WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

# DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|---|---|---|
| International application number: | | **PCT/US2022/050579** |
| International filing date: | | **21 November 2022 (21.11.2022)** |
| Document type: | | **Certified copy of priority document** |
| Document details: | Country/Office: | **US** |
| | Number: | **63/281,978** |
| | Filing date: | **22 November 2021 (22.11.2021)** |
| Date of receipt at the International Bureau: | | **22 December 2022 (22.12.2022)** |

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

1239469

# THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

*December 21, 2022*

**THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.**

**APPLICATION NUMBER:** *63/281,978*
**FILING DATE:** *November 22, 2021*
**RELATED PCT APPLICATION NUMBER:** *PCT/US22/50579*

**THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS** *US63/281,978*

Certified by

Performing the Functions and Duties of the
Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

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

PTO/AIA/82A (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

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

| | |
|---|---|
| Application Number | Not yet assigned |
| Filing Date | Herewith |
| First Named Inventor | Simon David Lincoln Fellows |
| Title | CYBER SECURITY TOOLS TO PROTECT A SYSTEM |
| Art Unit | Not yet assigned |
| Examiner Name | Not yet assigned |
| Attorney Docket Number | 034306-0014PRO |

**SIGNATURE of Applicant or Patent Practitioner**

| | | | |
|---|---|---|---|
| Signature | /Thomas S. Ferrill/ | Date (Optional) | November 22, 2021 |
| Name | Thomas S. Ferrill | Registration Number | 42,532 |
| Title (if Applicant is a juristic entity) | | | |
| Applicant Name (if Applicant is a juristic entity) | | | |

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

☐ *Total of _____ forms are submitted.

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

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

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

PTO/AIA/82B (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

# POWER OF ATTORNEY BY APPLICANT

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

| Application Number | Filing Date |
|---|---|
| | |

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

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 34284

OR

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

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

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

| | | | | | |
|---|---|---|---|---|---|
| ☐ Firm or Individual Name | Rutan and Tucker, LLP | | | | |
| Address | 18575 Jamboree Road, 9th Floor | | | | |
| City | Irvine | State | CA | Zip | 92612 |
| Country | | | | | |
| Telephone | | Email | | | |

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

☐ Inventor or Joint Inventor (title not required below)

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

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

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

**SIGNATURE of Applicant for Patent**

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

| | | | |
|---|---|---|---|
| Signature | /xxxxxxx/ | Date | 2.2. Oct 2018 |
| Name | Steve Chamberlain | | |
| Title | Chief Operating Officer of Darktrace Holdings Limited | | |

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

☐ Total of forms are submitted.

PTO/SB/16 (10-20)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


# PROVISIONAL APPLICATION FOR PATENT COVER SHEET -- Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

**Priority Mail Express® Label No.** _____

| INVENTOR(S) | | |
|---|---|---|
| Given Name (first and middle [if any]) | Family Name or Surname | Residence (City and either State or Foreign Country) |
| Simon David Lincoln | Fellows | Cambridge, UK |
| Jack | Pearson | Northumberland, UK |
| Matthew | Dunn | Ely, UK |
| Jack Benjamin | Stockdale | Cambridge, UK |
| | | |

Additional inventors are being named on the _____ separately numbered sheets attached hereto.

**TITLE OF THE INVENTION (500 characters max):**

CYBER SECURITY TOOLS TO PROTECT A SYSTEM

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☑ The address corresponding to Customer Number: 34284

**OR**

☐ Firm or Individual Name

Address

| City | State | Zip |
|---|---|---|
| Country | Telephone | Email |

**ENCLOSED APPLICATION PARTS (*check all that apply*)**

☒ Application Data Sheet. See 37 CFR 1.76.
☐ CD(s), Number of CDs _____
☐ Drawing(s) *Number of Sheets* _____
☐ Other (specify) _____
☑ Specification (e.g., description of the invention) *Number of Pages* 41

**Fees Due:** Filing Fee of $300 ($150 for small entity) ($75 for micro entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $420 ($210 for small entity) ($105 for micro entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

**METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT**

☐ Applicant asserts small entity status. See 37 CFR 1.27.
☐ Applicant certifies micro entity status. See 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
☐ A check or money order made payable to the *Director of the United States Patent and Trademark Office* is enclosed to cover the filing fee and application size fee (if applicable).
☐ Payment by credit card. Form PTO-2038 is attached.
☑ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: 50-2191

300.00
**TOTAL FEE AMOUNT ($)**

***USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT***

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 10 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/16 (10-20)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


# PROVISIONAL APPLICATION FOR PATENT COVER SHEET -- Page 2 of 2

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government. (NOTE: Providing this information on a provisional cover sheet, such as this Provisional Application for Patent Cover Sheet (Form PTO/SB/16), does not satisfy the requirement of 35 U.S.C. 202(c)(6), which requires that the *specification* contain a statement specifying that the invention was made with Government support and that the Government has certain rights in the invention.)

☑ No.

☐ Yes, the invention was made by an agency of the U.S. Government. The U.S. Government agency name is:

_____

☐ Yes, the invention was made under a contract with an agency of the U.S. Government.

The contract number is: _____

The U.S. Government agency name is: _____

_____

In accordance with 35 U.S.C. 202(c)(6) and 37 CFR 401.14(f)(4), the specifications of any United States patent applications and any patent issuing thereon covering the invention, including the enclosed provisional application, must state the following:

"This invention was made with government support under [IDENTIFY THE CONTRACT] awarded by [IDENTIFY THE FEDERAL AGENCY]. The government has certain rights in the invention."

## WARNING:

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

SIGNATURE /Thomas S. Ferrill/ DATE 2021-11-22

TYPED OR PRINTED NAME Thomas S. Ferrill REGISTRATION NO. 42,532 (*if appropriate*)

TELEPHONE 650-320-1500 DOCKET NUMBER 034306-0014PRO

| Given Name (first and middle [if any]) | Family Name or Surname | Residence (City and either State or Foreign Country) |
|---|---|---|
| Fraser | Greenlee | Cambridge, UK |
| Andres Curto | Martin | Cambridge, UK |
| Timothy Owen | Bazalgette | Knebworth, UK |
| Matthew | Dunn | Ely, UK |
| Jack Benjamin | Stockdale | Cambridge, UK |

# Electronic Acknowledgement Receipt

| | |
|---|---|
| **EFS ID:** | 44344059 |
| **Application Number:** | 63281978 |
| **International Application Number:** | |
| **Confirmation Number:** | 1065 |
| **Title of Invention:** | CYBER SECURITY TOOLS TO PROTECT A SYSTEM |
| **First Named Inventor/Applicant Name:** | Simon David Lincoln Fellows |
| **Customer Number:** | 34284 |
| **Filer:** | Thomas Ferrill/Matthew Kwak |
| **Filer Authorized By:** | Thomas Ferrill |
| **Attorney Docket Number:** | 034306-0014PRO |
| **Receipt Date:** | 22-NOV-2021 |
| **Filing Date:** | |
| **Time Stamp:** | 16:38:34 |
| **Application Type:** | Provisional |

## Payment information:

| | |
|---|---|
| Submitted with Payment | yes |
| Payment Type | DA |
| Payment was successfully received in RAM | $300 |
| RAM confirmation Number | E2021ALG38533723 |
| Deposit Account | 502191 |
| Authorized User | Matthew Kwak |
| The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:<br>37 CFR 1.16 (National application filing, search, and examination fees)<br>37 CFR 1.17 (Patent application and reexamination processing fees) | |

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

## File Listing:

| Document Number | Document Description | File Name | File Size(Bytes)/ Message Digest | Multi Part /.zip | Pages (if appl.) |
|---|---|---|---|---|---|
| 1 | | 0014PRO_Application.pdf | 871651<br>750e06fff194b74eb51eb76aef8773cbadafbf03 | yes | 41 |
| | **Multipart Description/PDF files in .zip description** | | | | |
| | **Document Description** | | **Start** | **End** | |
| | Specification | | 1 | 40 | |
| | Claims | | 41 | 41 | |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 2 | Application Data Sheet | 034306_0014PRO_ADS_V1.pdf | 115757<br>0c66794c80c4d79e53a0ba32691d10e816d63dc3 | no | 9 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| This is not an USPTO supplied ADS fillable form | | | | | |
| 3 | Power of Attorney | 034306_0014PRO_POA_V1.pdf | 299940<br>ac8cf0e136709d46ef5f40abed8bcca720b17cdd | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 4 | Provisional Cover Sheet (SB16) | 034306-0014PRO_ProvisionalCoverSheet_V1.pdf | 167794<br>0014a33f84c8f526ba3aca7e4ab31cefaf7204b1 | no | 3 |
| **Warnings:** | | | | | |
| This is not a USPTO supplied Provisional Cover Sheet SB16 form. | | | | | |
| **Information:** | | | | | |
| 5 | Fee Worksheet (SB06) | fee-info.pdf | 37573<br>ff96884c762fe92421e946f39755535bbb1beb00 | no | 2 |

| Warnings: | |
|---|---|
| Information: | |
| Total Files Size (in bytes): | 1492715 |

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PROVISIONAL PATENT APPLICATION

FOR

# CYBER SECURITY TOOLS TO PROTECT A SYSTEM

SIMON FELLOWS, JACK PEARSON, MATTHEW DUNN, AND JACK STOCKDALE

PREPARED BY

RUTAN & TUCKER, LLP

18575 JAMBOREE ROAD

9TH FLOOR

IRVINE, CA 92612

(650) 320-1500

ATTORNEY DOCKET NO.: 034306-0014PRO

## NOTICE OF COPYRIGHT



## FIELD

[0002] Embodiments of the design provided herein generally relate to a cyber threat defense system. In an embodiment, Artificial Intelligence is applied to analyzing Cyber Security threats.

## BACKGROUND

[0003] Existing methods such as vulnerability scanning performed by humans are less targeted and may lead to security resource allocation in the wrong places. Also, some vulnerability scanners actually test and compromise the actual network devices themselves, which may adversely affect the network during this testing and scanning.

[0004] Cyber threat protection systems generally ingest network data to detect cyber threats but not to assess how a cyber threat might spread through a network. A human Red team of cyber security professionals typically is hired to test a network's vulnerability to cyber-attacks.

## DRAWINGS

[0005] The drawings refer to some embodiments of the design provided herein in.

[0006] While the design is subject to various modifications, equivalents, and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and will now be described in detail. It should be understood that the design is not limited to the particular embodiments disclosed, but – on the contrary – the intention is to cover all modifications, equivalents, and alternative forms using the specific embodiments.

## DESCRIPTION

[0007] In the following description, numerous specific details are set forth, such as examples of specific data signals, named components, number of servers in a system, etc., in order to provide a thorough understanding of the present design. It will be apparent, however, to one of ordinary skill in the art that the present design can be practiced without these specific details. In other instances, well known components or methods have not been described in detail but rather in a block diagram in order to avoid unnecessarily obscuring the present design. Further, specific numeric references such as a first server, can be made. However, the specific numeric reference should not be interpreted as a literal sequential order but rather interpreted that the first server is different than a second server. Thus, the specific details set forth are merely exemplary. Also, the features implemented in one embodiment may be implemented in another embodiment where logically possible. The specific details can be varied from and still be contemplated to be within the spirit and scope of the present design. The term coupled is defined as meaning connected either directly to the component or indirectly to the component through another component.

[0008] The Artificial Intelligence based cyber security appliance can utilize a number of tools such as example tools: 1) a telecomms immune system to protect a telecom system from a cyber threat; 2) A cyber security self-healing system to restore the protected system back to a state before a compromise (e.g. abnormalities started) by a cyber threat occurred to the protected system; and 3) many other tools herein.

A telecomms immune system to protect a telecom system from a cyber threat

[0009] The telecomms immune system to protect a telecom system from a cyber threat is configured to use machine learning approaches to protect telecom industries from cyber threats. The telecomms immune system is configured to use device behaviour modelling specialized to that type of device's behaviour. The telecomms immune system is configured to use device behaviour modelling for these telecom specific AI models, logic models, and other machine learning approaches, specializing in telecoms protocols and processes. The telecomms immune system can use, for example, Bayesian techniques to establish a pattern of life feature for the nodes of the telecom system with telecom devices and a quite different pattern of life from traditional TCP/IP network systems.

[0010] The telecomms immune system can detect for cyber threats (e.g. malicious actors) that are trying to 1) take over the control system for the telecom infrastructure, 2) merely degrade the telecom infrastructure via, for example, interfering with/disrupting the transmission of the data within the system, and/or 3) spy/collect data on the telecom infrastructure.

[0011] The AI of the telecomms immune system is configured and trained to understand specifically to view the "control plane" of the telecom system rather than "user plane" data. This means the AI is configured and trained to understand how the provider controls user data movements rather than monitoring the user data itself. The telecomms immune system performs several processes including supplying user interfaces, machine learning on telecom device types to be modelled, other machine learning approaches to understand what is benign and normal behaviour and what is abnormal, as well as other processes.

[0012] The AI of the telecomms immune system is configured and trained to understand and protect existing 4G infrastructures (e.g. broadband cellular network technology). In an embodiment, the AI of the telecomms immune system is configured and trained to understand and protect 5G infrastructures. The AI of the telecomms immune system is configured and trained to understand each of the devices in the telecom infrastructure as well as the different protocols being processed in the respective 4G and/or 5G infrastructure. The AI of the telecomms immune system is configured and trained to understand telecoms transport protocols, such as Stream Control Transmission Protocol (SCTP). SCTP can be an example computer networking communications protocol in the transport layer of the Internet Protocol Suite. The SIGTRAN family and related protocols are another telecoms application protocols that the AI is trained to understand. The SIGTRAN family includes specifications for a family of protocols that provide reliable datagram service and user layer adaptations for Signalling System and ISDN communications protocols. Extension to telecoms processes are also telecoms application protocols that the AI is trained to understand.

Telecoms authentication protocols are another extension to the telecoms application protocols that the AI is trained to understand, such as Diameter. The AI of the telecomms immune system is configured and trained to understand each of the specific metrics for telecoms activities. The AI of the telecomms immune system is configured and trained to understand an operation of each of the Specific device types. The telecomms immune system can have specific model decks.

[0013] The modules of the telecomms immune system can be configured to work with a set of agents external to the cyber security appliance housing the telecomms immune system. For example, an agent can be coded to be able to handle Kubernetes pod deployments into 3rd-party owned hyperscale cloud. Kubernetes like Docker is an open-source container-orchestration system for automating computer application deployment, scaling, and management. The pods are monitored whenever they get deployed by including an agent (basically csensor) either as part of the telco's container itself or as a sidecar container deployed within the same pod.

[0014] Another agent can be configured to reside in and monitor a central services directory.

[0015] The agents can exist in various parts of the telecoms system to provide more narrowly focused / surgical autonomous responses to contain the disruption, via UI, and programmable acceptable autonomous responses selected by the user. The agents can control the networking capabilities of the particle container that the agent is installed on.

A cyber security self-healing system to restore the protected system back to a state before a compromise by a cyber threat occurred to the protected system

[0016] The cyber security self-healing system to restore the protected system can identify and respond to a cyber threat, take actions to remediate a cyber threat, and restore the protected system back to a state before a compromise by a cyber threat occurred to the protected system.

[0017] The cyber security self-healing system to restore the protected system can use 1) an AI tracking mechanism, such as modelling a normal pattern of life, for each entity in the protected system, 2) an AI mechanism trained to identify the malicious actor/device/file causing the abnormal/malicious behavior, 3) an AI mechanism trained on how to regulate communications, and 4) an AI mechanism trained on how to isolate the compromised device, as well as taking measures to entities with a direct nexus to the compromised device. For example, the cyber security self-healing system to restore the protected system can use AI Analyst incident modelling to map and identify an entire lifecycle of attack, work with the AI models trained on cyber security threats in the cyber security Darktrace appliance to identify a source of the cyber-attack, and recommend restore points and/or where in the protected system remediation action is needed.

[0018] The cyber security self-healing system to restore the protected system can "use AI self-learning algorithms and pattern of life analysis of the protected system (EIS data) to continually know the state of everything to be able to heal the protected system

back to a heathy state with the minimum number of changes to achieve that goal, and with a minimum disruption to legitimate on-going operations.

[0019] The cyber security self-healing system to restore the protected system can use AI Analyst with external data input (e.g., crowdstrike) to identify an infected patient zero and additional devices actually compromised and/or directly linked to devices actually compromised in need of remediation. The linked devices or the activity may not be directly visible to the cyber security Darktrace appliance. The cyber security self-healing system to restore the protected system can potentially use the external data input that the system is receiving from third party integrations (e.g., from host based agents from 3rd party vendors, antivirus and based testing antivirus, etc. to identify patient zero of the attack, identify, where the attack has happened and is happening, identify devices that the system reasonably believes are linked to the compromised entity, and recommend remediation or perform remediation via AI alone, and/or AI in combination with human assistance.

[0020] The cyber security self-healing system to restore the protected system can use AI Analyst incident modelling to identify risky individuals, behaviors, or endpoints (metaphorically, match that always starts the fire) that should be restricted internally whether through process or software policy.

[0021] A cyber security self-healing system can restore the protected system back to a state before a compromise (e.g. abnormalities started) by a cyber threat occurred to the protected system.

[0022] The cyber security self-healing system to restore the protected system can also apply self-healing to in progress attacks – so heal in real time, as an attack happens, rather than after an attack has taken place. Self-healing that the cyber security self-healing system to restore the protected system applies is a next step beyond its other function of restricting the user or the device to its normal pattern of activity. The autonomous response module of the cyber security self-healing system to restore the protected system can take an action to only allow actions that are within that entities normal pattern of that activity. However, the AI in the cyber security self-healing system to restore the protected system is going and trying to isolate other devices around a compromised entity as well as identify the malicious entity – (file/process/actor) as the source causing the abnormal activity, as well as trying to figure out how to heal and remediate from that cyber-attack to get the system back to a state before the attack began.

[0023] The cyber security self-healing system can take various example restoration actions in real time. The cyber security self-healing system to restore the protected system can use historic SaaS/IaaS resource access, privilege information and clustered similar users to reset user access and permissions after a privilege escalation incident. Next, the cyber security self-healing system to restore the protected system can use historic IaaS data on virtual resource usage to identify errant virtual resources and spin down those resources or disable overactive microservices like lambdas. AWS Lambda can be a server less compute service for running code without having to provision or manage servers. Next, the cyber security self-healing system to restore the protected system can use historic IaaS data on virtual resource usage to understand

when a client is undergoing some kind of DDOS and recommend scaling to handle the load until the overload is over. Part of the self-healing can recommend scaling when the system understands deliberate overloading of traffic is occurring and then bringing that scaling back down again so assisting their service architectures to deal with situations when some cyber threat is trying to overload those systems to bring that customer down.

[0024] Next, the cyber security self-healing system to restore the protected system can use historic source codebase information and modelling from cyber security Darktrace appliance for development to revert commits and code changes that potentially introduce bad or compromised code. The cyber security self-healing system to restore the protected system can use profiling data on process behavior seen by Antigena Endpoint/cSensors to decide to remove an executable across a fleet of devices (and/or invoke a 3rd party's API to do so). The cyber security self-healing system to restore the protected system can also use historic records of a source code database information to find out when during the development of a product that the cyber-attack occurred on the source code in order to restore the source code back to the state before the compromise occurred, as well as use historic code base analysis and understanding to identify supply chain and products vulnerable to bad code / compromised code and sending an update package / at least a notice to revert those products and further prevent the source code vulnerabilities from trickling down the supply chains from the vendor to the end user. Once file data of a cyber threat is identified, then that file data and its characteristics are captured in an inoculation package and then cascade that file information to network cyber security system, SaaS

cyber security system, host based system, etc., and quarantine the identical and very similar files in order to remove them from all of the environments before anything can spread even more than it has via immediate remediation and using also the system's own inoculation data.

[0025] Next, the cyber security self-healing system to restore the protected system can use AI driven Red Team to identify risk profiles of users and subsequently create pre-emptive training material based upon the security mistakes they make. The cyber security self-healing system to restore the protected system can look at people's/user's historic behavior, using, for example, Antigena email, and use our email and machine learning awareness of people's behavior to see what risky behavior they've performed, e.g. have a look at what sorts of dodgy links does this person open, do they open emails from complete strangers, are they credential re-users across different platforms, and recommend actual education to prevent this risky behavior in the future by remediating that bad behavior they currently have. The cyber security self-healing system to restore the protected system can use historic Antigena Email data (such as clicking on dodgy links/opening mail from rare recipients) to create pre-emptive training material to prevent users from being tricked in the same way. The cyber security self-healing system to restore the protected system will report the instigators of any kind of anomalous activity; and therefore, the system recommends that you sort of review your processes and restrict these endpoint devices and/or these individuals.

[0026] In essence, the cyber security self-healing system to restore the protected system has the capabilities to isolate and/or control parts of the network that the system suspects could be infected from those parts are clean, while remediation work can be

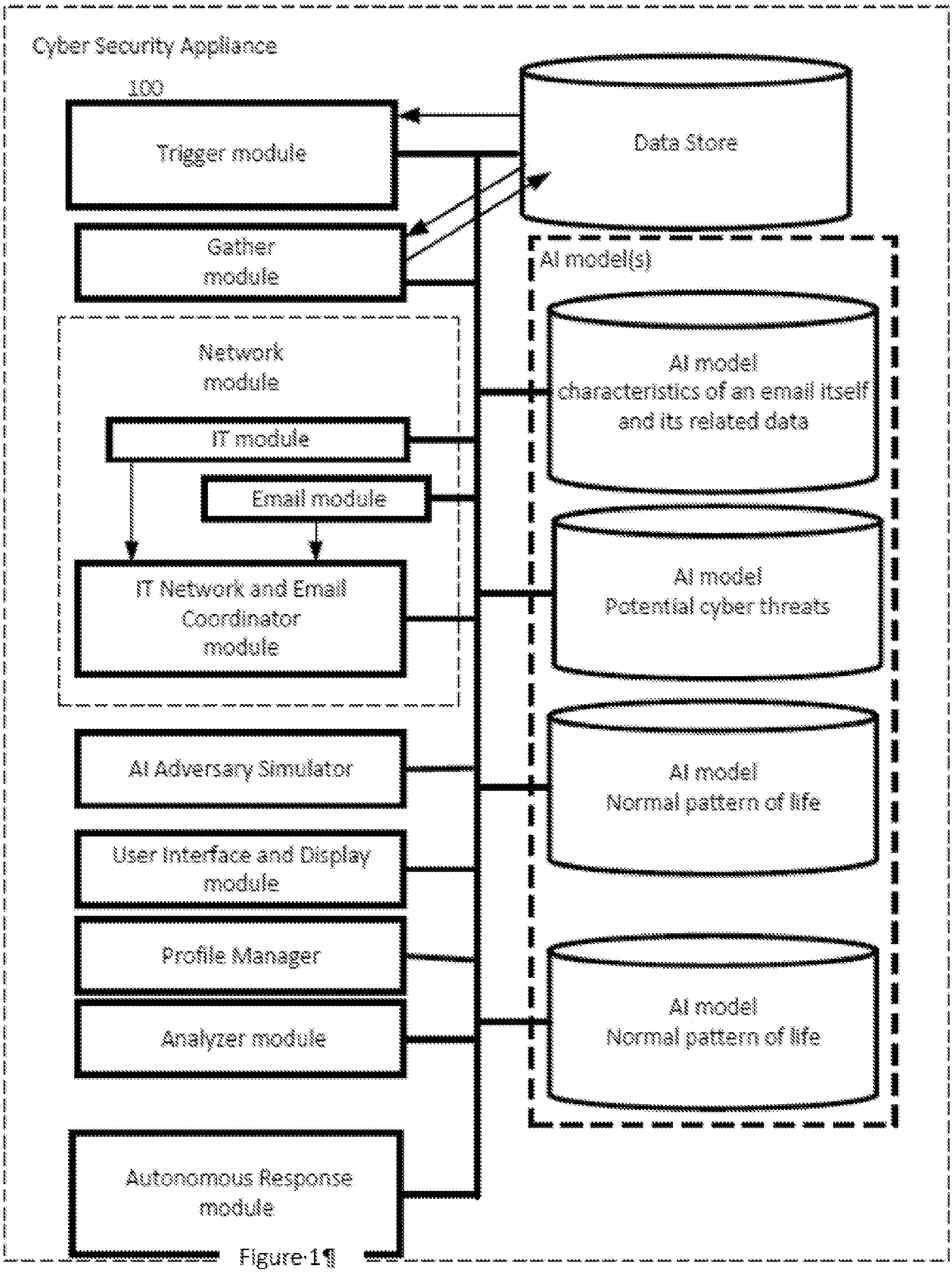
performed. The system can stop a device that is infected from connecting to other nodes. In addition, the system can restrict reading and writing traffic to restrict traffic movement and process activity to nodes close to an entity that the system thinks is performing erroneously or infected. The cyber security self-healing system to restore the protected system uses the historic knowledge of connectivity (e.g., industrial control systems (ICS) READ COMMANDS) to create continuity to these other nodes if a device with an established behavior pattern goes down / behaving anomalously, in order to prevent the attack from growing and or spreading. Thus, in an example, control those related nodes in such a way that the infected node can't talk to those nodes. The system will control these other nodes/entities, perform surgical actions on that device that we believe is infected to heal it back to an original state prior to the compromise and not allow the cyber-attack to spread any further.

[0027] An AI red team and the predictive modelling cooperate to assist in the detection, and then the remediation response and healing that are all part of one continuous loop system where components in the cyber security system communicate and share information with each other. The cyber security self-healing system to restore the protected system can use an autonomous response module / Antigena Network and/or Endpoint agent to restrict traffic movement and process activity in nodes close to a potential patient zero using an AI driven Red Team attack path modelling. The cyber security self-healing system to restore the protected system can suggest high priority routes of traversal that any attacks would take via/from AI driven Red Team so that customers can kind of concentrate their efforts on backups and physical mediums to use for remediation. The cyber security self-healing system to restore the protected

system can use an autonomous response module / Antigena Network and/or Endpoint agent in real time to cut off sections of the network environment that are known-infected until they can be restored. In addition, the cyber security self-healing system to restore the protected system can use AI driven Red Team modelling to recommend and deploy honeypots around known infectious environments to direct malicious actor energy there whilst cutting off "real" resources. The honeypot can be a computer or computer system intended to mimic likely targets of cyberattacks. The deployed honeypots can be used to detect attacks or deflect them from a legitimate target. The system uses its understanding of network connectivity, historic network connectivity, machine learning awareness, and cyber-attack modelling, in order to deploy the system's own honey pots to areas that the system believes are currently infectious to draw malicious acts or activity and allow the system to implement its auto response capabilities to prevent the cyber threat from going anywhere other than those honey pots, whilst that remediation action can be performed on that to the patient zero.

[0028] The cyber security self-healing system to restore the protected system can use file data seen in Antigena Email (AI based email protection) to identify new files entering the network, then quarantining and remediating those files in SaaS platforms/on hosts.

[0029] The cyber security self-healing system to restore the protected system can use recommend restoration points where remediation should be performed across the entire life cycle of a cyber incident.


Cyber Security Appliance
100
Trigger module
Data Store
Gather module
AI model(s)
Network module
AI model characteristics of an email itself and its related data
IT module
Email module
AI model Potential cyber threats
IT Network and Email Coordinator module
AI Adversary Simulator
AI model Normal pattern of life
User Interface and Display module
Profile Manager
Analyzer module
AI model Normal pattern of life
Autonomous Response module

Figure·1¶

Example cyber security appliance

[0030] Again, Figure 1 shows some modules of an example cyber security appliance 100. Various Artificial Intelligence models and modules of a cyber security appliance 100 cooperate to protect a system, including but not limited to an email network, from cyber threats. The cyber security appliance 100 may include a trigger module, a gatherer module, an analyser module, an assessment module, a formatting module, an autonomous report composer, a data store, one or more Artificial Intelligence models trained on potential cyber threats and their characteristics, symptoms, remediations, etc., one or more Artificial Intelligence models trained with machine learning on a normal pattern of life for entities in the network, one or more Artificial Intelligence models trained with machine learning on threat report generation, and multiple libraries of text and visual representations to cooperate the library of page templates to populate visual representations, such as graphs, and text on the pages of the threat report. An example network of an email system will be used to illustrate portions of a cyber security appliance 100.

[0031] Referring to Figure 1, the trigger module may detect time stamped data indicating an event is occurring and then triggers that something unusual is happening. The gatherer module is triggered by specific events or alerts of i) an abnormal behaviour, ii) a suspicious activity, and iii) any combination of both. The trigger module may identify, with one or more AI models trained with machine learning on a normal email pattern of life for entities in the email network, at least one of i) an abnormal

behaviour, ii) a suspicious activity, and iii) any combination of both, from one or more entities in the system.

[0032] The inline data may be gathered on the deployment when the traffic is observed. The gatherer module may initiate a collection of data to support or refute each of the one or more possible cyber threat hypotheses that could include this abnormal behaviour or suspicious activity by the one or more AI models trained on possible cyber threats. The gatherer module cooperates with a data store. The data store stores comprehensive logs for network traffic observed. These logs can be filtered with complex logical queries and each IP packet can be interrogated on a vast number of metrics in the network information stored in the data store.

[0033] The data store can store the metrics and previous threat alerts associated with network traffic for a period of time, which is, by default, at least 27 days. This corpus of data is fully searchable. The cyber security appliance 100 works with network probes to monitor network traffic and store and record the data and meta data associated with the network traffic in the data store. Figure 2 illustrates an example cyber security appliance 100 using an intelligent-adversary simulator cooperating with a network module and network probes ingesting traffic data for network devices and network users in the network under analysis.

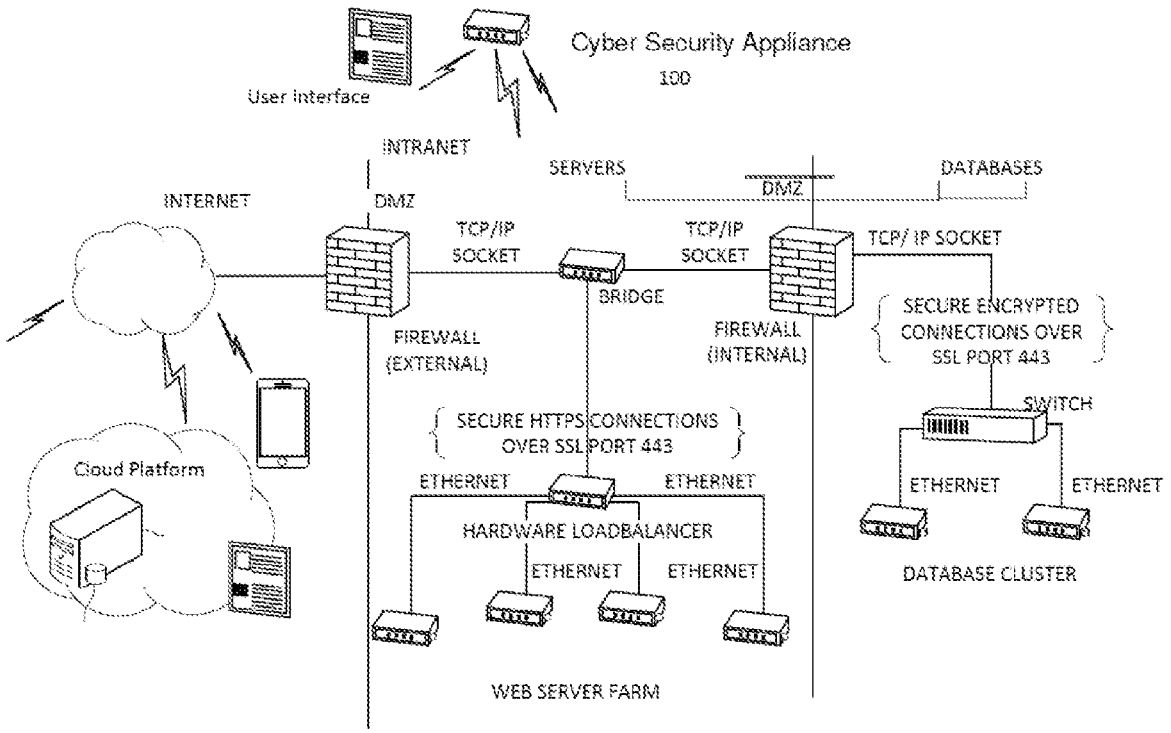



Figure 2

[0034] Referring back to Figure 1, the gatherer module may consist of multiple automatic data gatherers that each look at different aspects of the data depending on the particular hypothesis formed for the analysed event. The data relevant to each type of possible hypothesis can be automatically pulled from additional external and internal sources. Some data is pulled or retrieved by the gatherer module for each possible hypothesis.

[0035] The gatherer module may further extract data, at the request of the analyser module, on each possible hypothetical threat that would include the abnormal behaviour or suspicious activity; and then, filter that collection of data down to relevant points of data to either 1) support or 2) refute each particular hypothesis of what the potential cyber threat, e.g. the suspicious activity and/or abnormal behaviour, relates to. The gatherer module and the data store can cooperate to store an inbound and

outbound email flow, network traffic, log files, SaaS and cloud data, etc. received over a period of time as well as autonomous actions performed by the autonomous response module on that data. The gatherer module may send the filtered down relevant points of data to either 1) support or 2) refute each particular hypothesis to the analyser module, comprised of one or more algorithms used by the AI models trained with machine learning on possible cyber threats to make a determination on a probable likelihood of whether that particular hypothesis is supported or refuted.

[0036] A feedback loop of cooperation between the gatherer module and the analyser module may be used to apply one or more models trained on different aspects of this process.

[0037] The analyser module can form one or more hypotheses on what are a possible set of activities including cyber threats that could include the identified abnormal behaviour and/or suspicious activity from the trigger module with one or more AI models trained with machine learning on possible cyber threats. The analyser module may request further data from the gatherer module to perform this analysis. The analyser module can cooperate with the one or more Artificial Intelligence models trained with machine learning on the normal pattern of life for entities in the system/network under analysis to detect anomalous behaviour which is detected as outside the usual pattern of life for each entity, such as a user, of the system/network. The analyser module can cooperate with the Artificial Intelligence models trained on potential cyber threats to detect, for example, suspicious emails that exhibit traits that may suggest a malicious intent, such as phishing links, scam language, sent from suspicious domains, etc. In addition, the gatherer module and the analyser module may

use a set of scripts to extract data on each possible hypothetical threat to supply to the analyser module. The gatherer module and analyser module may use a plurality of scripts to walk through a step-by-step process of what to collect to filter down to the relevant data points (from the potentially millions of data points occurring in the network) to make a decision what is required by the analyser module.

[0038] The analyser module may further analyse a collection of system data, including metrics data, to support or refute each of the one or more possible cyber threat hypotheses that could include the identified abnormal behaviour and/or suspicious activity data with the one or more AI models trained with machine learning on possible cyber threats. The analyser module then generates at least one or more supported possible cyber threat hypotheses from the possible set of cyber threat hypotheses as well as could include some hypotheses that were not supported/refuted.

[0039] The analyser module may get threat information from Open Source APIs as well as from databases as well as information trained into AI models. Also, probes collect the user activity and the email activity and then feed that activity to the network module to draw an understanding of the email activity and user activity in the email system.

[0040] The analyser module learns how expert humans tackle investigations into specific cyber threats. The analyser module may use i) one or more AI models and/or ii) rules-based models and iii) combinations of both that are hosted within the plug-in appliance connecting to the network.

[0041] The AI models use data sources, such as simulations, database records, and actual monitoring of different human exemplar cases, as input to train the AI model

on how to make a decision. The analyser module also may utilize repetitive feedback, as time goes on, for the AI models trained with machine learning on possible cyber threats via reviewing a subsequent resulting analysis of the supported possible cyber threat hypothesis and supply that information to the training of the AI models trained with machine learning on possible cyber threats in order to reinforce the model's finding as correct or inaccurate.

[0042] Each hypothesis has various supporting points of data and other metrics associated with that possible threat, and a machine learning algorithm will look at the relevant points of data to support or refute that particular hypothesis of what the suspicious activity and/or abnormal behaviour relates to.

[0043] The analyser module may perform analysis of internal and external data including readout from machine learning models, which output a likelihood of the suspicious activity and/or abnormal behaviour related for each hypothesis on what the suspicious activity and/or abnormal behaviour relates to with other supporting data to support or refute that hypothesis.

[0044] The assessment module may assign a probability, or confidence level, of a given cyber threat hypothesis that is supported, and a threat level posed by that cyber threat hypothesis, which includes this abnormal behaviour or suspicious activity, with the one or more AI models trained on possible cyber threats. The assessment module can cooperate with the autonomous response module to determine an appropriate response to mitigate various cyber-attacks that could be occurring.

[0045] The analyser module can reference machine learning models that are trained on the normal behaviour of email activity and user activity associated with at

least the email system, where the analyser module cooperates with the assessment module to determine a threat risk parameter that factors in 'the likelihood that a chain of one or more unusual behaviours of the email activity and user activity under analysis fall outside of derived normal benign behaviour;' and thus, are likely malicious behaviour.

[0046] The autonomous response module, rather than a human taking an action, is configured to cause one or more actions to be taken to contain a detected cyber threat when a cyber-threat risk score is indicative of a likelihood of a cyber-threat is equal to or above an actionable threshold. A cyber threat module (which can be part of the analyser module) is configured to generate the cyber-threat risk score based on the analysis of the potential cyber threats on the end-point computing-device in light of the collected pattern of life data that deviates from the normal pattern of life for that end-point computing-device. The autonomous response module is configured to cooperate with the cyber threat module to cause the one or more actions to be taken to contain the detected cyber threat when the cyber-threat risk score is indicative of the likelihood of the cyber-threat is equal to or above the actionable threshold, which is configured to improve the computing-device being protected by this system by limiting an impact of the cyber threat from consuming unauthorized CPU cycles by the one or more processors, memory space in the one or more memories, and power consumption in the computing-device via responding to the cyber threat without waiting for some human intervention.

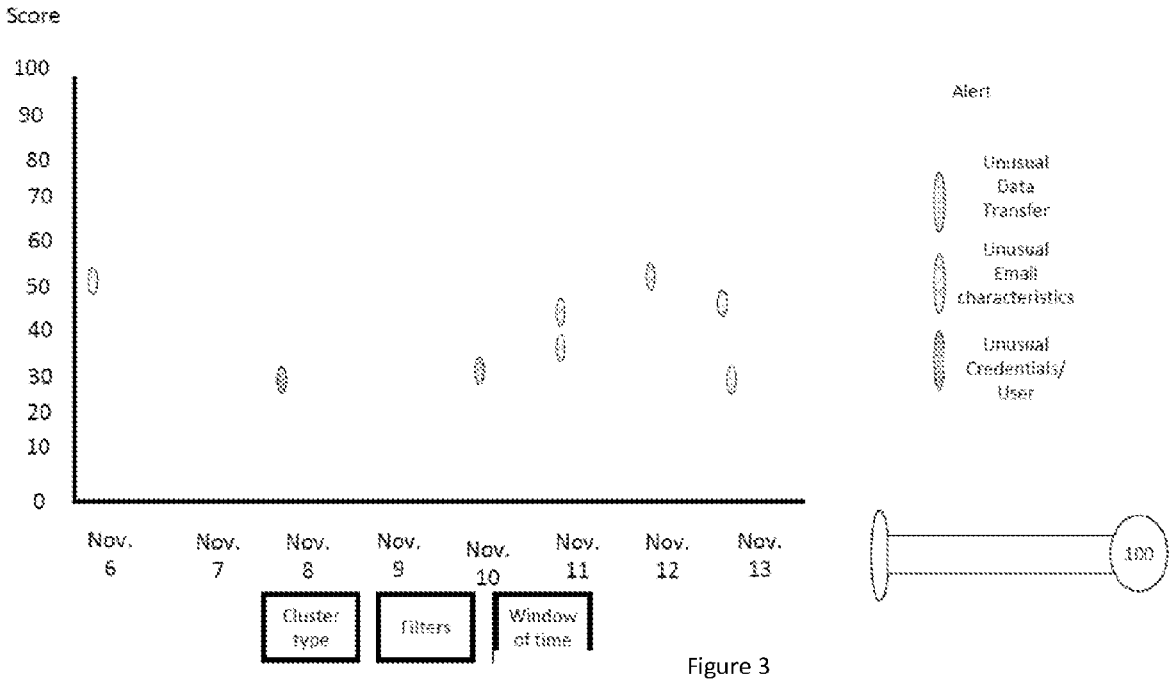



Figure 3

[0047] In an example, a behavioural pattern analysis of what are the unusual behaviours of the network/system/device/user under analysis by the machine learning models may be as follows. The cyber security appliance uses unusual behaviour deviating from the normal behaviour and then builds a chain of unusual behaviour and the causal links between the chain of unusual behaviour to detect cyber threats (for example see Figure 3). Figure 3 illustrates a block diagram of an embodiment of an example chain of unusual behaviour for the email(s) deviating from a normal pattern of life in connection with the rest of the network under analysis. The unusual pattern can be determined by filtering out what activities/events/alerts that fall within the window of what is the normal pattern of life for that network/system/device/user under analysis, and then the pattern of the behaviour of the activities/events/alerts that are left, after the filtering, can be analysed to determine whether that pattern is indicative of a behaviour of a malicious actor – human, program, or other threat. Next, the cyber security

appliance can go back and pull in some of the filtered out normal activities to help support or refute a possible hypothesis of whether that pattern is indicative of a behaviour of a malicious actor. The analyser module can cooperate with one or more models trained on cyber threats and their behaviour to try to determine if a potential cyber threat is causing these unusual behaviours. If the pattern of behaviours under analysis is believed to be indicative of a malicious actor, then a score of how confident is the system in this assessment of identifying whether the unusual pattern was caused by a malicious actor is created. Next, also assigned is a threat level score or probability indicative of what level of threat does this malicious actor pose. Lastly, the cyber security appliance is configurable in a user interface, by a user, enabling what type of automatic response actions, if any, the cyber security appliance may take when different types of cyber threats, indicated by the pattern of behaviours under analysis, that are equal to or above a configurable level of threat posed by this malicious actor.

[0048] The AI models may perform by the threat detection through a probabilistic change in a normal behaviour through the application of an unsupervised Bayesian mathematical model to detect behavioural change in computers and computer networks. The core threat detection system is termed the 'Bayesian probabilistic'. The Bayesian probabilistic approach can determine periodicity in multiple time series data and identify changes across single and multiple time series data for the purpose of anomalous behaviour detection. From the email and potentially IT network raw sources of data, a large number of metrics can be derived each producing time series data for the given metric.

[0049] The detectors in the analyser module including its network module

(simulator can get extract meta data from network module) and email module components can be discrete mathematical models that implement a specific mathematical method against different sets of variables with the target. Thus, each model is specifically targeted on the pattern of life of alerts and/or events coming from, for example, i) that cyber security analysis tool analysing various aspects of the emails, iii) coming from specific devices and/or users within a system, etc.

[0050] At its core, the cyber security appliance 100 mathematically characterizes what constitutes 'normal' behaviour in line with the normal pattern of life for that entity and organization based on the analysis of a large number/set of different measures of a device's network behaviour. The cyber security appliance 100 can build a sophisticated 'pattern of life' – that understands what represents normality for every person, device, email activity, and network activity in the system being protected by the cyber security appliance 100.

[0051] The assessment module may rank supported candidate cyber threat hypotheses by a combination of likelihood that this candidate cyber threat hypothesis is supported as well as a severity threat level of this incident type.

[0052] The formatting module can be coded to generate the report with the identified critical devices connecting to the virtualized instance of the network that should have the priority to allocate security resources to them, along with one or more portions of the constructed graph (See Figure 2). The formatting module can have an autonomous email-report composer that cooperates with the various AI models and modules of the cyber security appliance 100 as well as at least a set of one or more libraries of sets of prewritten text and visual representations to populate on templates of

pages in the email threat report. The autonomous email-report composer can compose an email threat report on cyber threats that is composed in a human-readable format with natural language prose, terminology, and level of detail on the cyber threats aimed at a target audience being able to understand the terminology and the detail. The modules and AI models cooperate with the autonomous email-report composer to indicate in the email threat report, for example, an email attack's 1) purpose and/or 2) targeted group (such as members of the finance team, or high-level employees).

[0053] The formatting module may format, present a rank for, and output the current email threat report, from a template of a plurality of report templates, that is outputted for a human user's consumption in a medium of, any of 1) a printable report, 2) presented digitally on a user interface, 3) in a machine readable format for further use in machine-learning reinforcement and refinement, and 4) any combination of the three.

[0054] The system may use at least three separate machine learning models. For example, a machine learning model may be trained on specific aspects of the normal pattern of life for entities in the system, such as devices, users, network traffic flow, outputs from one or more cyber security analysis tools analysing the system, etc. One or more machine learning models may also be trained on characteristics and aspects of all manner of types of cyber threats. One or more machine learning models may also be trained on composing email threat reports.

[0055] The various modules cooperate with each other, the AI models, and the data store to carry out the operations discussed herein. The trigger module, the AI models, the gatherer module, the analyser module, the assessment module, the formatting module, and the data store cooperate to improve the analysis and formalized

report generation with less repetition to consume less CPU cycles, as well as doing this more efficiently and effectively than humans. For example, the modules can repetitively go through these steps and re-duplicate steps to filter and rank the one or more supported possible cyber threat hypotheses from the possible set of cyber threat hypotheses and/or compose the detailed information to populate into the email threat report.

[0056] One or more processing units are configured to execute software instructions associated with the intelligent-adversary simulator, the formatting module, other modules, and models in the cyber security appliance 100.

[0057] One or more non-transitory storage mediums are configured to store at least software associated with the intelligent-adversary simulator, the other modules, and AI models.

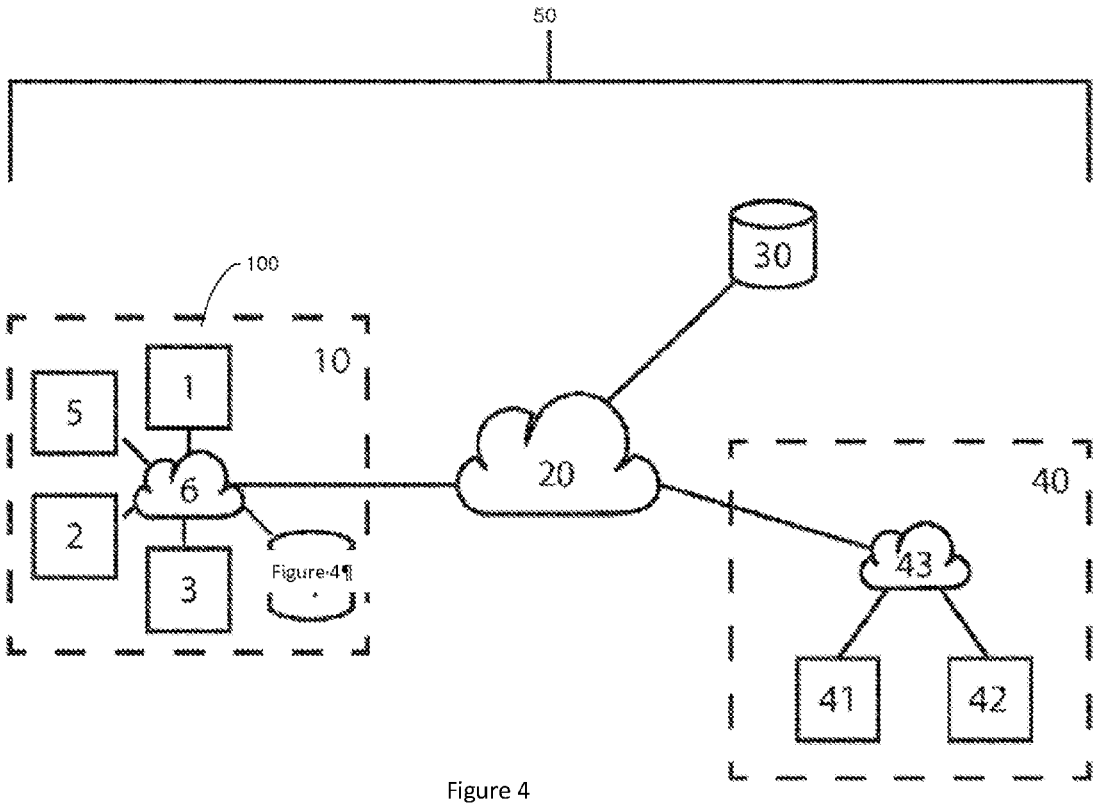



Figure 4

[0058] Figure 4 illustrates an example cyber security appliance to protect an example network. The example network of computer systems 50 uses a cyber security appliance 100. The system depicted is a simplified illustration, which is provided for ease of explanation. The system 50 comprises a first computer system 10 within a building, which uses the threat detection system to detect and thereby attempt to prevent threats to computing devices within its bounds.

[0059] The first computer system 10 comprises three computers 1, 2, 3, a local server 4, and a multifunctional device 5 that provides printing, scanning and facsimile functionalities to each of the computers 1, 2, 3. All of the devices within the first computer system 10 are communicatively coupled via a Local Area Network 6. Consequently, all of the computers 1, 2, 3 are able to access the local server 4 via the LAN 6 and use the functionalities of the MFD 5 via the LAN 6.

[0060] The LAN 6 of the first computer system 10 is connected to the Internet 20, which in turn provides computers 1, 2, 3 with access to a multitude of other computing devices 18 including server 30 and second computer system 40. The second computer system 40 also includes two computers 41, 42, connected by a second LAN 43.

[0061] In this exemplary embodiment of the cyber security appliance 100, computer 1 on the first computer system 10 has the hardware and software of the cyber security appliance 100; and therefore, runs threat detection for detecting threats to the first computer system. As such, the computer system includes one or more processors arranged to run the steps of the process described herein, memory storage components required to store information related to the running of the process, as well as a network interface for collecting the required information from the lightweight probes.

[0062] The cyber security appliance 100 in computer 1 builds and maintains a dynamic, ever-changing model of the 'normal behaviour' of each user and machine within the system 10. The approach is based on Bayesian mathematics, and monitors all interactions, events and communications within the system 10 - which computer is talking to which, files that have been created, networks that are being accessed.

[0063] For example, computer 2 is based in a company's San Francisco office and operated by a marketing employee who regularly accesses the marketing network, usually communicates with machines in the company's U.K. office in second computer system 40 between 9.30 AM and midday, and is active from about 8:30 AM until 6 PM.

[0064] The same employee virtually never accesses the employee time sheets, very rarely connects to the company's Atlanta network and has no dealings in South-East Asia. The threat detection system takes all the information that is available relating to this employee and establishes a 'pattern of life' for that person and the devices used by that person in that system, which is dynamically updated as more information is gathered. The 'normal' of the model of the normal pattern of life is used as a moving benchmark, allowing the system to spot behaviour on a system that seems to fall outside of this normal pattern of life, and flags this behaviour as anomalous, requiring further investigation.

[0065] The cyber security appliance 100 is built to deal with the fact that today's attackers are getting stealthier and an attacker/malicious agent may be 'hiding' in a system to ensure that they avoid raising suspicion in an end user, such as by slowing their machine down.

[0066] The cyber security appliance builds a sophisticated 'pattern of life' – that understands what represents normality for every person, device, and network activity in the system being protected by the cyber security appliance 100.

[0067] The cyber security appliance 100 can use unsupervised machine learning to works things out without pre-defined labels. In the case of sorting a series of different entities, such as animals, the system analyses the information and works out the different classes of animals. This allows the system to handle the unexpected and embrace uncertainty when new entities and classes are examined. The system does not always know what it is looking for, but can independently classify data and detect compelling patterns.

[0068] The cyber security appliance 100's unsupervised machine learning methods do not require training data with pre-defined labels. Instead, they are able to identify key patterns and trends in the data, without the need for human input. The advantage of unsupervised learning in this system is that it allows computers to go beyond what their programmers already know and discover previously unknown relationships. The unsupervised machine learning methods can use a probabilistic approach based on a Bayesian framework. The machine learning allows the cyber security appliance 100 to integrate a huge number of weak indicators/low threat values by themselves of potentially anomalous network behaviour to produce a single clear overall measure of these correlated anomalies to determine how likely a network device is to be compromised. This probabilistic mathematical approach provides an ability to understand important information, amid the noise of the network – even when it does not know what it is looking for.

[0069] The cyber security appliance 100 can use a Recursive Bayesian Estimation. To combine these multiple analyses of different measures of network behaviour to generate a single overall/comprehensive picture of the state of each device, the cyber security appliance 100 takes advantage of the power of Recursive Bayesian Estimation (RBE) via an implementation of the Bayes filter.

[0070] Using RBE, the cyber security appliance 100's AI models are able to constantly adapt themselves, in a computationally efficient manner, as new information becomes available to the system. The cyber security appliance 100's AI models continually recalculate threat levels in the light of new evidence, identifying changing attack behaviours where conventional signature-based methods fall down.

[0071] Training a model can be accomplished by having the model learn good values for all of the weights and the bias for labelled examples created by the system, and in this case; starting with no labels initially. A goal of the training of the model can be to find a set of weights and biases that have low loss, on average, across all examples.

[0072] An anomaly detection technique that can be used is supervised anomaly detection that requires a data set that has been labelled as "normal" and "abnormal" and involves training a classifier. Another anomaly detection technique that can be used is an unsupervised anomaly detection that detects anomalies in an unlabelled test data set under the assumption that the majority of the instances in the data set are normal, by looking for instances that seem to fit least to the remainder of the data set. The model representing normal behaviour from a given normal training data set can detect anomalies by establishing the normal pattern and then test the likelihood of a test

instance under analysis to be generated by the model. Anomaly detection can identify rare items, events or observations which raise suspicions by differing significantly from the majority of the data, which includes rare objects as well as things like unexpected bursts in activity.

[0073] The method, apparatus and system are arranged to be performed by one or more processing components with any portions of software stored in an executable format on a computer readable medium. Thus, any portions of the method, apparatus and system implemented as software can be stored in one or more non-transitory memory storage devices in an executable format to be executed by one or more processors. The computer readable medium may be non-transitory and does not include radio or other carrier waves. The computer readable medium could be, for example, a physical computer readable medium such as semiconductor memory or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disc, and an optical disk, such as a CD-ROM, CD-R/W or DVD.

[0074] The various methods described above may be implemented by a computer program product. The computer program product may include computer code arranged to instruct a computer to perform the functions of one or more of the various methods described above. The computer program and/or the code for performing such methods may be provided to an apparatus, such as a computer, on a computer readable medium or computer program product. For the computer program product, a transitory computer readable medium may include radio or other carrier waves.

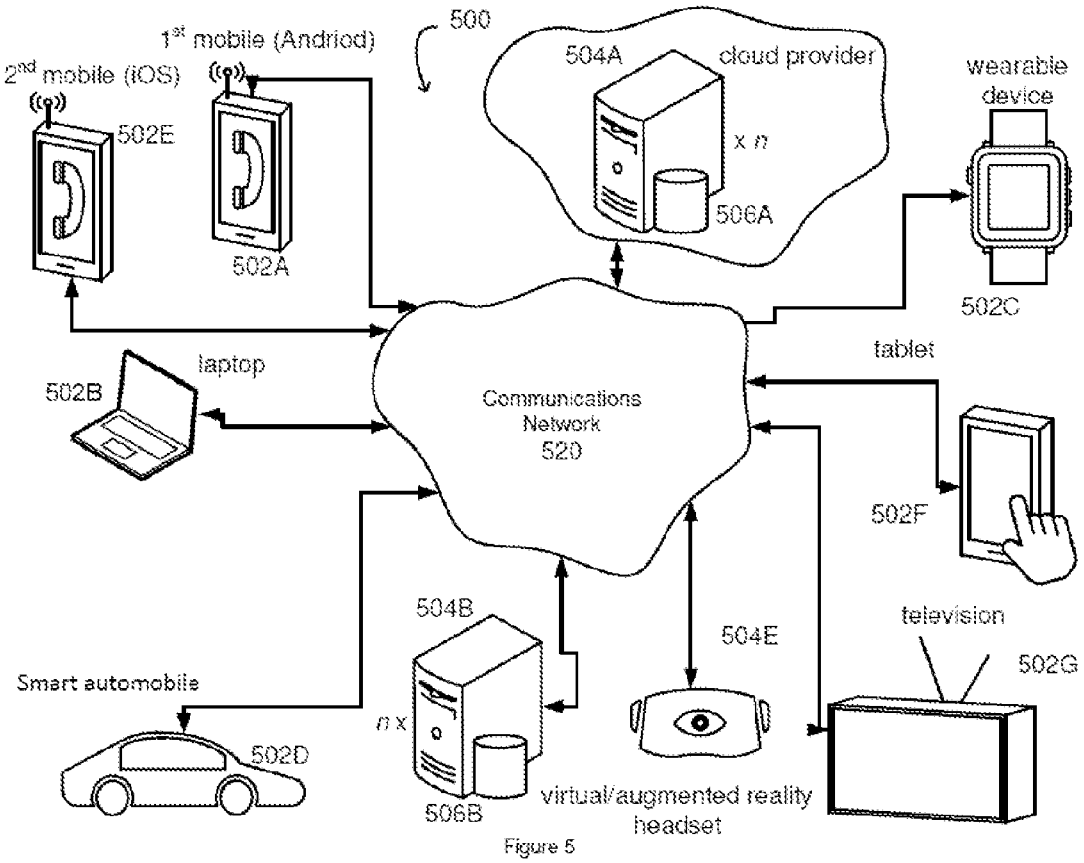


Figure 5

**Network**

[0075] Figure 5 illustrates a block diagram of a number of electronic systems and devices communicating with each other in a network environment in accordance with an embodiment of the current design.

[0076] The network environment has a communications network 520 that connects server computing systems 504A through 504B, and at least one or more client computing systems 502A to 502G. As shown, there may be many server computing systems 504A through 504B and many client computing systems 502A to 502G connected to each other via the network 520, which may be, for example, the Internet. Note, that alternatively the network 520 might be or include one or more of: an optical

network, a cellular network, the Internet, a Local Area Network (LAN), Wide Area Network (WAN), satellite link, fiber network, cable network, or a combination of these and/or others. Each server computing systems 504A-504B can have circuitry and software to communication with the other server computing systems 504A through 504B and the client computing systems 502A to 502G across the network 520. Each server computing systems 504A to 504B can be associated with one or more databases 506A to 506B. Each server 504A to 504B may have one or more instances of a virtual server running on that physical server and multiple virtual instances may be implemented by the design. A firewall may be established between a client computing system, for example, 502D and the network 520 to protect data integrity on the client computing system 502D.

[0077] A cloud provider service can install and operate application software in the cloud and users can access the software service from the client devices. Cloud users who have a site in the cloud may not solely manage the cloud infrastructure and platform where the application runs. Thus, the servers and databases may be shared hardware where the user is given a certain amount of dedicated use of these resources. The user's cloud-based site is given a virtual amount of dedicated space and bandwidth in the cloud. Cloud applications can be different from other applications in their scalability, which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user, who sees only a single access point.

[0078] The cloud-based remote access is coded to utilize a protocol, such as Hypertext Transfer Protocol (HTTP), to engage in a request and response cycle with both a mobile device application resident on a client device, 502A-502G, as well as a web-browser application resident on the client device, 502A-502G. In some situations, the cloud-based remote access for a wearable electronic device 502C, can be accessed via a mobile device, a desktop, a tablet device, cooperating with that wearable electronic device 502C. The cloud-based remote access between a client device 502A-502G and the cloud-based provider site 504A is coded to engage in one or more of the following 1) the request and response cycle from all web browser based applications, 2) SMS/twitter based request and response message exchanges, 3) the request and response cycle from a dedicated on-line server, 4) the request and response cycle directly between a native mobile application resident on a client device and the cloud-based remote access to a wearable electronic device, and 5) combinations of these.

[0079] In an embodiment, the server computing system 504A may include a server engine, a web page management component or online service or online app component, a content management component, and a database management component. The server engine performs basic processing and operating system level tasks. The web page management component, online service, or online app component handles creation and display or routing of web pages or screens associated with receiving and providing digital content and digital advertisements. Users may access the server-computing device by means of a URL associated therewith. The content management component handles most of the functions in the embodiments described herein. The database management component includes storage and

retrieval tasks with respect to the database, queries to the database, and storage of data.

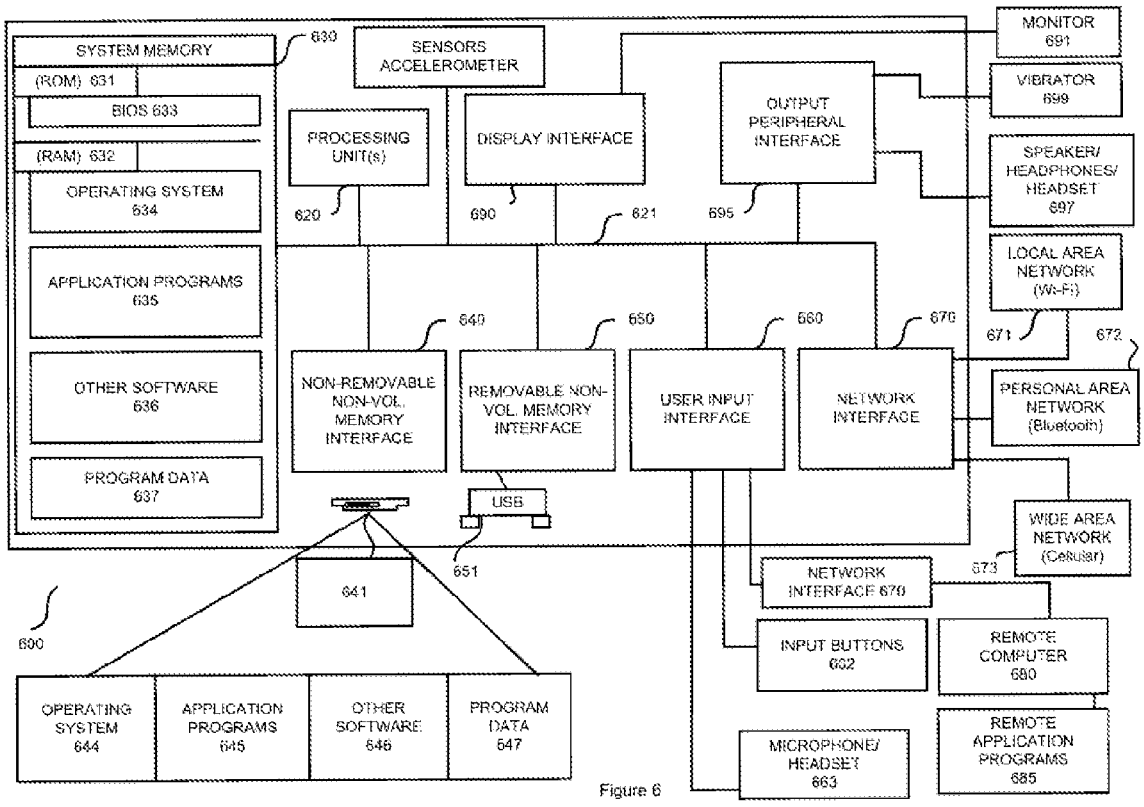


Figure 6

## Computing devices

[0080] Figure 6 illustrates a block diagram of an embodiment of one or more computing devices that can be a part of the conversational assistant for an embodiment of the current design discussed herein.

[0081] The computing device may include one or more processors or processing units 620 to execute instructions, one or more memories 630-632 to store information, one or more data input components 660-663 to receive data input from a user of the computing device 600, one or more modules that include the management module, a network interface communication circuit 670 to establish a communication link to

communicate with other computing devices external to the computing device, one or more sensors where an output from the sensors is used for sensing a specific triggering condition and then correspondingly generating one or more preprogrammed actions, a display screen 691 to display at least some of the information stored in the one or more memories 630-632 and other components. Note, portions of this design implemented in software 644, 645, 646 are stored in the one or more memories 630-632 and are executed by the one or more processors 620. The processing unit 620 may have one or more processing cores, which couples to a system bus 621 that couples various system components including the system memory 630. The system bus 621 may be any of several types of bus structures selected from a memory bus, an interconnect fabric, a peripheral bus, and a local bus using any of a variety of bus architectures.

[0082] Computing device 602 typically includes a variety of computing machine-readable media. Machine-readable media can be any available media that can be accessed by computing device 602 and includes both volatile and nonvolatile media, and removable and non-removable media. By way of example, and not limitation, computing machine-readable media use includes storage of information, such as computer-readable instructions, data structures, other executable software, or other data. Computer-storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other tangible medium which can be used to store the desired information and which can be accessed by the computing device 602. Transitory media such as wireless channels are not included in the machine-readable

media. Machine-readable media typically embody computer readable instructions, data structures, and other executable software.

[0083] In an example, a volatile memory drive 641 is illustrated for storing portions of the operating system 644, application programs 645, other executable software 646, and program data 647.

[0084] A user may enter commands and information into the computing device 602 through input devices such as a keyboard, touchscreen, or software or hardware input buttons 662, a microphone 663, a pointing device and/or scrolling input component, such as a mouse, trackball or touch pad 661. The microphone 663 can cooperate with speech recognition software. These and other input devices are often connected to the processing unit 620 through a user input interface 660 that is coupled to the system bus 621, but can be connected by other interface and bus structures, such as a lighting port, game port, or a universal serial bus (USB). A display monitor 691 or other type of display screen device is also connected to the system bus 621 via an interface, such as a display interface 690. In addition to the monitor 691, computing devices may also include other peripheral output devices such as speakers 697, a vibration device 699, and other output devices, which may be connected through an output peripheral interface 695.

[0085] The computing device 602 can operate in a networked environment using logical connections to one or more remote computers/client devices, such as a remote computing system 680. The remote computing system 680 can a personal computer, a mobile computing device, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described

above relative to the computing device 602. The logical connections can include a personal area network (PAN) 672 (e.g., Bluetooth®), a local area network (LAN) 671 (e.g., Wi-Fi), and a wide area network (WAN) 673 (e.g., cellular network). Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet. A browser application and/or one or more local apps may be resident on the computing device and stored in the memory.

[0086] When used in a LAN networking environment, the computing device 602 is connected to the LAN 671 through a network interface 670, which can be, for example, a Bluetooth® or Wi-Fi adapter. When used in a WAN networking environment (e.g., Internet), the computing device 602 typically includes some means for establishing communications over the WAN 673. With respect to mobile telecommunication technologies, for example, a radio interface, which can be internal or external, can be connected to the system bus 621 via the network interface 670, or other appropriate mechanism. In a networked environment, other software depicted relative to the computing device 602, or portions thereof, may be stored in the remote memory storage device. By way of example, and not limitation, remote application programs 685 as reside on remote computing device 680. It will be appreciated that the network connections shown are examples and other means of establishing a communications link between the computing devices that may be used.

[0087] It should be noted that the present design can be carried out on a computing device such as that described with respect to this Figure. However, the present design can be carried out on a server, a computing device devoted to message

handling, or on a distributed system in which different portions of the present design are carried out on different parts of the distributed computing system.

[0088] Note, an application described herein includes but is not limited to software applications, mobile applications, and programs that are part of an operating system application. Some portions of this description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. These algorithms can be written in a number of different software programming languages such as C, C++, HTTP, Java, or other similar languages. Also, an algorithm can be implemented with lines of code in software, configured logic gates in software, or a combination of both. In an embodiment, the logic consists of electronic circuits that follow the rules of Boolean Logic, software that contain patterns of instructions, or any combination of both. A module may be implemented in hardware electronic components, software components, and a combination of both.

[0089] Generally, an application includes programs, routines, objects, widgets, plug-ins, and other similar structures that perform particular tasks or implement particular abstract data types. Those skilled in the art can implement the description and/or figures herein as computer-executable instructions, which can be embodied on any form of computing machine-readable media discussed herein.

[0090] Many functions performed by electronic hardware components can be duplicated by software emulation. Thus, a software program written to accomplish those same functions can emulate the functionality of the hardware components in input-output circuitry.

[0091] While the foregoing design and embodiments thereof have been provided in considerable detail, it is not the intention of the applicant(s) for the design and embodiments provided herein to be limiting. Additional adaptations and/or modifications are possible, and, in broader aspects, these adaptations and/or modifications are also encompassed. Accordingly, departures may be made from the foregoing design and embodiments without departing from the scope afforded by the following claims, which scope is only limited by the claims when appropriately construed.

CLAIMS

1. An apparatus as described herein.

2. A method as described herein.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

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

## Secrecy Order 37 CFR 5.2:

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

## Inventor Information:

**Inventor 1** Remove

**Legal Name**

| Prefix | Given Name | Middle Name | Family Name | Suffix |
|---|---|---|---|---|
| | Simon | David Lincoln | Fellows | |

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

| City | Cambridge | Country of Residence [i] | UK |
|---|---|---|---|

**Mailing Address of Inventor:**

| Address 1 | 19 Broad Street, Great Cambourne | | |
|---|---|---|---|
| Address 2 | | | |
| City | Cambridge | State/Province | |
| Postal Code | CB23 6EL | Country [i] | UK |

**Inventor 2** Remove

**Legal Name**

| Prefix | Given Name | Middle Name | Family Name | Suffix |
|---|---|---|---|---|
| | Jack | | Pearson | |

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

| City | Northumberland | Country of Residence [i] | UK |
|---|---|---|---|

**Mailing Address of Inventor:**

| Address 1 | 5 Hampstead Close, Blyth | | |
|---|---|---|---|
| Address 2 | | | |
| City | Northumberland | State/Province | |
| Postal Code | NE24 3XE | Country [i] | UK |

**Inventor 3** Remove

**Legal Name**

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

| Prefix | Given Name | Middle Name | Family Name | Suffix |
|---|---|---|---|---|
| | Matthew | | Dunn | |

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

| City | Ely | Country of Residence [i] | UK |
|---|---|---|---|

Mailing Address of Inventor:

| Address 1 | Church Farm, The Hamlet, Chettisham | | |
|---|---|---|---|
| Address 2 | | | |
| City | Ely | State/Province | |
| Postal Code | CB61SB | Country [i] | UK |

Inventor 4 Remove

Legal Name

| Prefix | Given Name | Middle Name | Family Name | Suffix |
|---|---|---|---|---|
| | Jack | Benjamin | Stockdale | |

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

| City | Cambridge | Country of Residence [i] | UK |
|---|---|---|---|

Mailing Address of Inventor:

| Address 1 | The Old Rectory, Green End, Landbeach | | |
|---|---|---|---|
| Address 2 | | | |
| City | Cambridge | State/Province | |
| Postal Code | CB25 9FD | Country [i] | UK |

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

## Correspondence Information:

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

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

| Customer Number | 34284 | | |
|---|---|---|---|
| Email Address | patents@rutan.com | Add Email | Remove Email |

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

## Application Information:

| | | | |
|---|---|---|---|
| **Title of the Invention** | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | | |
| **Attorney Docket Number** | 034036-0014PRO | **Small Entity Status Claimed** | ☐ |
| **Application Type** | Provisional | | |
| **Subject Matter** | Utility | | |
| **Total Number of Drawing Sheets (if any)** | | **Suggested Figure for Publication (if any)** | |

## Filing By Reference:

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

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

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

## Publication Information:

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

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

## Representative Information:

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

| | | | |
|---|---|---|---|
| Please Select One: | ◉ Customer Number | ○ US Patent Practitioner | ○ Limited Recognition (37 CFR 11.9) |
| Customer Number | 34284 | | |

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

## Domestic Benefit/National Stage Information:

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

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

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

## Foreign Priority Information:

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

| Remove | | | |
|---|---|---|---|
| Application Number | Country[i] | Filing Date (YYYY-MM-DD) | Access Code[i] (if applicable) |
| | | | |

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

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

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

# Authorization or Opt-Out of Authorization to Permit Access:

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

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

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

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

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

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

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

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

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

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

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

# Applicant Information:

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

**Applicant 1**

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

Clear

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

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

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

| Organization Name | Darktrace Holdings Limited | | |
|---|---|---|---|
| **Mailing Address Information For Applicant:** | | | |
| **Address 1** | Maurice Wilkes Building, St John's Innovation Park | | |
| Address 2 | Cowley Road | | |
| **City** | Cambridge | **State/Province** | |
| **Country** | UK | Postal Code | CB4 0DS |
| Phone Number | | Fax Number | |
| Email Address | | | |

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

# Assignee Information including Non-Applicant Assignee Information:

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| **Application Data Sheet 37 CFR 1.76** | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

**Assignee 1**

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

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

| Prefix | **Given Name** | Middle Name | **Family Name** | Suffix |
|---|---|---|---|---|
| | | | | |

**Mailing Address Information For Assignee including Non-Applicant Assignee:**

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

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

## Signature:

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

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

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

| **Signature** | /Thomas S. Ferrill/ | | | Date (YYYY-MM-DD) | 2021-11-22 |
|---|---|---|---|---|---|
| First Name | Thomas S. | Last Name | Ferrill | Registration Number | 42532 |

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | 034036-0014PRO |
|---|---|---|
| | Application Number | |
| Title of Invention | CYBER SECURITY TOOLS TO PROTECT A SYSTEM | |

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

# Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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