server.

[0019] In an embodiment, the VIE rating is calculated using different values obtained from RAC and previous records and stored by linking the rating
5 to the hardware ID (HWID) of the device used by the user.

[0020] Another aspect of the disclosure is a method for monitoring and controlling over virtual private network including step for requesting, by the user through a domain name system (DNS) to provide access to a website for procuring data; monitoring user by checking their VPN connection time using a
10 first algorithm to work with a second algorithm as per pre-defined instructions; generating a watch list based on the rating of the user group that controls access to a new resource by the user, based at least in part on the domain name for sharing to external servers; evaluating the viability evolution algorithm-rating (VIE-rating) of the user and redirects the user to access appropriate pages of website;
15 restricting by flagging one or more flag that caution user as per user's rating; and connecting the user through wired and wireless based on categorization of the user based on VIE rating and flagging instruction.

[0021] Various objects, features, aspects, and advantages of the inventive subject matter will become more apparent from the following detailed description
20 of preferred embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF DRAWINGS

[0022] The accompanying drawings are included to provide a further
25 understanding of the present disclosure and are incorporated in, and constitute a part of this specification. The drawings illustrate exemplary embodiments of the present disclosure, and together with the description, serve to explain the principles of the present disclosure.

[0023] In the figures, similar components, and/or features may have the
30 same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that

distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

5 **[0024]** FIG. 1 illustrates an exemplary block diagram depicting network representation of the system, in accordance with an embodiment of the present disclosure.

10 **[0025]** FIG. 2 illustrates an exemplary scale of zones presentation for VIE-rating in the system, in accordance with an embodiment of the present disclosure

[0026] FIG. 3 illustrates an exemplary flow chart for VIE-rating, in accordance with an embodiment of the present disclosure.

15 **[0027]** FIG. 4 illustrates an exemplary screen shot for the network used for brick-level experiment, in accordance with an embodiment of the present disclosure.

[0028] FIG. 5 illustrates an exemplary screen shot for DNS mapping, in accordance with an embodiment of the present disclosure.

[0029] FIG. 6 illustrates an exemplary screen shot for simulated network depicted for CISCO Packet Tracer.

20 **[0030]** FIG. 7A illustrates an exemplary screen shot depicting home page flagging, in accordance with an embodiment of the present disclosure.

[0031] FIG. 7B illustrates an exemplary screen shot depicting full access flagging to a user, in accordance with an embodiment of the present disclosure.

25 **[0032]** FIG. 7C illustrates an exemplary screen shot depicting partial access flagging, in accordance with an embodiment of the present disclosure.

[0033] FIG. 7D illustrates an exemplary screen shot depicting flagging for no access except for advertisements and announcements, in accordance with an embodiment of the present disclosure.

30 **[0034]** FIG. 8 illustrates an exemplary method flow diagram, in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0035] The following is a detailed description of embodiments of the disclosure depicted in the accompanying drawings. The embodiments are in such detail as to clearly communicate the disclosure. However, the amount of detail
5 offered is not intended to limit the anticipated variations of embodiments. On the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit, and scope of the present disclosure as defined by the appended claims.

[0036] In the following description, numerous specific details are set forth
10 in order to provide a thorough understanding of the embodiments of the present invention. It will be apparent to one skilled in the art that embodiments of the present invention may be practiced without some of these specific details. Embodiments of this disclosure relate to a system and method for testing port vulnerability, which is secured and incorporates an effective mechanism for web
15 crawlers.

[0037] Embodiment of the present disclosure relate to the field of network security system. More particularly, the present disclosure relates to a system where a proposed algorithms RAP, RAC rate hardware connected to the network and website administrator can decide for a user by raising appropriate flag while
20 accessing websites using virtual private network communication.

[0038] In an embodiment, the present disclosure discloses a system and method to monitor and control over virtual private network includes a server in communication with the plurality of devices, at least one internet service provider in a network to restrict by flagging devices as per user's rating. A Rating
25 Algorithm Child and a Rating Algorithm Parent is deployed at router topological level and internet service provider respectively, to make the system robust that identify the threat to the internet. The Rating Algorithm Child detects user's connection with the VPN and starts counting the time of connection for the VIE rating which is calculated using different values obtained from Rating Algorithm
30 Child and previous records of the user. The obtained VIE rating made public for website administrators for controlling user's hardware access to websites.

[0039] Referring to FIG. 1 where an exemplary block diagram depicting network representation of the system 100 is shown. The system 100 to monitor and control over virtual private network includes a server 102 in communication with the plurality of devices 104 such that at least one device 104 is held by a user in at least one internet service provider 106 in a network 120.

[0040] In an embodiment, the system 100 provides a better understanding of the users utilize VPNs and rates users based on VPN usage time and other important metrics. Also, the website administrator can decide which data on the website 114 should be accessible to the user based on his/her hardware rating provided by the system.

[0041] In an embodiment, the server 102 is configured with a plurality of modules, one or more processors operatively coupled with memory storing instructions executable by one or more processors. When a user requests some data from the server 102, the website 114 can ask for cookies at maximum, from a user and maintain sessions with the same browser. Also, the website 114 can get to know about the geographical location and other interests of the user. This data also depends on the browser but when it comes to the case of a Virtual Private Network (VPN) user all the data is hidden or manipulated by the VPN servers. This manipulation includes geographical location, Internet Protocol (IP) address, and other crucial data which is considered by websites 114 to provide suitable data to a user.

[0042] In an embodiment, system 100 has two algorithms; one is Rating Algorithm Child (RAC) 110, which is a fixed length code of 1 octet and identifies a routing area within a location area. RAC Monitors users very closely by checking their VPN Connection Time (VCT) and deployed at router topological level. Second is Rating Algorithm Parent (RAP) 116 is a protocol that deals with device directions to send them from ISP 106 to LAN 112. It works like a map for devices 104 with an internet and helping them find their way. The RAC 110 is deployed at router topological level and RAP 116 is deployed in our own server 102 but has a software client working at Internet Service Provider (ISP) 106. RAP 116 is deployed in server 102 with a software client working at internet service

provider (ISP) 106. RAP116 works with server 102 which query data from RAC 110 and work as per pre-defined instructions. Both of these together make the system 100 robust enough to identify the threat to the Internet.

5 **[0043]** In an embodiment, the domain name system (DNS) is an application layer protocol for message exchange between user and the server 102 required for the functioning of the Internet 120 and to change domain name into Internet Protocol address number.

10 **[0044]** In an embodiment, the RAC 110 detects user's connection with the VPN and starts counting the time of connection for the VIE rating server 108. The system 100 rates each user using virtual private network to rate, to make the rating public for website administrators for providing access to websites 114 as per the user's rating by flagging user's device 104 as per the user's rating.

15 **[0045]** In an embodiment, the Viability Evolution algorithm consist of defining viability boundaries, creating an initial population, and repetitively applying reproduction, elimination, and boundary updates until the boundaries meet the desire values. Viability boundaries are expressed as inequalities on the problem objectives and define the characteristics of the desired solutions. The lower and upper bounds of the viability conditions are initially set to encompass all individuals, and are gradually modified during evolution to approximate the
20 desired value.

25 **[0046]** furthermore, all the viability boundaries are modified simultaneously so that at least a fraction on individuals defined as users are described from the population. After each boundary update, boundaries are not modified until the population generates a number of viable individuals equal to at least the number of eliminated individuals. As soon as the condition is satisfied, the viability boundaries are updated again and this process is repeated until the target value is reached. Once the boundaries are converged to the desired values, the algorithm returns the final population solutions to the user. The rating is obtained from RAC 110 and previous records and stored by linking the rating to
30 the hardware ID (HWID) of the device 104 used by the user.

[0047] In an embodiment, the user might have connection to the ISP 106

by selecting any network 120 including Wi-Fi/modem/router through one or more hope or directly to the ISP 106. The router and the ISP 106 are not able to read data of the user's activity, but able to know the time connected to the VPN server. The system 100 will rate every user who uses VPN and Rating is made public for website admins to access and let know what kind of user is accessing their website 114. They can restrict or block as per the user's rating. Users will be connected to either a router or directly to the ISP based on that we can categorize users into two cases. Connected through WIFI/modem/router as a case-I, or as an intermediate hope and directly connected to ISP as case-II. The system 100 takes Hardware ID (HWID) such as Media Access Control Address (MAC ID) as an element to recognize particular hardware. This helps proposed algorithm recognize a particular device in both cases of connections. RAC 110 is deployed at multiple levels for different cases. In case I, it is deployed the rating algorithm at WIFI/modem/router and ISP or intermediate hop for case II. This algorithm maintains a Table-1 that has all the data related to the device connected to the deployed hop.

Table-I

S.No.	Device Number	Display Name	Internal IP Address	HWID	Weekly VPN Time
1	Internal123	Mobile1	192.168.1.1	xx-xx-xx-xx-xx-x1	2.2 hours
2	Internal124	TV1	192.168.1.2	xx-xx-xx-xx-xx-x2	7.8 hours
3	Internal125	LAP1	192.168.1.3	xx-xx-xx-xx-xx-x3	18.2hours

[0048] In an embodiment, while connecting a device to WIFI/modem/router in case1 or hop in case2, ISP and Router level devices cannot read the data of a user's activity when connected to a VPN but can know the time connected to the VPN server. As per the existing algorithms once the VPN connection is detected RAC starts counting the time of connection. This VPN time is summed up to a week and then added to the table. The RAC 110 deployed

at desired hop will collect the information as mentioned in Table-1 given above. It has the HWID of each device connected to the WIFI/modem/router, Internal IP address, and weekly VPN time. We can use VPN detection algorithms for the calculation of VCT. Total time of VPN connection in a week gives VCT.

5 **[0049]** FIG. 2 illustrates an exemplary scale of zones presentation 200 for VIE-rating in the system 100. The zones are divided into a Green zone (G1 to G3), Blue zones (B1 to B3) and Red zones (R1 to R10) depending upon degree of restricted and used while flagging.

[0050] In an embodiment, RAP 116 is deployed at ISP 106. RAP 116 calculates the user rating with the predefined algorithm. RAP 116 is linked to the table created by the RAC 110. RAP 116 acquires necessary information from RAC 110. This is deployed in our servers to avoid user interference in changing VPN connection time (VCT) and other metrics. All the available entities at RAP 116 are shown Table-2 given below. The zone of a user based on the VIE-Rating
15 of the user is also suggested by the system 100.

Table-2

S. NO.	PUBLIC IP	DEVICE ID	HWID QUERIED FROM RAC	VCT QUERIED FROM RAC	VIE-RATING	ZONE
1	172.xx.xx.1	DEVICE1	xx-xx-xx-xx-xx-x1	2.2	2.9	GREEN2
2	172.xx.xx.2	DEVICE2	xx-xx-xx-xx-xx-x2	3.4	3.9	GREEN3
3	172.xx.xx.3	DEVICE3	xx-xx-xx-xx-xx-x3	7.8	7.1	BLUE3
4	172.xx.xx.3	DEVICE4	xx-xx-xx-xx-xx-x4	18.2	18.1	RED7

[0051] FIG. 3 illustrates an exemplary flow chart 300 for VIE-rating. VIE rating is calculated using different values obtained from RAC 110 and previous records. The consideration of multiple values for the calculation of the VIE-Rating includes the VCT of the current week and the VIE-ratings of three previous weeks. Considering the previous week's ratings in the calculation of the
20

VIE-Rating will help to rate the individual more accurately and analyze the user's time on VPN.

[0052] In an embodiment, VCT for the new user 302 for the current week is calculated at RAC 110 and will be shared with RAP 116. Now RAP 116 has
5 access to the current week's VCT and the last three week's VIE-Rating termed as prev1, prev 2, and prev 3 respectively. For a new user joining the algorithm values of VCT, prev1, prev2, and prev3 are 7, 7, 7, 7 respectively as represented in step 306.

[0053] In an embodiment, VCT for the current week is calculated at RAC
10 and will be shared with RAP. Now RAP has access to the current week's VCT and the last three week's VIE-Rating termed as prev1, prev 2, and prev 3 respectively. For a new user joining the algorithm values of VCT, prev1, prev2, and prev3 are 7, 7, 7, 7 respectively. New users will be in the blue3 zone. As soon
15 as a new user starts using VPN, VIE-Rating will start altering as per the VIE-rating algorithm 308. After calculating the VIE-Rating for every user based on the above-mentioned constraints, VIE rating is linked to the HWID of the device. All HWIDs with the corresponding VIE-Rating are stored in a table on our servers. Linking the VIE-Rating to HWID helps the VIE-Rating to remain constant even
20 when the user changes the public IP Address through different means like IP spoofing, change in ISP, and other means. After calculating the VIE-Rating, the same scale of zones can be used for checking the ambiguity of the user being a hacker. In an embodiment the algorithm I for the current week will be as under-

```
Start
If new user THEN
25     VCT=7
        Prev1=7
        Prev2=7
        Prev3=7
ELSE
30     VCT= RAC(VCT)
        Prev1=records (Prev1)
```

Prev1=records (Prev2)
Prev1=records (Prev3)
END IF
Average of VCT, Prev1, Prev2, Prev3

5 END

[0054] In an embodiment, a user can move forward in the scale of zones as shown in Algorithm 2 placed below. In Algorithm 2, Demonstrated VCT is current week's VPN Connection Time, PREV1 is last week's VIE RATING, PREV2 is before last week's VIE RATING, PREV3 is a week before last week's

10 VIE RATING. As the user is lowering, the use of VPN TIME the user can move ahead on the scale of zones and get access to new features of websites compared to the last week.

VCT = 6.1
Prev1 = 8.2 = Red1
Prev2 = 7.3 = Blue3
Prev3 = 9.2 = Red2
Rating for this week = (VCT + Prev1 + Prev2 + Prev3)/4
= 7.7 = Blue3

[0055] In an embodiment, a user can move backward in the scale of zones as shown below in Algorithm 3. In Algorithm 3, Demonstrated VCT is current week's VPN Connection Time, PREV1 is last week's VIE RATING, PREV2 is before last week's VIE RATING, PREV3 is a week before last week's VIE RATING. As the user is using more VPN Time the user can move backwards on the scale of zones and lose some features of websites compared to the last week.

25 VCT = 11.2
Prev1 = 8.2 = Red1
Prev2 = 8.3 = Red1
Prev3 = 8.4 = Red1
Rating for this week = (VCT + Prev1 + Prev2 + Prev3)/4
= 8.525 = Red2

30 **[0056]** In an embodiment, a user can stay constant in the scale of zones as

shown below in Algorithm 4. In Algorithm 4, Demonstrated VCT is current week's VPN Connection Time, PREV1 is last week's VIE RATING, PREV2 is before last week's VIE RATING, PREV3 is a week before last week's VIE RATING. As the user is maintaining constant VPN Time the user stays constant on the scale of zones and has no change in features of websites compared to the last week.

5 VCT = 8.2
 Prev1 = 8.2 = Red1
 Prev2 = 8.3 = Red1
 10 Prev3 = 8.4 = Red1
 Rating for this week = (VCT + Prev1 + Prev2 + Prev3)/4 = 8.275 = Red1

[0057] In an embodiment, if a user doesn't use the VPN for a few weeks and achieves the VIE-Rating zero then the user can be ranked GREEN1 to avoid this problem add the average of the previous ratings instead of zero in case of zero VPN usage. The same is shown below in Algorithm 5. In Algorithm 5, VCT is zero or a sudden drop in VCT is noticed. This can happen in many cases like the hardware is not used for a week. To avoid this situation Previously calculated VIE-Rating is maintained till there is an alteration in the current rating.

20 VCT = 0 = 8(Average of previously taken VIE-Rating)
 Prev1 = 8.2 = Red1
 Prev2 = 8.3 = Red1
 Prev3 = 8.4 = Red1
 Rating for this week = (VCT + Prev1 + Prev2 + Prev3)/4 = 8.225
 25 = Red1

[0058] FIG. 4 illustrates an exemplary screen shot for the network used for brick-level experiment 400. When an experiment consists of 4 different client devices 104 connected to form a single network 120 that mirrors a real-life situation is carried out, all the device's computers, switches, routers, and servers are configured to simulate the situation in the real world. After successful calculation of the VIE-Rating, this is stored by linking the rating to the HWID of

every individual device 104. When the user sends a request to access the website 114, the rating will be attached to the request at ISP 106 and sent to the website m114 (if requested). Then the website administrator can decide on the data that can be shared with the user as per the rating assigned to the device (HWID). The website's administrator can decide the access that can be given to the corresponding user. The access alteration can be done by the website administrator.

[0059] FIG. 5 illustrates an exemplary screen shot 500 for DNS mapping. Once DNS is perfectly configured, web server is designed and added to the network 120 with the necessary configurations. This has the home page of the domain "vielabs.com" with all the pre-written code using the vie-rating of the device. This server has a website home page, once the user accesses the home page website evaluates the VIE-rating of the user and redirects the user to the appropriate access level holding pages. Here web server has multiple web pages including ads.html which has only ads and announcements, full.html which has full features of the website, and partial.html which has partial features of the website.

[0060] FIG. 6 illustrates an exemplary screen shot for simulated network depicted for CISCO Packet Tracer 600. An experiment is carried out using CISCO PACKET TRACER 8.2.1. The network of the experiment consists of 4 different client devices connected to form a single network that mirrors a real-life situation. All the device's computers 104, switches, routers, and server 102 are configured to simulate the situation in the real world. A sample website with the domain name "vielabs.com" is created and linked with "123.0.0.3"

[0061] In an embodiment, the server 102 has a website home page, once the user accesses the home page website evaluates the VIE-rating of the user and redirects the user to the appropriate access level holding pages. Here webserver has multiple web pages including ads.html which has only ads and announcements, full.html which has full features of the website, and partial.html which has partial features of the website.

[0062] In an embodiment, here in this experiment, a VIE-rating server is

added to provide and store the VIE-rating and HWID of corresponding devices connected. A data packet with VIE-rating is passed to web Server, and then the website admin has a pre-written code on their website which can redirect their users as per VIE-rating to appropriate access leveled pages. As a part of the experiment carried out, there are only three outcomes as classified according to the inputs of this brick-level experiment.

[0063] In an embodiment, when the VIE-rating of PC1 is set to 3 and falls in the green zone as per the Scale of zones, the device will get access to the whole page without any restriction. When the VIE-rating of PC2 is set to 6 and falls in the blue zone as per the Scale of zones, the device will get access to partial access to the website, and when the VIE-rating of PC3 is set to 20 and falls in the red zone as per the Scale of zones the device will get access to a ads/announcements-only page.

[0064] FIG. 7A, 7B, 7C, and 7D illustrates an exemplary screen shot depicting home page 702-1, full access flagging 702-2, partial access flagging 702-3, and flagging for no access except for advertisements and announcements 702-4 to a user, respectively.

[0065] In an embodiment, when the experiment is carried out using CISCO PACKET TRACER 8.2.1. The network of the experiment consists of 4 different client devices connected to form a single network that mirrors a real-life situation. All the device's computers, switches, routers, and servers are configured to simulate the situation in the real world. Initially home page 702-1 is displayed, and when the VIE-rating of PC1 is set to 3 and falls in the green zone as per the Scale of zones, the device will get access to the whole page without any restriction and the screen 702-2 will be displayed . When the VIE-rating of PC2 is set to 6 and falls in the blue zone as per the Scale of zones, the device will get partial access depicting screen 702-3 to the website 114, and when the VIE-rating of PC3 is set to 20 and falls in the red zone as per the Scale of zones showing screen as 702-4 indicating that the device 104 will get access to a ads/announcements-only page.

[0066] FIG. 8 illustrates an exemplary method flow diagram 800. The

method 800 for monitoring and controlling over virtual private network including step 802 for requesting, by the user through a domain name system to provide access to a website 114 for procuring data, and step 804 for monitoring user by checking their VPN connection time using a first algorithm to work with a second
5 algorithm as per pre-defined instructions.

[0067] In an embodiment, according to step 806, generating a watch list based on the rating of the user group that controls access to a new resource by the user, based at least in part on the domain name for sharing to external servers, and step 808 for evaluating the viability evolution algorithm-rating (VIE-rating) of the
10 user and redirects the user to access appropriate pages of website.

[0068] In an embodiment, as per step 810, the method 800 restricting by flagging one or more flag that caution user as per user's rating, step 812 for connecting the user through the at least one route based on categorization of the user based on VIE rating and flagging instruction.

15 **[0069]** The main goal of system 100 is to monitor and control the VPN network communication where the website administrator can decide for a user by raising appropriate flag while accessing websites 104 using virtual private network communication.

[0070] Those skilled in the art would also appreciate that as the proposed
20 system can be used as a multi-country model and 'N' numbers of devices 104 can be flagged. Also, as the requirements of large system infrastructure at multi-places are avoided making the system 100 is simple, cost-effective, and easily implementable. System 100 operates with a plurality of devices 104 like a smart mobile, desktop, laptop, television, and personal digital assistant.

25 **[0071]** Moreover, in interpreting the specification, all terms should be interpreted in the broadest possible manner consistent with the context. In particular, the terms "comprises" and "comprising" should be interpreted as referring to elements, components, or steps in a non-exclusive manner, indicating that the referenced elements, components, or steps may be present, or utilized, or
30 combined with other elements, components, or steps that are not expressly referenced. Where the specification claims refer to at least one of something

selected from the group consisting of A, B, C....and N, the text should be interpreted as requiring only one element from the group, not A plus N, or B plus N, etc.

5 [0072] While the foregoing describes various embodiments of the invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof. The scope of the invention is determined by the claims that follow. The invention is not limited to the described embodiments, versions or examples, which are comprised to enable a person having ordinary skill in the art to make and use the invention when combined with
10 information and knowledge available to the person having ordinary skill in the art.

ADVANTAGES OF THE INVENTION

[0073] Some of the advantages of the present disclosure, which at least one embodiment herein satisfy are as listed herein below.

15 [0074] The present disclosure provides a simple, efficient, reliable, and cost-efficient system and methodology that can rate and categorize hardware devices like smart mobile, personal computer, laptop, television etc. using their VIE-Rating.

[0075] The present disclosure solves the problem of increasing anonymity
20 caused by over use of virtual private networks or proxies.

[0076] The present disclosure provides a solution to website administrators to get to know the possibility of threat from their user.

[0077] The present disclosure helps national security in finding more threat possible networks and isolate them in tough times.

25

We Claim:

1. A system (100) to monitor and control over virtual private network, the system (100) comprising:
 - 5 a server (102) in communication with the plurality of devices (104), wherein at least one device (104) is held by a user in at least one internet service provider (106) in a network (120), wherein the server (102) is configured with a plurality of modules, one or more processors operatively coupled with memory storing instructions executable by one or more processors, the one or more processors are configured to:
 - 10 request, by the user through a domain name system (108) to provide access to a website for procuring data;
monitor user by checking their VPN connection time using a first algorithm (110) to work with a second algorithm (116) as per pre-defined instructions;
 - 15 generate a watch list based on the rating of the user group that controls access to a new resource by the user, based at least in part on the domain name for sharing to external servers;
evaluate the viability evolution algorithm-rating (VIE-rating) (308) of the user and redirects the user to access appropriate pages of website (114);
 - 20 restrict by flagging one or more flag (702) that caution user as per user's rating; and
connect the user through wired and wireless based on categorisation of the user based on VIE rating (308) and flagging instruction.
2. The system as claimed in claim 1, wherein the domain name system (DNS) (108) is application layer protocol for message exchange between user and the server (102) required for the functioning of the Internet (120) and to change domain name into Internet Protocol address number.
3. The system as claimed in claim 1, wherein the first algorithm (110) is a

Rating Algorithm Child (RAC) and the second algorithm (116) is Rating Algorithm Parent (RAP).

4. The system as claimed in claim 3, wherein the RAC (110) is deployed at router topological level, the RAP (116) is deployed in own server (102) with
5 a software client working at internet service provider (ISP) (106), and wherein both working together to make the system (100) robust that identify the threat to the internet (120).
5. The system as claimed in claim 4, wherein the Rating Algorithm Child (RAC) (110) detects user's connection with the VPN and starts counting the
10 time of connection for the VIE rating (308).
6. The system as claimed in claim 1, wherein the system (100) rates user's hardware using virtual private network to make the rating public for website administrators for providing access to websites (114) as per the user's rating.
- 15 7. The system as claimed in claim 1, wherein the router and the ISP (106) are not able to read data of the user's activity, but internet service provider (ISP) able to know the time connected to the VPN server.
8. The system as claimed in claim 1, wherein the VIE rating (308) is calculated using different values obtained from RAC (110) and previous records and
20 stored by linking the rating to the hardware ID (HWID) of the device (104) used by the user.
9. A method (800) for monitoring and controlling over virtual private network, the method (800) comprising steps for:
 requesting, by the user through a domain name system (DNS) (108)
25 to provide access to a website for procuring data;
 monitoring user by checking their VPN connection time using a first algorithm (110) to work with a second algorithm as per pre-defined instructions;
 generating a watch list based on the rating of the user group that
30 controls access to a new resource by the user, based at least in part on the domain name for sharing to external servers;

evaluating the viability evolution algorithm-rating (VIE-rating) (308) of the user and redirects the user to access appropriate pages of website (114);

5 restricting by flagging one or more flag (702) that caution user as per user's rating; and

connecting the user through the at least one route based on categorisation of the user based on VIE rating (308) and flagging instruction.

For VIT-AP University



10

Tarun Khurana
Regd. Patent Agent [IN/PA-1325]
Dated: 19th October, 2023

ABSTRACT

FLAGGING USER HARDWARE BASED ON VIRTUAL PRIVATE NETWORK CONNECTION TIME

5 A system 100 and method to monitor and control over virtual private network includes a server 102 in communication with the plurality of devices 104, at least one internet service provider 106 in a network 120 to restrict by flagging devices 104 as per user's rating. A Rating Algorithm Child 110 and a Rating Algorithm Parent 116 is deployed at router topological level and our own servers with client
10 at ISP topological level, to make the system 100 robust that identify the threat to the internet 120. The Rating Algorithm Child 110 detects user's connection with the VPN and starts counting the time of connection for the VIE rating which is calculated using different values obtained from RAC 110 and previous records of the user. The system 100 rates each hardware using virtual private network and
15 the rating made public for website administrators for providing access to websites 114 using appropriate flags and VIE-rating provided on user's device 104.

100

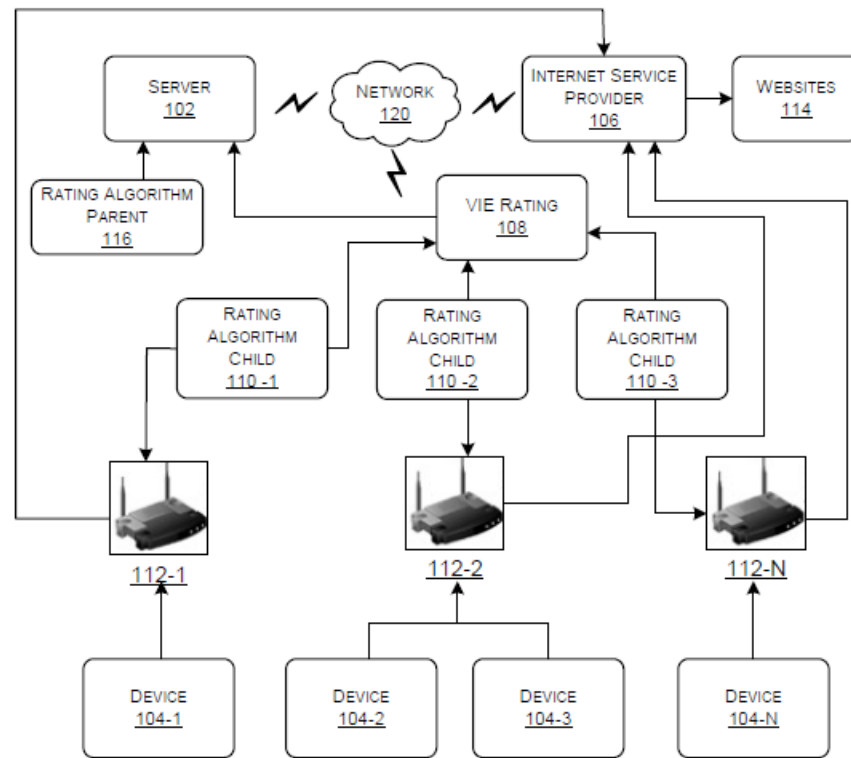


FIG. 1