US 20250260702A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0260702 A1**

**Goldstein** (43) **Pub. Date: Aug. 14, 2025**

(54) **SYSTEM AND METHOD FOR AI-BASED INTRUSION BEHAVIOUR ANALYSIS**

(71) Applicant: **Steven W. Goldstein**, Delray Beach, FL (US)

(72) Inventor: **Steven W. Goldstein**, Delray Beach, FL (US)

(21) Appl. No.: **18/436,482**

(22) Filed: **Feb. 8, 2024**

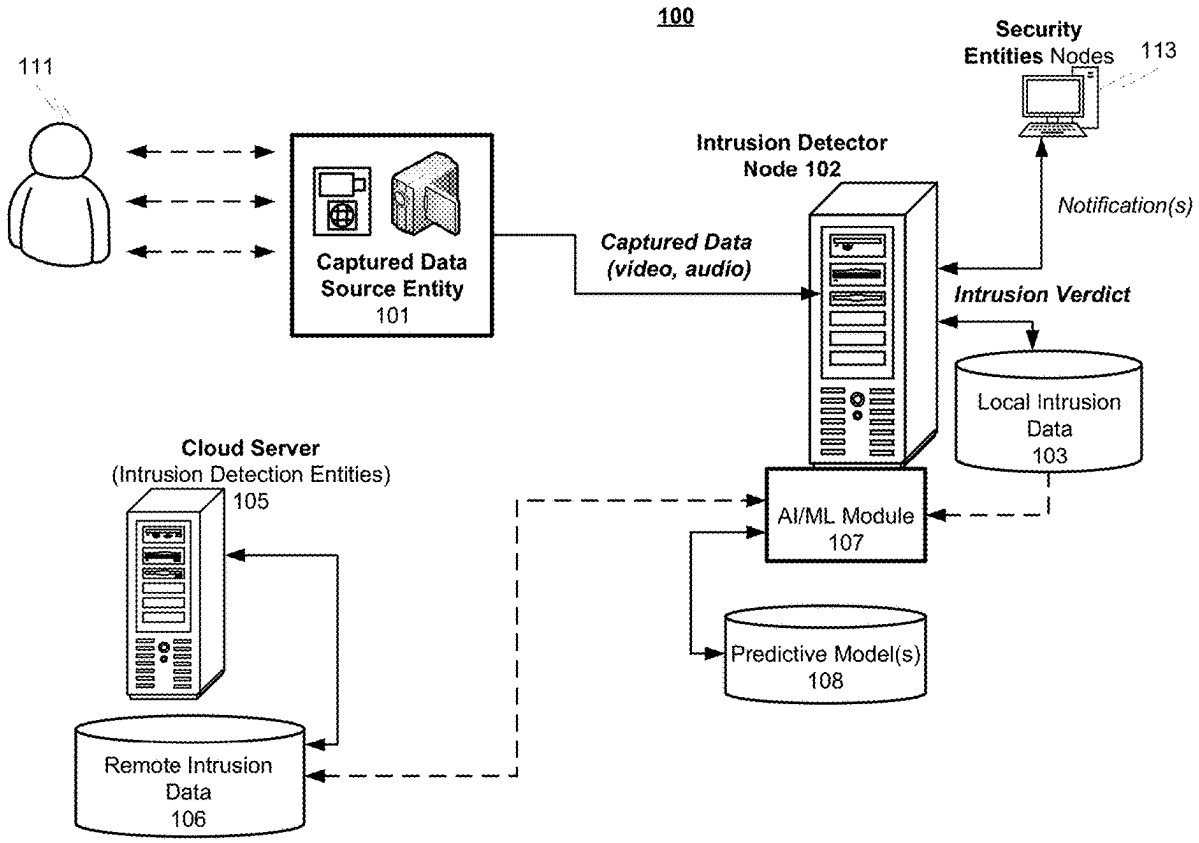
**Publication Classification**

(51) **Int. Cl.**
***H04L 9/40*** (2022.01)

(52) **U.S. Cl.**
CPC ..... ***H04L 63/1425*** (2013.01); ***H04L 63/1416*** (2013.01)

(57) **ABSTRACT**

A system for an automated real-time intrusion detection based on predictive analytics of intrusion-related data, including a processor of an intrusion detection (ID) node configured to host a machine learning (ML) module and connected to at least one captured data source entity node over a network and a memory on which are stored machine-readable instructions that when executed by the processor, cause the processor to: acquire intrusion-related captured data from the at least one captured data source entity node; parse the captured data to derive a plurality of key features; query a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features; generate at least one feature vector based on the plurality of key features and the local historical intrusions'-related data; and provide the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict.



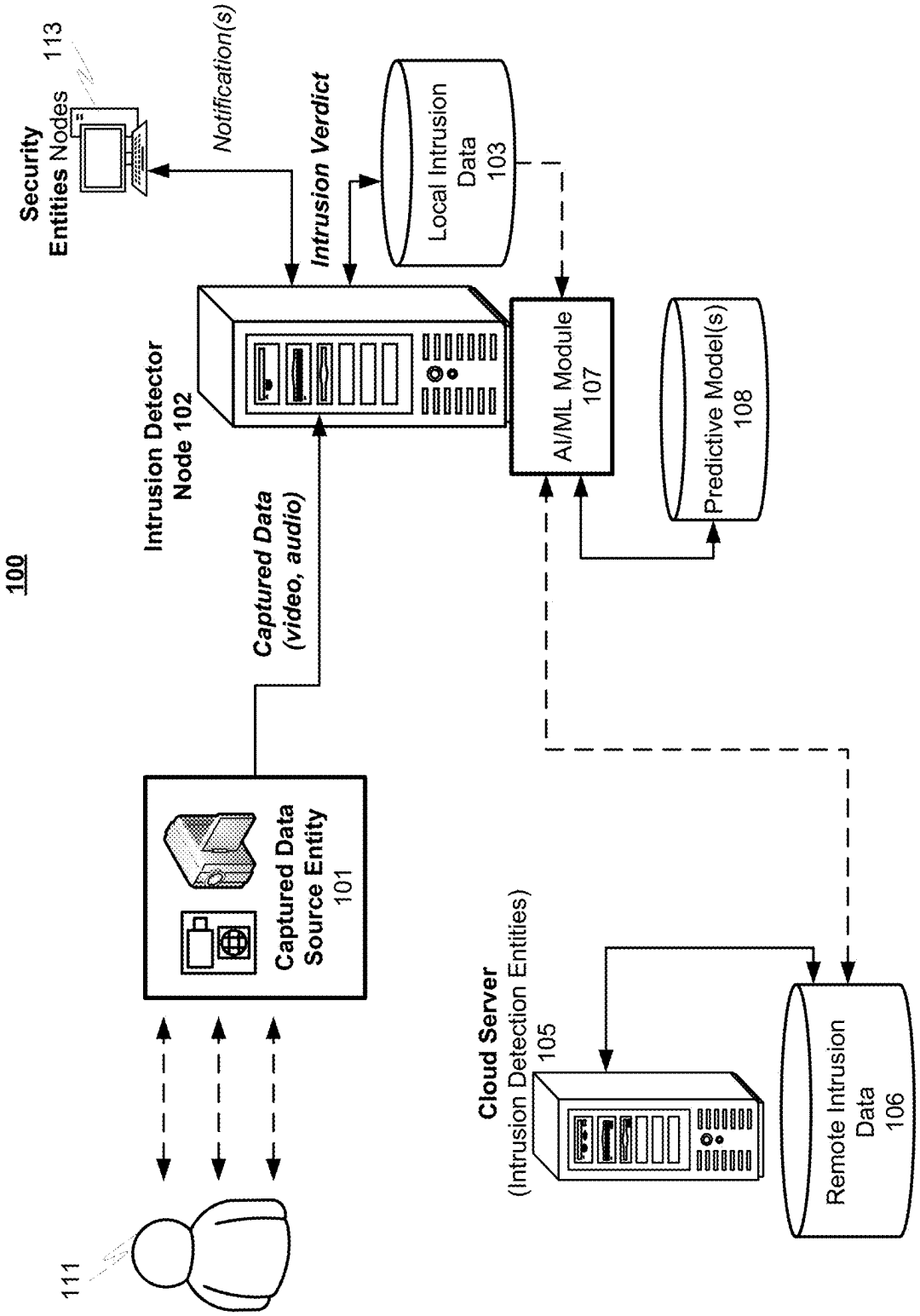

100
Security Entities Nodes
113
Notification(s)
Intrusion Verdict
Local Intrusion Data
103
Intrusion Detector Node 102
AI/ML Module
107
Predictive Model(s)
108
Captured Data (video, audio)
Captured Data Source Entity
101
Cloud Server
(Intrusion Detection Entities)
105
Remote Intrusion Data
106
111

FIG. 1A

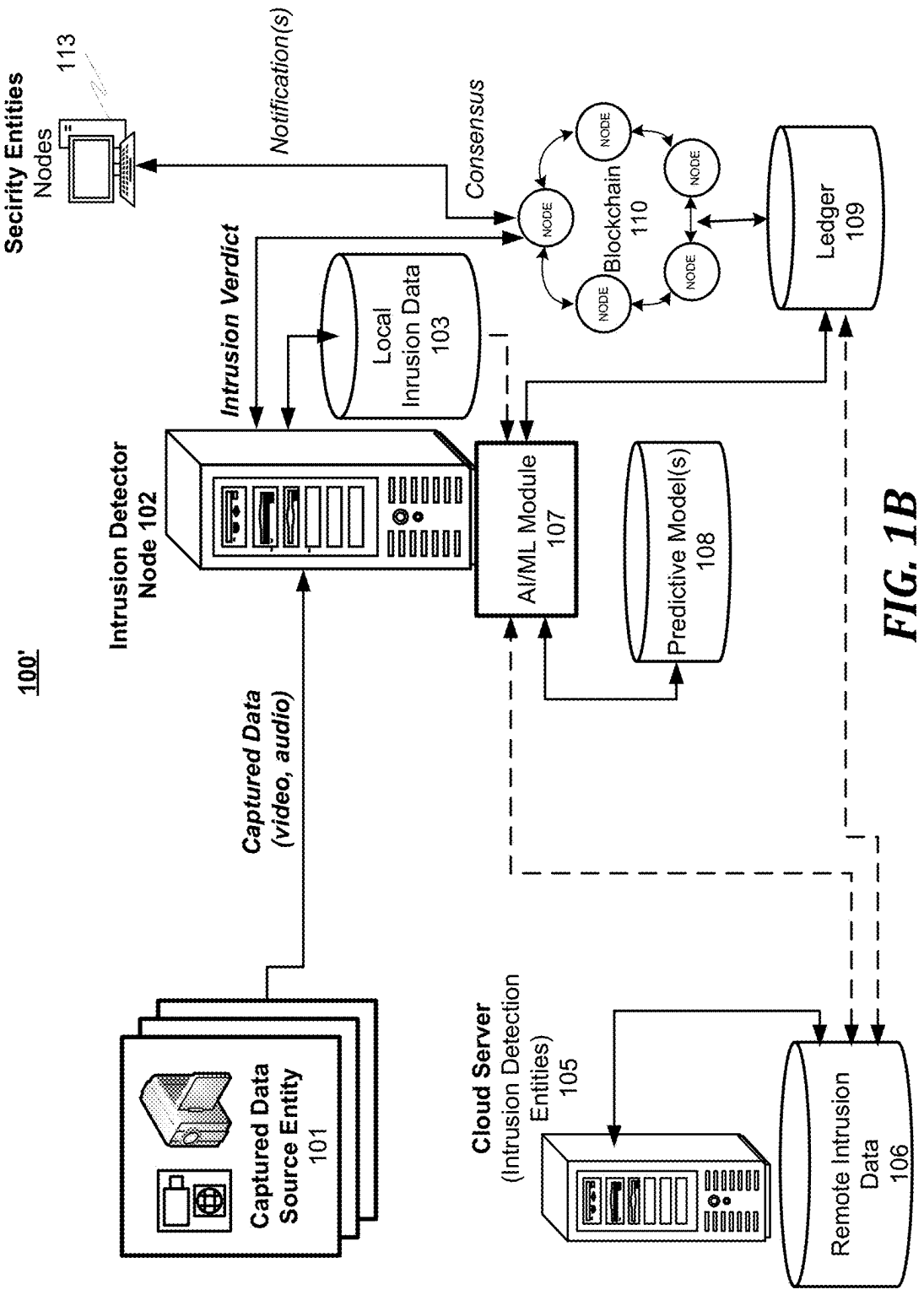

100'
Secirity Entities
Nodes
113
Notification(s)
Consensus
Intrusion Verdict
Local
Inrusion Data
103
Blockchain
110
NODE
Ledger
109
Intrusion Detector
Node 102
AI/ML Module
107
Predictive Model(s)
108
Captured Data
(video, audio)
Captured Data
Source Entity
101
Cloud Server
(Intrusion Detection
Entities)
105
Remote Intrusion
Data
106

FIG. 1B

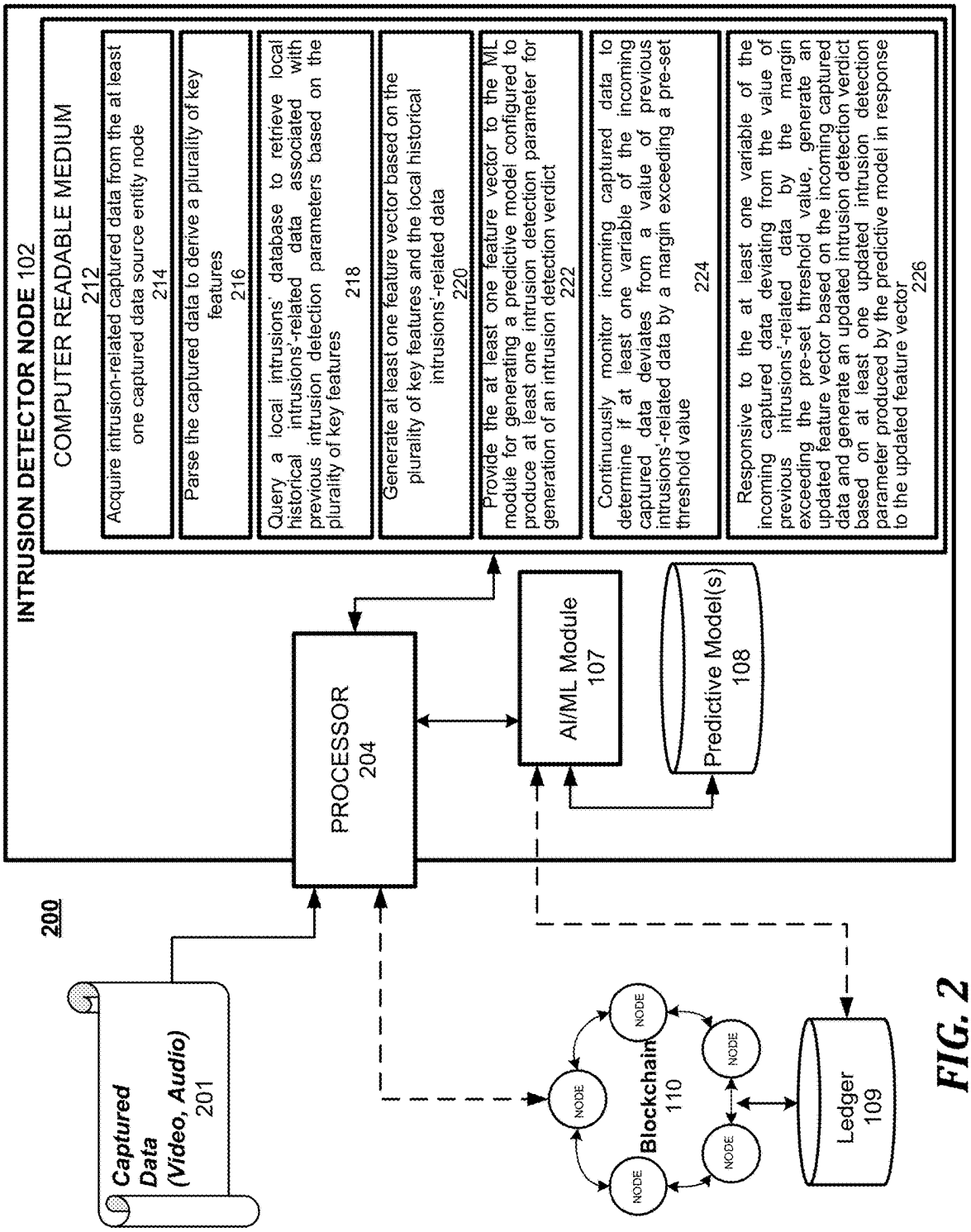

200
INTRUSION DETECTOR NODE 102
COMPUTER READABLE MEDIUM
212
Acquire intrusion-related captured data from the at least one captured data source entity node
214
Parse the captured data to derive a plurality of key features
216
Query a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features
218
Generate at least one feature vector based on the plurality of key features and the local historical intrusions'-related data
220
Provide the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict
222
Continuously monitor incoming captured data to determine if at least one variable of the incoming captured data deviates from a value of previous intrusions'-related data by a margin exceeding a pre-set threshold value
224
Responsive to the at least one variable of the incoming captured data deviating from the value of previous intrusions'-related data by the margin exceeding the pre-set threshold value, generate an updated feature vector based on the incoming captured data and generate an updated intrusion detection verdict based on at least one updated intrusion detection parameter produced by the predictive model in response to the updated feature vector
226
PROCESSOR
204
AI/ML Module
107
Predictive Model(s)
108
Captured Data (Video, Audio)
201
Blockchain
110
NODE
NODE
NODE
NODE
NODE
Ledger
109

FIG. 2

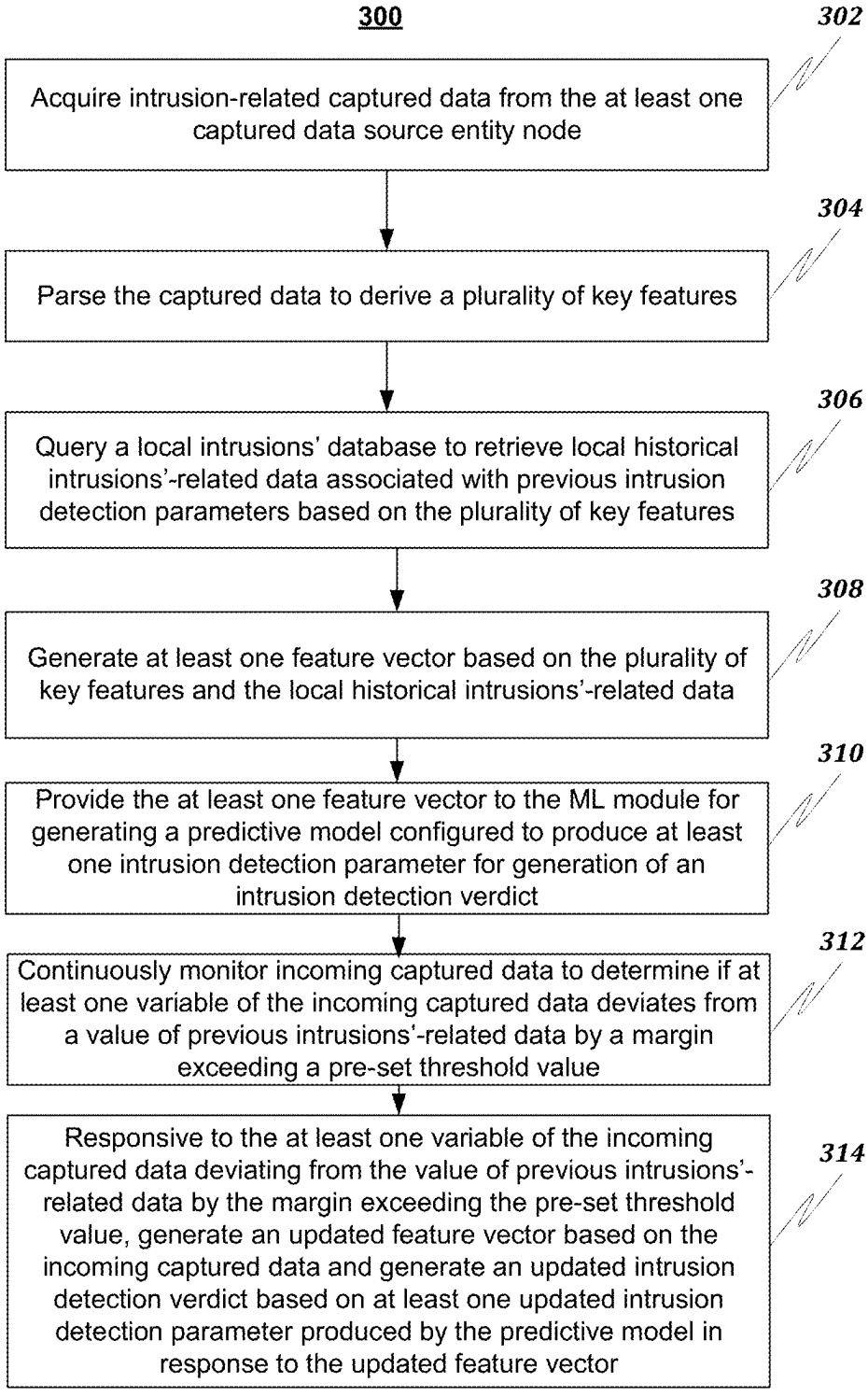

300
302
Acquire intrusion-related captured data from the at least one captured data source entity node
304
Parse the captured data to derive a plurality of key features
306
Query a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features
308
Generate at least one feature vector based on the plurality of key features and the local historical intrusions'-related data
310
Provide the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict
312
Continuously monitor incoming captured data to determine if at least one variable of the incoming captured data deviates from a value of previous intrusions'-related data by a margin exceeding a pre-set threshold value
314
Responsive to the at least one variable of the incoming captured data deviating from the value of previous intrusions'-related data by the margin exceeding the pre-set threshold value, generate an updated feature vector based on the incoming captured data and generate an updated intrusion detection verdict based on at least one updated intrusion detection parameter produced by the predictive model in response to the updated feature vector

*FIG. 3A*

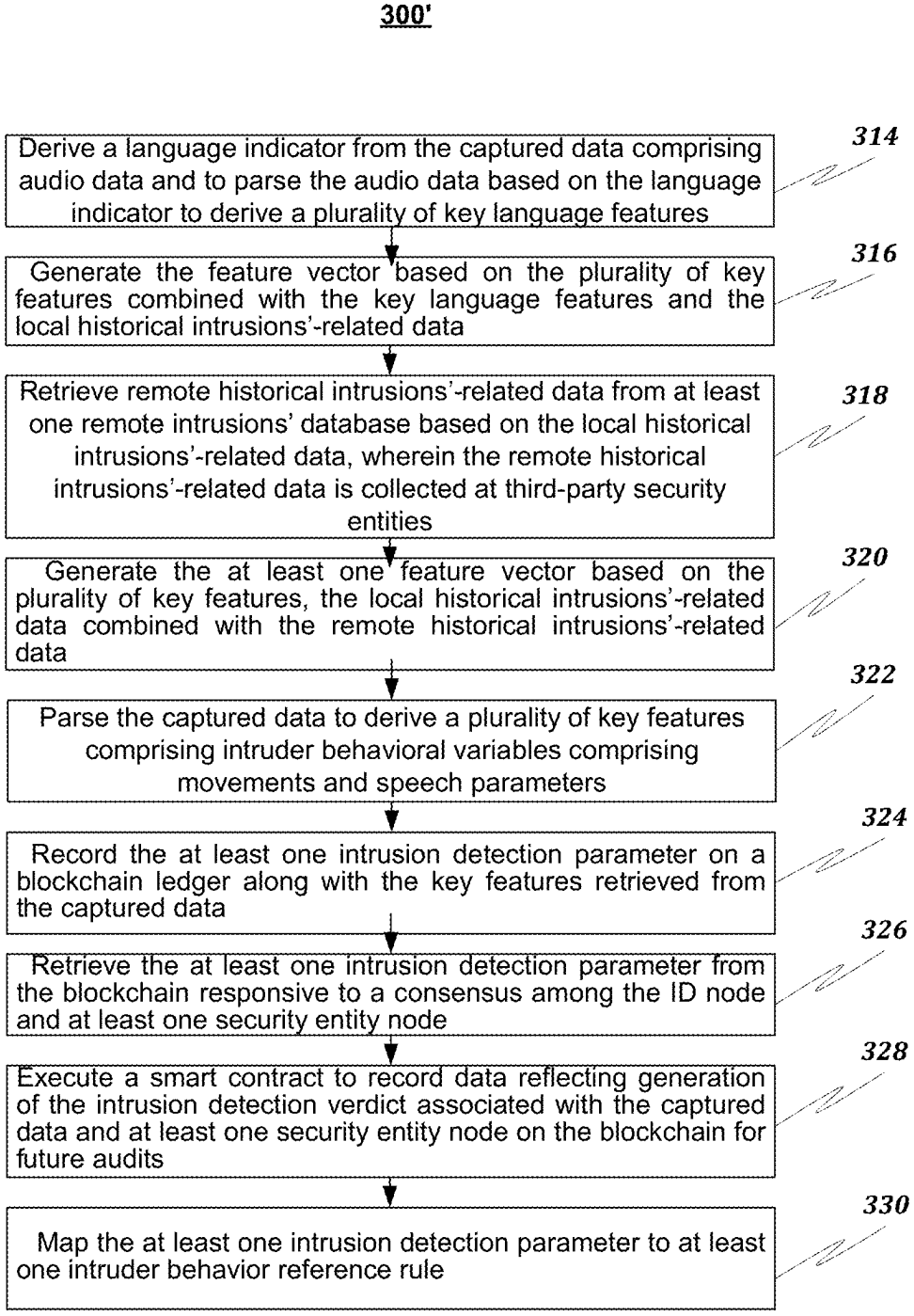

300'
Derive a language indicator from the captured data comprising audio data and to parse the audio data based on the language indicator to derive a plurality of key language features
314
Generate the feature vector based on the plurality of key features combined with the key language features and the local historical intrusions'-related data
316
Retrieve remote historical intrusions'-related data from at least one remote intrusions' database based on the local historical intrusions'-related data, wherein the remote historical intrusions'-related data is collected at third-party security entities
318
Generate the at least one feature vector based on the plurality of key features, the local historical intrusions'-related data combined with the remote historical intrusions'-related data
320
Parse the captured data to derive a plurality of key features comprising intruder behavioral variables comprising movements and speech parameters
322
Record the at least one intrusion detection parameter on a blockchain ledger along with the key features retrieved from the captured data
324
Retrieve the at least one intrusion detection parameter from the blockchain responsive to a consensus among the ID node and at least one security entity node
326
Execute a smart contract to record data reflecting generation of the intrusion detection verdict associated with the captured data and at least one security entity node on the blockchain for future audits
328
Map the at least one intrusion detection parameter to at least one intruder behavior reference rule
330

*FIG. 3B*

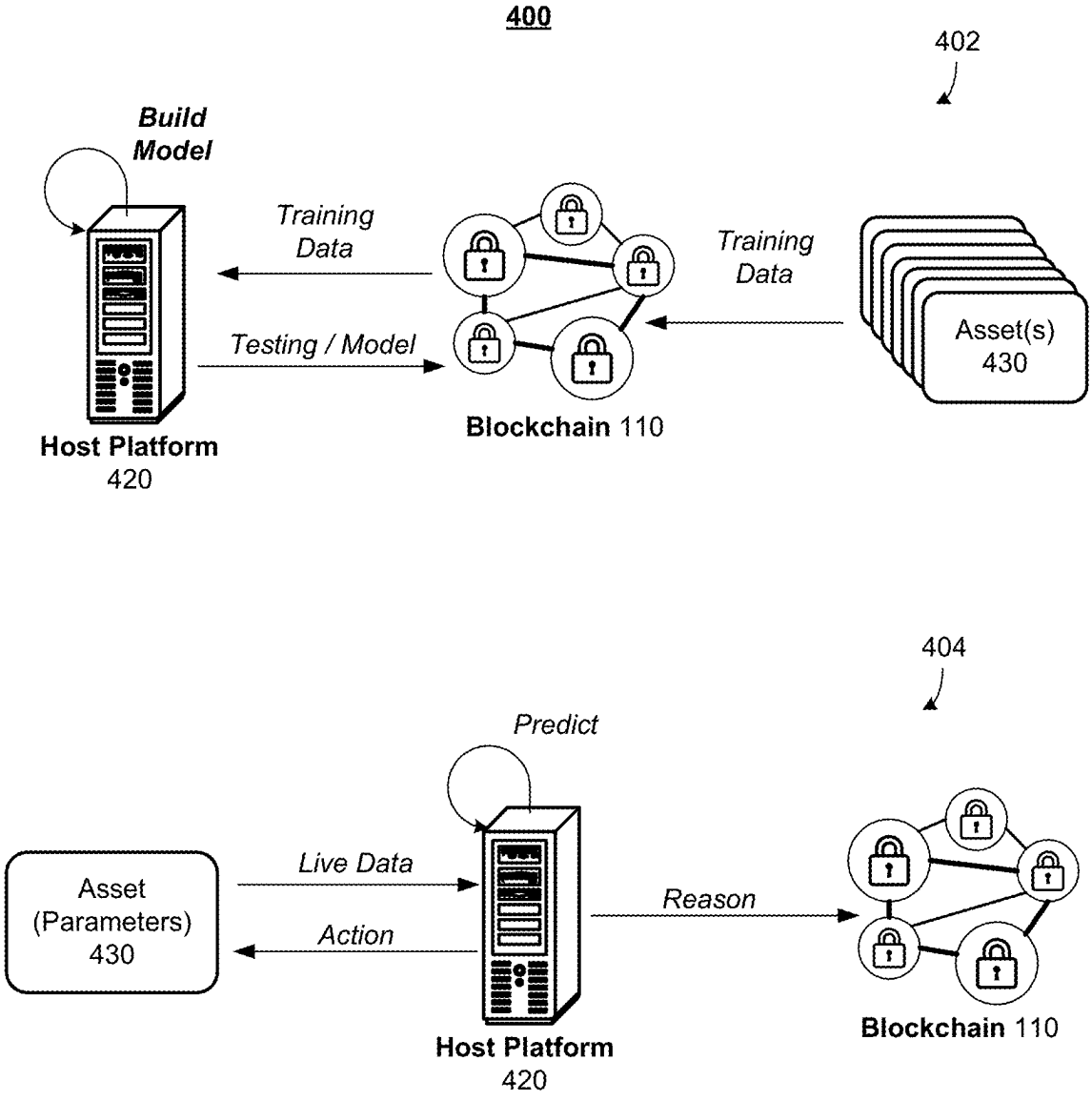

400
402
Build Model
Training Data
Testing / Model
Training Data
Asset(s) 430
Host Platform 420
Blockchain 110
404
Predict
Asset (Parameters) 430
Live Data
Action
Reason
Host Platform 420
Blockchain 110

*FIG. 4*

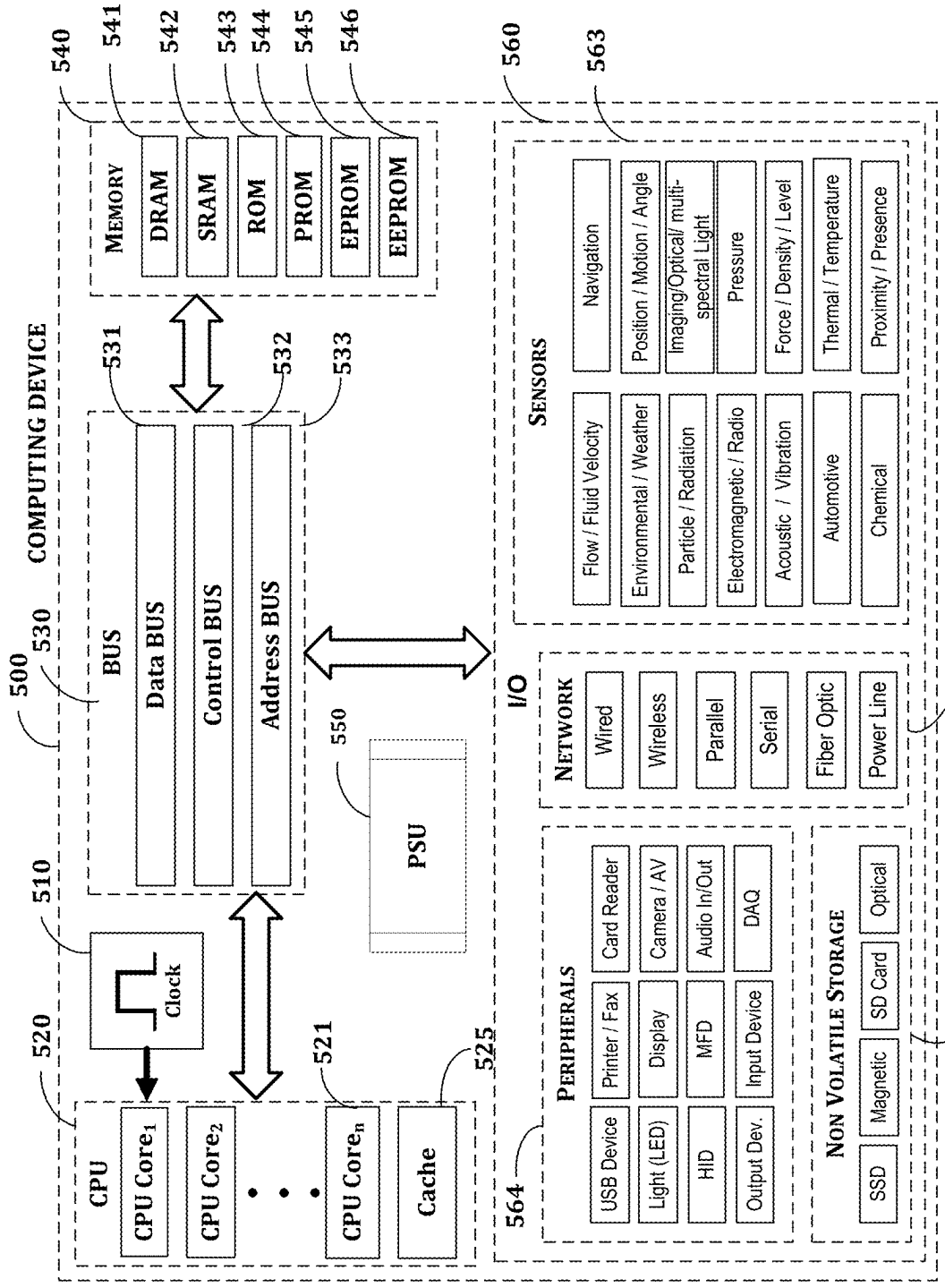

COMPUTING DEVICE
500
CPU
520
CPU Core1
CPU Core2
CPU Coren
521
Cache
525
Clock
510
BUS
530
Data BUS
Control BUS
Address BUS
531
532
533
MEMORY
540
DRAM
541
SRAM
542
ROM
543
PROM
544
EPROM
545
EEPROM
546
PSU
550
I/O
560
SENSORS
563
Navigation
Position / Motion / Angle
Imaging/Optical/ multi-spectral Light
Pressure
Force / Density / Level
Thermal / Temperature
Proximity / Presence
Flow / Fluid Velocity
Environmental / Weather
Particle / Radiation
Electromagnetic / Radio
Acoustic / Vibration
Automotive
Chemical
NETWORK
562
Wired
Wireless
Parallel
Serial
Fiber Optic
Power Line
PERIPHERALS
564
USB Device
Printer / Fax
Card Reader
Light (LED)
Display
Camera / AV
HID
MFD
Audio In/Out
Output Dev.
Input Device
DAQ
NON VOLATILE STORAGE
561
SSD
Magnetic
SD Card
Optical

FIG. 5

# SYSTEM AND METHOD FOR AI-BASED INTRUSION BEHAVIOUR ANALYSIS

## FIELD OF DISCLOSURE

**[0001]** The present disclosure generally relates to automated intrusion detection, and more particularly, to an AI-based automated system for real-time intrusion detection based on predictive analytics of intrusion-related captured data.

## BACKGROUND

**[0002]** Existing security systems are prone to error and often fail to adequately distinguish between genuine threats posed by intrusions and harmless visitors, employees or workers deployed in an organization. On the other hand, human security that may monitor large facilities is expensive and prone to errors and biases.

**[0003]** Currently there are two primary parts to the physical security world, the first is monitoring which is a passive process meant to be rewatched after an incident that is captured and replayed as a video. The next step is detection. In this mode the security system may be actively looking and monitoring for specific features in order to send notifications to the security personnel of a possible intrusion action in progress. For many intrusion actions or scenarios various levels of training for the security personnel are required. These levels of training may not allow for a low-level of training security personnel to perform the same intrusion detection tasks as the high-level of training individual. Additionally, at any level, the intrusion detection process largely depends on human error and judgements.

**[0004]** Accordingly, an AI-based automated system and method for real-time intrusion detection based on predictive analytics of captured intrusion-related data are desired.

## BRIEF OVERVIEW

**[0005]** This brief overview is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This brief overview is not intended to identify key features or essential features of the claimed subject matter. Nor is this brief overview intended to be used to limit the claimed subject matter's scope.

**[0006]** One embodiment of the present disclosure provides a system for an automated real-time intrusion detection based on predictive analytics of intrusion-related data, including a processor of an intrusion detection (ID) node configured to host a machine learning (ML) module and connected to at least one captured data source entity node over a network and a memory on which are stored machine-readable instructions that when executed by the processor, cause the processor to: acquire intrusion-related captured data from the at least one captured data source entity node; parse the captured data to derive a plurality of key features; query a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features; generate at least one feature vector based on the plurality of key features and the local historical intrusions'-related data; and provide the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict.

**[0007]** Another embodiment of the present disclosure provides a method that includes one or more of: acquiring intrusion-related captured data from the at least one captured data source entity node; parsing the captured data to derive a plurality of key features; querying a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features; generating at least one feature vector based on the plurality of key features and the local historical intrusions'-related data; and providing the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict.

**[0008]** Another embodiment of the present disclosure provides a computer-readable medium including instructions for: acquiring intrusion-related captured data from the at least one captured data source entity node; parsing the captured data to derive a plurality of key features; querying a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features; generating at least one feature vector based on the plurality of key features and the local historical intrusions'-related data; and providing the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict.

**[0009]** Both the foregoing brief overview and the following detailed description provide examples and are explanatory only. Accordingly, the foregoing brief overview and the following detailed description should not be considered to be restrictive. Further, features or variations may be provided in addition to those set forth herein. For example, embodiments may be directed to various feature combinations and sub-combinations described in the detailed description.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0010]** The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate various embodiments of the present disclosure. The drawings contain representations of various trademarks and copyrights owned by the Applicant. In addition, the drawings may contain other marks owned by third parties and are being used for illustrative purposes only. All rights to various trademarks and copyrights represented herein, except those belonging to their respective owners, are vested in and the property of the Applicant. The Applicant retains and reserves all rights in its trademarks and copyrights included herein, and grants permission to reproduce the material only in connection with reproduction of the granted patent and for no other purpose.

**[0011]** Furthermore, the drawings may contain text or captions that may explain certain embodiments of the present disclosure. This text is included for illustrative, non-limiting, explanatory purposes of certain embodiments detailed in the present disclosure. In the drawings:

**[0012]** FIG. **1**A illustrates a network diagram of a system for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data consistent with the present disclosure.

**[0013]** FIG. **1**B illustrates a network diagram of a system for an automated real-time intrusion detection based on

predictive analytics of intrusion-related captured data employing a blockchain consistent with the present disclosure;

**[0014]** FIG. **2** illustrates a network diagram of a system including detailed features of an intrusion detector (ID) node consistent with the present disclosure;

**[0015]** FIG. **3**A illustrates a flowchart of a method for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data consistent with the present disclosure;

**[0016]** FIG. **3**B illustrates a further flowchart of a method for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data consistent with the present disclosure;

**[0017]** FIG. **4** illustrates deployment of a machine learning model for intrusion detection parameters using blockchain assets consistent with the present disclosure;

**[0018]** FIG. **5** illustrates a block diagram of a system including a computing device for performing the method of FIGS. **3**A and **3**B.

## DETAILED DESCRIPTION

**[0019]** As a preliminary matter, it will readily be understood by one having ordinary skill in the relevant art that the present disclosure has broad utility and application. As should be understood, any embodiment may incorporate only one or a plurality of the above-disclosed aspects of the disclosure and may further incorporate only one or a plurality of the above-disclosed features. Furthermore, any embodiment discussed and identified as being "preferred" is considered to be part of a best mode contemplated for carrying out the embodiments of the present disclosure. Other embodiments also may be discussed for additional illustrative purposes in providing a full and enabling disclosure. Moreover, many embodiments, such as adaptations, variations, modifications, and equivalent arrangements, will be implicitly disclosed by the embodiments described herein and fall within the scope of the present disclosure.

**[0020]** Accordingly, while embodiments are described herein in detail in relation to one or more embodiments, it is to be understood that this disclosure is illustrative and exemplary of the present disclosure and are made merely for the purposes of providing a full and enabling disclosure. The detailed disclosure herein of one or more embodiments is not intended, nor is to be construed, to limit the scope of patent protection afforded in any claim of a patent issuing here from, which scope is to be defined by the claims and the equivalents thereof. It is not intended that the scope of patent protection be defined by reading into any claim a limitation found herein that does not explicitly appear in the claim itself.

**[0021]** Thus, for example, any sequence(s) and/or temporal order of steps of various processes or methods that are described herein are illustrative and not restrictive. Accordingly, it should be understood that, although steps of various processes or methods may be shown and described as being in a sequence or temporal order, the steps of any such processes or methods are not limited to being carried out in any particular sequence or order, absent an indication otherwise. Indeed, the steps in such processes or methods generally may be carried out in various different sequences and orders while still falling within the scope of the present invention. Accordingly, it is intended that the scope of patent protection is to be defined by the issued claim(s) rather than the description set forth herein.

**[0022]** Additionally, it is important to note that each term used herein refers to that which an ordinary artisan would understand such a term to mean based on the contextual use of such term herein. To the extent that the meaning of a term used herein—as understood by the ordinary artisan based on the contextual use of such term—differs in any way from any particular dictionary definition of such term, it is intended that the meaning of the term as understood by the ordinary artisan should prevail.

**[0023]** Regarding applicability of 35 U.S.C. § 112, ¶6, no claim element is intended to be read in accordance with this statutory provision unless the explicit phrase "means for" or "step for" is actually used in such claim element, whereupon this statutory provision is intended to apply in the interpretation of such claim element.

**[0024]** Furthermore, it is important to note that, as used herein, "a" and "an" each generally denotes "at least one," but does not exclude a plurality unless the contextual use dictates otherwise. When used herein to join a list of items, "or" denotes "at least one of the items," but does not exclude a plurality of items of the list. Finally, when used herein to join a list of items, "and" denotes "all of the items of the list."

**[0025]** The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description to refer to the same or similar elements. While many embodiments of the disclosure may be described, modifications, adaptations, and other implementations are possible. For example, substitutions, additions, or modifications may be made to the elements illustrated in the drawings, and the methods described herein may be modified by substituting, reordering, or adding stages to the disclosed methods. Accordingly, the following detailed description does not limit the disclosure. Instead, the proper scope of the disclosure is defined by the appended claims. The present disclosure contains headers. It should be understood that these headers are used as references and are not to be construed as limiting upon the subject matter disclosed under the header.

**[0026]** The present disclosure includes many aspects and features. Moreover, while many aspects and features relate to, and are described in, the context of lead-based recommendations, embodiments of the present disclosure are not limited to use only in this context.

**[0027]** The present disclosure provides a system, method and computer-readable medium for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data. In one embodiment, the system overcomes the limitations of existing security systems and methods by employing fine-tuned machine learning models configured to generate intrusion detection parameters that may be used for automated generation of an intrusion verdict. By leveraging the capabilities of the AI and machine learning, the disclosed approach offers a significant improvement over existing solutions discussed above in the background section.

**[0028]** In one embodiment of the present disclosure, the system provides for AI and machine learning (ML)-generated intrusion detection parameters based on analysis of the captured video and/or audio data.

**[0029]** The disclosed embodiments may be platform agnostic. The disclosed system, advantageously, seamlessly integrates with a multitude security interfaces, enabling users to manage intrusion detection alerts and mitigations through a singular universal interface.

**[0030]** In one embodiment, an automated intrusion detection prediction model may be generated to provide for the intrusion detection parameters associated with a current captured potential intrusion-related data. The automated intrusion detection prediction model may use historical intrusion detection data collected at the current security system development location and at third-party security systems of the same type located within the same security network or even located globally. The relevant intrusions' data may include data related to other captured data source entities having the same or similar parameters.

**[0031]** In one disclosed embodiment, the AI/ML technology may be combined with a blockchain technology for secure use of the intrusion detection-related data. A blockchain consensus mechanism may be implemented where multiple nodes or instances of the system validate the intrusion detection verdict for a particular intrusion instance or location. This approach not only provides an additional layer of verification, but also reduces dependency on local unsecure data bases.

**[0032]** In one embodiment, the security personnel entities may be connected to the intrusion detector (ID) node over a blockchain network to achieve a consensus prior to executing a transaction to release the intrusion verdict decision data for the potential intrusion incident based on the intrusion detection parameters produced by the AI/ML module.

**[0033]** In one embodiment, the intrusion detection parameters or recommendations may be produced directly on a granular level based on input-associated digital data according to the AI-based predictive analysis and the intrusion processing/mitigation recommendations (based on predictive intrusion detection parameters). This process includes a transparent recommendations/verdicts mechanism that may be coupled with a secure communications chat channel (implemented over a blockchain network) which supports all clients of the security and intrusion detection service. In one embodiment, the secure chat channel may be implemented using a chat Bot.

**[0034]** FIG. **1**A illustrates a network diagram of a system for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data consistent with the present disclosure.

**[0035]** Referring to FIG. **1**A, the example network **100** includes the intrusion detector (ID) node **102** connected to a cloud server node(s) **105** over a network. The ID node **102** is configured to host an AI/ML module **107**.

**[0036]** As discussed above, the ID node **102** may receive captured video and/or audio data from captured data source entities **101**. The ID node **102** may receive the captured data from the entities **101** that may be associated with an intruder **111** and may be intended for the security entity nodes **113**. In one embodiment, the received captured video and/or audio data may be processed by the ID node **102** using the pre-trained models including large language models (LLMs) to derive a language indicator and to parse out the data of the intruder **111** based on the language indicator metadata. In other words, the key features of the intruder actions may be derived from the intruder-related audio/video data based on the language of the intruder.

**[0037]** The ID node **102** may query a local intrusion database for the historical local intrusions' data **103** associated with the current captured data. The ID node **102** may acquire relevant remote intrusions' data **106** from a remote database residing on a cloud server **105** of a third-party security system(s). The remote intrusions' data **106** may be collected from other security facilities off the current security infrastructure network. The remote intrusions' data **106** may be collected from captured data source entities similar to the source entities **101** based on, for example, capture device types, models, IP addresses, language or locations, URLs, etc. as the local intrusions' data **103** that is associated with the current captured data.

**[0038]** The ID node **102** may generate a feature vector or classifier based on the captured video/audio intrusion-related data and the collected intrusions' data (i.e., pre-stored local data **103** and remote data **106**). The features derived for the classifier may be indicative of potential intruder behavior (including speech).

**[0039]** The ID node **102** may ingest the feature vector/classifier into an AI/ML module **107**. The AI/ML module **107** may generate a predictive model(s) **108** based on the feature vector applied to a neural network to predict intrusion detection parameters for automatically generating intrusion detection verdict or notification to be provided to the security entities **113**. As discussed above, the intrusion detection parameters may be further analyzed by the ID node **102** to map the intrusion detection parameters to variables of the security system that may be updated.

**[0040]** FIG. **1**B illustrates a network diagram of a system for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data employing a blockchain consistent with the present disclosure.

**[0041]** Referring to FIG. **1**B, the example network **100'** includes the intrusion detector (ID) node **102** connected to a cloud server node(s) **105** over a network. The ID node **102** is configured to host an AI/ML module **107**.

**[0042]** The ID node **102** may receive the captured data from the entities **101** that may be associated with an intruder **111** and may be intended for the security entity nodes **113**. In one embodiment, the received captured video and/or audio data may be processed by the ID node **102** using the pre-trained models including large language models (LLMs) to derive a language indicator and to parse out the data of the intruder **111** based on the language indicator metadata. In other words, the key features of the intruder actions may be derived from the intruder-related audio/video data based on the language of the intruder.

**[0043]** The ID node **102** may query a local intrusion database for the historical local intrusions' data **103** associated with the current captured data. The ID node **102** may acquire relevant remote intrusions' data **106** from a remote database residing on a cloud server **105** of a third-party security system(s). The remote intrusions' data **106** may be collected from other security facilities off the current security infrastructure network. The remote intrusions' data **106** may be collected from captured data source entities similar to the source entities **101** based on, for example, capture device types, models, IP addresses, language or locations, URLs, etc. as the local intrusions' data **103** that is associated with the current captured data.

**[0044]** The ID node **102** may generate a feature vector or classifier based on the captured video/audio intrusion-re-

lated data and the collected intrusions' data (i.e., pre-stored local data **103** and remote data **106**). The features derived for the classifier may be indicative of potential intruder behavior (including speech).

**[0045]** The ID node **102** may ingest the feature vector/classifier into an AI/ML module **107**. The AI/ML module **107** may generate a predictive model(s) **108** based on the feature vector applied to a neural network to predict intrusion detection parameters for automatically generating intrusion detection verdict or notification to be provided to the security entities **113**. As discussed above, the intrusion detection parameters may be further analyzed by the ID node **102** to map the intrusion detection parameters to variables of the security system that may be updated.

**[0046]** The AI/ML module **107** may generate a predictive model(s) **108** to predict the intrusion detection parameters in response to the specific relevant pre-stored intrusions'-related data acquired from the blockchain **110** ledger **109**. This way, the current intrusion detection parameters may be predicted based not only on the current intrusion-related captured video/audio data, but also based on the previously collected heuristics and intrusions'-related data associated with the given captured video/audio data and the current intrusion detection parameters derived from the captured data. This way, the most optimal way of handling the intrusion detection and mediation orchestration may be employed and recorded on the blockchain **110** ledger **109** for future references.

**[0047]** FIG. **2** illustrates a network diagram of a system including detailed features of an intrusion detector (ID) node consistent with the present disclosure.

**[0048]** Referring to FIG. **2**, the example network **200** includes the intrusion detector (ID) node **102** connected to the captured data source entity **101** (see FIG. **1**A) to receive the captured video/audio data **201**. The ID node **102** is configured to host an AI/ML module **107**. As discussed above with respect to FIGS. **1**A-B, the ID node **102** may receive the captured data **201** provided by the source entity **101** (FIG. **1**A) and pre-stored intrusions' data retrieved from local and remote third-party databases. As discussed above, the pre-stored intrusions' data may be retrieved from the ledger **109** of the blockchain **110**.

**[0049]** The AI/ML module **107** may generate a predictive model(s) **108** based on the received captured video/audio data **201** provided by the ID node **102**. In one embodiment, the incoming captured data may be normalized and standardized by a data normalization engine (not shown). As discussed above, the AI/ML module **107** may provide predictive outputs data in the form of intrusion detection parameters for an automatic generation of an intrusion detection verdict and/or mitigation recommendation. The ID node **102** may process the predictive outputs data received from the AI/ML module **107** to ultimately generate the security alert or notification to be provided to the security entities (not shown). In one embodiment, the ID node **102** may acquire the captured video/audio data **201** from the source entity(s) continuously or periodically in order to check if new security update/notification need to be generated. In another embodiment, the ID node **102** may continually monitor intrusion-related data and may detect an intrusion detection parameter/variable that deviates from a previously recorded parameter related to the same potential intrusion threat (or from a median reading value) by a margin that exceeds a threshold value pre-set for this particular intrusion detection parameter. Accordingly, once the threshold is met or exceeded by at least one intrusion detection parameter, the ID node **102** may provide the currently acquired intrusion detection parameter to the AI/ML module **107** to generate a list of updated intrusion detection parameters based on the currently acquired intrusion-related data.

**[0050]** While this example describes in detail only one ID node **102**, multiple such nodes may be connected to the network and to the blockchain **110**. It should be understood that the ID node **102** may include additional components and that some of the components described herein may be removed and/or modified without departing from a scope of the ID node **102** disclosed herein. The ID node **102** may be a computing device or a server computer, or the like, and may include a processor **204**, which may be a semiconductor-based microprocessor, a central processing unit (CPU), an application specific integrated circuit (ASIC), a field-programmable gate array (FPGA), and/or another hardware device. Although a single processor **204** is depicted, it should be understood that the ID node **102** may include multiple processors, multiple cores, or the like, without departing from the scope of the ID node **102** system.

**[0051]** The ID node **102** may also include a non-transitory computer readable medium **212** that may have stored thereon machine-readable instructions executable by the processor **204**. Examples of the machine-readable instructions are shown as **214**-**226** and are further discussed below. Examples of the non-transitory computer readable medium **212** may include an electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. For example, the non-transitory computer readable medium **212** may be a Random-Access memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a hard disk, an optical disc, or other type of storage device.

**[0052]** The processor **204** may fetch, decode, and execute the machine-readable instructions **214** to acquire intrusion-related captured data from the at least one captured data source entity node **101** (FIGS. **1**A-B). The processor **204** may fetch, decode, and execute the machine-readable instructions **216** to parse the captured data to derive a plurality of key features. The processor **204** may fetch, decode, and execute the machine-readable instructions **218** to query a local intrusions' database **103** to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features. The processor **204** may fetch, decode, and execute the machine-readable instructions **220** to generate at least one feature vector based on the plurality of key features and the local historical intrusions'-related data.

**[0053]** The processor **204** may fetch, decode, and execute the machine-readable instructions **222** to provide the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict. The processor **204** may fetch, decode, and execute the machine-readable instructions **224** to continuously monitor incoming captured data to determine if at least one variable of the incoming captured data deviates from a value of previous intrusions'-related data by a margin exceeding a pre-set threshold value.

**[0054]** The processor **204** may fetch, decode, and execute the machine-readable instructions **226** to responsive to the at

least one variable of the incoming captured data deviating from the value of previous intrusions'-related data by the margin exceeding the pre-set threshold value, generate an updated feature vector based on the incoming captured data and generate an updated intrusion detection verdict based on at least one updated intrusion detection parameter produced by the predictive model in response to the updated feature vector.

**[0055]** The permissioned blockchain **110** may be configured to use one or more smart contracts that manage transactions for multiple participating nodes and for recording the transactions on the ledger **109**. As discussed above, the ID node **102** system prioritizes using its own heuristic data **103** from local DBs. This ensures a faster, more tailored response to the intrusion-related threats. Local datasets may be recorded on a private (permissioned) blockchain **110**. This provides a tamper-evident log of identified and detected intrusions, enhancing security and transparency. The blockchain log may also contain a trail of how the ML models **108** have been trained and evolved over time, which offers an auditable history of model adjustments and training.

**[0056]** FIG. **3**A illustrates a flowchart of a method for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data consistent with the present disclosure.

**[0057]** Referring to FIG. **3**A, the method **300** may include one or more of the steps described below. FIG. **3**A illustrates a flow chart of an example method executed by the ID node **102** (see FIG. **2**). It should be understood that method **300** depicted in FIG. **3**A may include additional operations and that some of the operations described therein may be removed and/or modified without departing from the scope of the method **300**. The description of the method **300** is also made with reference to the features depicted in FIG. **2** for purposes of illustration. Particularly, the processor **204** of the ID node **102** may execute some or all of the operations included in the method **300**.

**[0058]** With reference to FIG. **3**A, at block **302**, the processor **204** may acquire intrusion-related captured data from the at least one captured data source entity node. At block **304**, the processor **204** may parse the captured data to derive a plurality of key features. At block **306**, the processor **204** may query a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features. At block **308**, the processor **204** may generate at least one feature vector based on the plurality of key features and the local historical intrusions'-related data. At block **310**, the processor **204** may provide the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict. At block **312**, the processor **204** may continuously monitor incoming captured data to determine if at least one variable of the incoming captured data deviates from a value of previous intrusions'-related data by a margin exceeding a pre-set threshold value. At block **314**, the processor **204** may responsive to the at least one variable of the incoming captured data deviating from the value of previous intrusions'-related data by the margin exceeding the pre-set threshold value, generate an updated feature vector based on the incoming captured data and generate an updated intrusion detection verdict based on at least one updated intrusion detection parameter produced by the predictive model in response to the updated feature vector.

**[0059]** FIG. **3**B illustrates a further flowchart of a method for an automated real-time intrusion detection based on predictive analytics of intrusion-related captured data consistent with the present disclosure.

**[0060]** Referring to FIG. **3**B, the method **300'** may include one or more of the steps described below. FIG. **3**B illustrates a flow chart of an example method executed by the ID node **102** (see FIG. **2**). It should be understood that method **300'** depicted in FIG. **3**B may include additional operations and that some of the operations described therein may be removed and/or modified without departing from the scope of the method **300'**. The description of the method **300'** is also made with reference to the features depicted in FIG. **2** for purposes of illustration. Particularly, the processor **204** of the ID node **102** may execute some or all of the operations included in the method **300'**.

**[0061]** With reference to FIG. **3**B, at block **314**, the processor **204** may derive a language indicator from the captured data comprising audio data and to parse the audio data based on the language indicator to derive a plurality of key language features. The language indicator may be included into metadata of the digital data voice packets. At block **316**, the processor **204** may generate the feature vector based on the plurality of key features combined with the key language features and the local historical intrusions'-related data.

**[0062]** At block **318**, the processor **204** may retrieve remote historical intrusions'-related data from at least one remote intrusions' database based on the local historical intrusions'-related data. Note that the remote historical intrusions'-related data is collected at third-party security entities. At block **320**, the processor **204** may generate the at least one feature vector based on the plurality of key features, the local historical intrusions'-related data combined with the remote historical intrusions'-related data.

**[0063]** At block **322**, the processor **204** may parse the captured data to derive a plurality of key features comprising intruder behavioral variables comprising movements and speech parameters. At block **324**, the processor **204** may record the at least one intrusion detection parameter on a blockchain ledger along with the key features retrieved from the captured data.

**[0064]** At block **326**, the processor **204** may retrieve the at least one intrusion detection parameter from the blockchain responsive to a consensus among the ID node and at least one security entity node. At block **328**, the processor **204** may execute a smart contract to record data reflecting generation of the intrusion detection verdict associated with the captured data and at least one security entity node on the blockchain **110** (FIG. **2**) for future audits. At block **330**, the processor **204** may map the at least one intrusion detection parameter to at least one intruder behavior reference rule. The intruder behavior may include motions, gestures, language use, etc.

**[0065]** In one disclosed embodiment, the intrusion detection parameters' model may be generated by the AI/ML module **107** that may use training data sets to improve accuracy of the prediction of the intrusion detection parameters for the security entities **113** (FIG. **1**A). The intrusion detection parameters used in training data sets may be stored in a centralized local database (such as one used for storing local intrusions' data **103** depicted in FIG. **1**A). In one

embodiment, a neural network may be used in the AI/ML module **107** for the intrusion detection parameters' modeling and intrusion verdict predictions or generations.

**[0066]** In another embodiment, the AI/ML module **107** may use a decentralized storage such as a blockchain **110** (see FIG. **1**B) that is a distributed storage system, which includes multiple nodes that communicate with each other. The decentralized storage includes an append-only immutable data structure resembling a distributed ledger capable of maintaining records between mutually untrusted parties. The untrusted parties are referred to herein as peers or peer nodes. Each peer maintains a copy of the parameter(s) records and no single peer can modify the records without a consensus being reached among the distributed peers. For example, the peers **113** and **102** (FIG. **1**B) may execute a consensus protocol to validate blockchain **110** storage transactions, group the storage transactions into blocks, and build a hash chain over the blocks. This process forms the ledger **109** by ordering the storage transactions, as is necessary, for consistency. In various embodiments, a permissioned and/or a permissionless blockchain can be used. In a public or permissionless blockchain, anyone can participate without a specific identity. Public blockchains can involve assets and use consensus based on various protocols such as Proof of Work (PoW). On the other hand, a permissioned blockchain provides secure interactions among a group of entities which share a common goal such as storing lead response parameters for efficient handling of leads, but which do not fully trust one another.

**[0067]** This application utilizes a permissioned (private) blockchain that operates arbitrary, programmable logic, tailored to a decentralized storage scheme and referred to as "smart contracts" or "chaincodes." In some cases, specialized chaincodes may exist for management functions and parameters which are referred to as system chaincodes. The application can further utilize smart contracts that are trusted distributed applications which leverage tamper-proof properties of the blockchain database and an underlying agreement between nodes, which is referred to as an endorsement or endorsement policy. Blockchain transactions associated with this application can be "endorsed" before being committed to the blockchain while transactions, which are not endorsed, are disregarded. An endorsement policy allows chaincodes to specify endorsers for a transaction in the form of a set of peer nodes that are necessary for endorsement. When a client sends the transaction to the peers specified in the endorsement policy, the transaction is executed to validate the transaction. After a validation, the transactions enter an ordering phase in which a consensus protocol is used to produce an ordered sequence of endorsed transactions grouped into blocks.

**[0068]** In the example depicted in FIG. **4**, a host platform **420** (such as the ID node **102**) builds and deploys a machine learning model for predictive monitoring of assets **430**. Here, the host platform **420** may be a cloud platform, an industrial server, a web server, a personal computer, a user device, and the like. Assets **430** can represent intrusion detection-related parameters. The blockchain **110** can be used to significantly improve both a training process **402** of the machine learning model and the intrusion detection parameters' predictive process **405** based on a trained machine learning model. For example, in **402**, rather than requiring a data scientist/engineer or other user to collect the data, historical data (heuristics—i.e., intrusion detection-related data) may be stored by the assets **430** themselves (or through an intermediary, not shown) on the blockchain **110**.

**[0069]** This can significantly reduce the collection time needed by the host platform **420** when performing predictive model training. For example, using smart contracts, data can be directly and reliably transferred straight from its place of origin (e.g., from the ID node **102** or from intrusions' databases **103** and **106** in FIGS. **1**A-**1**B) to the blockchain **110**. By using the blockchain **110** to ensure the security and ownership of the collected data, smart contracts may directly send the data from the assets to the entities that use the data for building a machine learning model. This allows for sharing of data among the assets **430**. The collected data may be stored in the blockchain **110** based on a consensus mechanism. The consensus mechanism pulls in (permissioned nodes) to ensure that the data being recorded is verified and accurate. The data recorded is time-stamped, cryptographically signed, and immutable. It is therefore auditable, transparent, and secure.

**[0070]** Furthermore, training of the machine learning model on the collected data may take rounds of refinement and testing by the host platform **420**. Each round may be based on additional data or data that was not previously considered to help expand the knowledge of the machine learning model. In **402**, the different training and testing steps (and the data associated therewith) may be stored on the blockchain **110** by the host platform **420**. Each refinement of the machine learning model (e.g., changes in variables, weights, etc.) may be stored on the blockchain **110**. This provides verifiable proof of how the model was trained and what data was used to train the model. Furthermore, when the host platform **420** has achieved a finally trained model, the resulting model itself may be stored on the blockchain **110**.

**[0071]** After the model has been trained, it may be deployed to a live environment where it can make intrusion detection-related predictions/decisions based on the execution of the final trained machine learning model using the intrusion detection parameters. In this example, data fed back from the asset **430** may be input into the machine learning model and may be used to make event predictions such as most accurate intrusion detection parameters or verdicts. Determinations made by the execution of the machine learning model (e.g., verdicts or recommendations or threat mitigation orchestration parameters, etc.) at the host platform **420** may be stored on the blockchain **110** to provide auditable/verifiable proof. As one non-limiting example, the machine learning model may predict a future change of a part of the asset **430** (e.g., the intrusion detection parameters). The data behind this decision may be stored by the host platform **420** on the blockchain **110**.

**[0072]** As discussed above, in one embodiment, the features and/or the actions described and/or depicted herein can occur on or with respect to the blockchain **110**. The above embodiments of the present disclosure may be implemented in hardware, in computer-readable instructions executed by a processor, in firmware, or in a combination of the above. The computer computer-readable instructions may be embodied on a computer-readable medium, such as a storage medium. For example, the computer computer-readable instructions may reside in random access memory ("RAM"), flash memory, read-only memory ("ROM"), erasable programmable read-only memory ("EPROM"), electrically erasable programmable read-only memory ("EEPROM"),

registers, hard disk, a removable disk, a compact disk read-only memory ("CD-ROM"), or any other form of storage medium known in the art.

**[0073]** An exemplary storage medium may be coupled to the processor such that the processor may read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an application specific integrated circuit ("ASIC"). In the alternative embodiment, the processor and the storage medium may reside as discrete components. For example, FIG. **5** illustrates an example computing device (e.g., a server node) **500**, which may represent or be integrated in any of the above-described components, etc.

**[0074]** FIG. **5** illustrates a block diagram of a system including computing device **500**. The computing device **500** may comprise, but not be limited to the following:

**[0075]** Mobile computing device, such as, but is not limited to, a laptop, a tablet, a smartphone, a drone, a wearable, an embedded device, a handheld device, an Arduino, an industrial device, or a remotely operable recording device;

**[0076]** A supercomputer, an exa-scale supercomputer, a mainframe, or a quantum computer;

**[0077]** A minicomputer, wherein the minicomputer computing device comprises, but is not limited to, an IBM AS500/iSeries/System I, A DEC VAX/PDP, a HP3000, a Honeywell-Bull DPS, a Texas Instruments TI-990, or a Wang Laboratories VS Series;

**[0078]** A microcomputer, wherein the microcomputer computing device comprises, but is not limited to, a server, wherein a server may be rack mounted, a workstation, an industrial device, a raspberry pi, a desktop, or an embedded device;

**[0079]** The ID node **102** (see FIG. **2**) may be hosted on a centralized server or on a cloud computing service. Although method **300** has been described to be performed by the ID node **102** implemented on a computing device **500**, it should be understood that, in some embodiments, different operations may be performed by a plurality of the computing devices **500** in operative communication at least one network.

**[0080]** Embodiments of the present disclosure may comprise a computing device having a central processing unit (CPU) **520**, a bus **530**, a memory unit **550**, a power supply unit (PSU) **550**, and one or more Input/Output (I/O) units. The CPU **520** coupled to the memory unit **550** and the plurality of I/O units **560** via the bus **530**, all of which are powered by the PSU **550**. It should be understood that, in some embodiments, each disclosed unit may actually be a plurality of such units for the purposes of redundancy, high availability, and/or performance. The combination of the presently disclosed units is configured to perform the stages of any method disclosed herein.

**[0081]** Consistent with an embodiment of the disclosure, the aforementioned CPU **520**, the bus **530**, the memory unit **550**, a PSU **550**, and the plurality of I/O units **560** may be implemented in a computing device, such as computing device **500**. Any suitable combination of hardware, software, or firmware may be used to implement the aforementioned units. For example, the CPU **520**, the bus **530**, and the memory unit **550** may be implemented with computing device **500** or any of other computing devices **500**, in combination with computing device **500**. The aforementioned system, device, and components are examples and other systems, devices, and components may comprise the aforementioned CPU **520**, the bus **530**, the memory unit **550**, consistent with embodiments of the disclosure.

**[0082]** At least one computing device **500** may be embodied as any of the computing elements illustrated in all of the attached figures, including the ID node **102** (FIG. **2**). A computing device **500** does not need to be electronic, nor even have a CPU **520**, nor bus **530**, nor memory unit **550**. The definition of the computing device **500** to a person having ordinary skill in the art is "A device that computes, especially a programmable [usually] electronic machine that performs high-speed mathematical or logical operations or that assembles, stores, correlates, or otherwise processes information." Any device which processes information qualifies as a computing device **500**, especially if the processing is purposeful.

**[0083]** With reference to FIG. **5**, a system consistent with an embodiment of the disclosure may include a computing device, such as computing device **500**. In a basic configuration, computing device **500** may include at least one clock module **510**, at least one CPU **520**, at least one bus **530**, and at least one memory unit **550**, at least one PSU **550**, and at least one I/O **560** module, wherein I/O module may be comprised of, but not limited to a non-volatile storage sub-module **561**, a communication sub-module **562**, a sensors sub-module **563**, and a peripherals sub-module **565**.

**[0084]** A system consistent with an embodiment of the disclosure the computing device **500** may include the clock module **510** may be known to a person having ordinary skill in the art as a clock generator, which produces clock signals. Clock signal is a particular type of signal that oscillates between a high and a low state and is used like a metronome to coordinate actions of digital circuits. Most integrated circuits (ICs) of sufficient complexity use a clock signal in order to synchronize different parts of the circuit, cycling at a rate slower than the worst-case internal propagation delays. The preeminent example of the aforementioned integrated circuit is the CPU **520**, the central component of modern computers, which relies on a clock. The only exceptions are asynchronous circuits such as asynchronous CPUs. The clock **510** can comprise a plurality of embodiments, such as, but not limited to, single-phase clock which transmits all clock signals on effectively 1 wire, two-phase clock which distributes clock signals on two wires, each with non-overlapping pulses, and four-phase clock which distributes clock signals on 5 wires.

**[0085]** Many computing devices **500** use a "clock multiplier" which multiplies a lower frequency external clock to the appropriate clock rate of the CPU **520**. This allows the CPU **520** to operate at a much higher frequency than the rest of the computer, which affords performance gains in situations where the CPU **520** does not need to wait on an external factor (like memory **550** or input/output **560**). Some embodiments of the clock **510** may include dynamic frequency change, where the time between clock edges can vary widely from one edge to the next and back again.

**[0086]** A system consistent with an embodiment of the disclosure the computing device **500** may include the CPU unit **520** comprising at least one CPU Core **521**. A plurality of CPU cores **521** may comprise identical CPU cores **521**, such as, but not limited to, homogeneous multi-core systems. It is also possible for the plurality of CPU cores **521** to comprise different CPU cores **521**, such as, but not limited

to, heterogeneous multi-core systems, big.LITTLE systems and some AMD accelerated processing units (APU). The CPU unit **520** reads and executes program instructions which may be used across many application domains, for example, but not limited to, general purpose computing, embedded computing, network computing, digital signal processing (DSP), and graphics processing (GPU). The CPU unit **520** may run multiple instructions on separate CPU cores **521** at the same time. The CPU unit **520** may be integrated into at least one of a single integrated circuit die and multiple dies in a single chip package. The single integrated circuit die and multiple dies in a single chip package may contain a plurality of other aspects of the computing device **500**, for example, but not limited to, the clock **510**, the CPU **520**, the bus **530**, the memory **550**, and I/O **560**.

**[0087]** The CPU unit **520** may contain cache **522** such as, but not limited to, a level 1 cache, level 2 cache, level 3 cache or combination thereof. The aforementioned cache **522** may or may not be shared amongst a plurality of CPU cores **521**. The cache **522** sharing comprises at least one of message passing and inter-core communication methods may be used for the at least one CPU Core **521** to communicate with the cache **522**. The inter-core communication methods may comprise, but not limited to, bus, ring, two-dimensional mesh, and crossbar. The aforementioned CPU unit **520** may employ symmetric multiprocessing (SMP) design.

**[0088]** The plurality of the aforementioned CPU cores **521** may comprise soft microprocessor cores on a single field programmable gate array (FPGA), such as semiconductor intellectual property cores (IP Core). The plurality of CPU cores **521** architecture may be based on at least one of, but not limited to, Complex instruction set computing (CISC), Zero instruction set computing (ZISC), and Reduced instruction set computing (RISC). At least one of the performance-enhancing methods may be employed by the plurality of the CPU cores **521**, for example, but not limited to Instruction-level parallelism (ILP) such as, but not limited to, superscalar pipelining, and Thread-level parallelism (TLP).

**[0089]** Consistent with the embodiments of the present disclosure, the aforementioned computing device **500** may employ a communication system that transfers data between components inside the aforementioned computing device **500**, and/or the plurality of computing devices **500**. The aforementioned communication system will be known to a person having ordinary skill in the art as a bus **530**. The bus **530** may embody internal and/or external plurality of hardware and software components, for example, but not limited to a wire, optical fiber, communication protocols, and any physical arrangement that provides the same logical function as a parallel electrical bus. The bus **530** may comprise at least one of, but not limited to a parallel bus, wherein the parallel bus carry data words in parallel on multiple wires, and a serial bus, wherein the serial bus carry data in bit-serial form. The bus **530** may embody a plurality of topologies, for example, but not limited to, a multidrop/electrical parallel topology, a daisy chain topology, and a connected by switched hubs, such as USB bus. The bus **530** may comprise a plurality of embodiments, for example, but not limited to:

**[0090]** Internal data bus (data bus) **531**/Memory bus

**[0091]** Control bus **532**

**[0092]** Address bus **533**

**[0093]** System Management Bus (SMBus)

**[0094]** Front-Side-Bus (FSB)

**[0095]** External Bus Interface (EBI)

**[0096]** Local bus

**[0097]** Expansion bus

**[0098]** Lightning bus

**[0099]** Controller Area Network (CAN bus)

**[0100]** Camera Link

**[0101]** ExpressCard

**[0102]** Advanced Technology management Attachment (ATA), including embodiments and derivatives such as, but not limited to, Integrated Drive Electronics (IDE)/Enhanced IDE (EIDE), ATA Packet Interface (ATAPI), Ultra-Direct Memory Access (UDMA), Ultra ATA (UATA)/Parallel ATA (PATA)/Serial ATA (SATA), CompactFlash (CF) interface, Consumer Electronics ATA (CE-ATA)/Fiber Attached Technology Adapted (FATA), Advanced Host Controller Interface (AHCI), SATA Express (SATAe)/External SATA (eSATA), including the powered embodiment eSATAp/Mini-SATA (mSATA), and Next Generation Form Factor (NGFF)/M.2.

**[0103]** Small Computer System Interface (SCSI)/Serial Attached SCSI (SAS)

**[0104]** HyperTransport

**[0105]** InfiniBand

**[0106]** RapidIO

**[0107]** Mobile Industry Processor Interface (MIPI)

**[0108]** Coherent Processor Interface (CAPI)

**[0109]** Plug-n-play

**[0110]** 1-Wire

**[0111]** Peripheral Component Interconnect (PCI), including embodiments such as, but not limited to, Accelerated Graphics Port (AGP), Peripheral Component Interconnect extended (PCI-X), Peripheral Component Interconnect Express (PCI-e) (e.g., PCI Express Mini Card, PCI Express M.2 [Mini PCIe v2], PCI Express External Cabling [ePCIe], and PCI Express OCuLink [Optical Copper{Cu} Link]), Express Card, AdvancedTCA, AMC, Universal IO, Thunderbolt/Mini DisplayPort, Mobile PCIe (M-PCIe), U.2, and Non-Volatile Memory Express (NVMe)/Non-Volatile Memory Host Controller Interface Specification (NVMHCIS).

**[0112]** Industry Standard Architecture (ISA), including embodiments such as, but not limited to Extended ISA (EISA), PC/XT-bus/PC/AT-bus/PC/105 bus (e.g., PC/105-Plus, PCI/105-Express, PCI/105, and PCI-105), and Low Pin Count (LPC).

**[0113]** Music Instrument Digital Interface (MIDI)

**[0114]** Universal Serial Bus (USB), including embodiments such as, but not limited to, Media Transfer Protocol (MTP)/Mobile High-Definition Link (MHL), Device Firmware Upgrade (DFU), wireless USB, Inter-Chip USB, IEEE 1395 Interface/Firewire, Thunderbolt, and extensible Host Controller Interface (xHCI).

**[0115]** Consistent with the embodiments of the present disclosure, the aforementioned computing device **500** may employ hardware integrated circuits that store information for immediate use in the computing device **500**, known to the person having ordinary skill in the art as primary storage or memory **550**. The memory **550** operates at high speed, distinguishing it from the non-volatile storage sub-module **561**, which may be referred to as secondary or tertiary

storage, which provides slow-to-access information but offers higher capacities at lower cost. The contents contained in memory **550**, may be transferred to secondary storage via techniques such as, but not limited to, virtual memory and swap. The memory **550** may be associated with addressable semiconductor memory, such as integrated circuits consisting of silicon-based transistors, used for example as primary storage but also other purposes in the computing device **500**. The memory **550** may comprise a plurality of embodiments, such as, but not limited to volatile memory, non-volatile memory, and semi-volatile memory. It should be understood by a person having ordinary skill in the art that the ensuing are non-limiting examples of the aforementioned memory:

**[0116]** Volatile memory which requires power to maintain stored information, for example, but not limited to, Dynamic Random-Access Memory (DRAM) **551**, Static Random-Access Memory (SRAM) **552**, CPU Cache memory **525**, Advanced Random-Access Memory (A-RAM), and other types of primary storage such as Random-Access Memory (RAM).

**[0117]** Non-volatile memory which can retain stored information even after power is removed, for example, but not limited to, Read-Only Memory (ROM) **553**, Programmable ROM (PROM) **555**, Erasable PROM (EPROM) **555**, Electrically Erasable PROM (EEPROM) **556** (e.g., flash memory and Electrically Alterable PROM [EAPROM]), Mask ROM (MROM), One Time Programmable (OTP) ROM/Write Once Read Many (WORM), Ferroelectric RAM (FeRAM), Parallel Random-Access Machine (PRAM), Split-Transfer Torque RAM (STT-RAM), Silicon Oxime Nitride Oxide Silicon (SONOS), Resistive RAM (RRAM), Nano RAM (NRAM), 3D XPoint, Domain-Wall Memory (DWM), and millipede memory.

**[0118]** Semi-volatile memory which may have some limited non-volatile duration after power is removed but loses data after said duration has passed. Semi-volatile memory provides high performance, durability, and other valuable characteristics typically associated with volatile memory, while providing some benefits of true non-volatile memory. The semi-volatile memory may comprise volatile and non-volatile memory and/or volatile memory with battery to provide power after power is removed. The semi-volatile memory may comprise, but not limited to spin-transfer torque RAM (STT-RAM).

**[0119]** Consistent with the embodiments of the present disclosure, the aforementioned computing device **500** may employ the communication system between an information processing system, such as the computing device **500**, and the outside world, for example, but not limited to, human, environment, and another computing device **500**. The aforementioned communication system will be known to a person having ordinary skill in the art as I/O **560**. The I/O module **560** regulates a plurality of inputs and outputs with regard to the computing device **500**, wherein the inputs are a plurality of signals and data received by the computing device **500**, and the outputs are the plurality of signals and data sent from the computing device **500**. The I/O module **560** interfaces a plurality of hardware, such as, but not limited to, non-volatile storage **561**, communication devices **562**, sensors **563**, and peripherals **565**. The plurality of hardware is used by at least one of, but not limited to, human, environment, and another computing device **500** to communicate with the present computing device **500**. The I/O module **560** may comprise a plurality of forms, for example, but not limited to channel I/O, port mapped I/O, asynchronous I/O, and Direct Memory Access (DMA).

**[0120]** Consistent with the embodiments of the present disclosure, the aforementioned computing device **500** may employ the non-volatile storage sub-module **561**, which may be referred to by a person having ordinary skill in the art as one of secondary storage, external memory, tertiary storage, off-line storage, and auxiliary storage. The non-volatile storage sub-module **561** may not be accessed directly by the CPU **520** without using an intermediate area in the memory **550**. The non-volatile storage sub-module **561** does not lose data when power is removed and may be two orders of magnitude less costly than storage used in memory modules, at the expense of speed and latency. The non-volatile storage sub-module **561** may comprise a plurality of forms, such as, but not limited to, Direct Attached Storage (DAS), Network Attached Storage (NAS), Storage Area Network (SAN), nearline storage, Massive Array of Idle Disks (MAID), Redundant Array of Independent Disks (RAID), device mirroring, off-line storage, and robotic storage. The non-volatile storage sub-module (**561**) may comprise a plurality of embodiments, such as, but not limited to:

**[0121]** Optical storage, for example, but not limited to, Compact Disk (CD) (CD-ROM/CD-R/CD-RW), Digital Versatile Disk (DVD) (DVD-ROM/DVD-R/DVD+R/DVD-RW/DVD+RW/DVD+RW/DVD±R DL/DVD-RAM/HD-DVD), Blu-ray Disk (BD) (BD-ROM/BD-R/BD-RE/BD-R DL/BD-RE DL), and Ultra-Density Optical (UDO).

**[0122]** Semiconductor storage, for example, but not limited to, flash memory, such as, but not limited to, USB flash drive, Memory card, Subscriber Identity Module (SIM) card, Secure Digital (SD) card, Smart Card, CompactFlash (CF) card, Solid-State Drive (SSD) and memristor.

**[0123]** Magnetic storage such as, but not limited to, Hard Disk Drive (HDD), tape drive, carousel memory, and Card Random-Access Memory (CRAM).

**[0124]** Phase-change memory

**[0125]** Holographic data storage such as Holographic Versatile Disk (HVD).

**[0126]** Molecular Memory

**[0127]** Deoxyribonucleic Acid (DNA) digital data storage

**[0128]** Consistent with the embodiments of the present disclosure, the aforementioned computing device **500** may employ the communication sub-module **562** as a subset of the I/O **560**, which may be referred to by a person having ordinary skill in the art as at least one of, but not limited to, computer network, data network, and network. The network allows computing devices **500** to exchange data using connections, which may be known to a person having ordinary skill in the art as data links, between network nodes. The nodes comprise network computer devices **500** that originate, route, and terminate data. The nodes are identified by network addresses and can include a plurality of hosts consistent with the embodiments of a computing device **500**. The aforementioned embodiments include, but not limited to

personal computers, phones, servers, drones, and networking devices such as, but not limited to, hubs, switches, routers, modems, and firewalls.

**[0129]** Two nodes can be networked together, when one computing device **500** is able to exchange information with the other computing device **500**, whether or not they have a direct connection with each other. The communication sub-module **562** supports a plurality of applications and services, such as, but not limited to World Wide Web (WWW), digital video and audio, shared use of application and storage computing devices **500**, printers/scanners/fax machines, email/online chat/instant messaging, remote control, distributed computing, etc. The network may comprise a plurality of transmission mediums, such as, but not limited to conductive wire, fiber optics, and wireless. The network may comprise a plurality of communications protocols to organize network traffic, wherein application-specific communications protocols are layered, may be known to a person having ordinary skill in the art as carried as payload, over other more general communications protocols. The plurality of communications protocols may comprise, but not limited to, IEEE 802, ethernet, Wireless LAN (WLAN/Wi-Fi), Internet Protocol (IP) suite (e.g., TCP/IP, UDP, Internet Protocol version 5 [IPv5], and Internet Protocol version 6 [IPv6]), Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH), Asynchronous Transfer Mode (ATM), and cellular standards (e.g., Global System for Mobile Communications [GSM], General Packet Radio Service [GPRS], Code-Division Multiple Access [CDMA], and Integrated Digital Enhanced Network [IDEN]).

**[0130]** The communication sub-module **562** may comprise a plurality of size, topology, traffic control mechanism and organizational intent. The communication sub-module **562** may comprise a plurality of embodiments, such as, but not limited to:

- **[0131]** Wired communications, such as, but not limited to, coaxial cable, phone lines, twisted pair cables (ethernet), and InfiniBand.
- **[0132]** Wireless communications, such as, but not limited to, communications satellites, cellular systems, radio frequency/spread spectrum technologies, IEEE 802.11 Wi-Fi, Bluetooth, NFC, free-space optical communications, terrestrial microwave, and Infrared (IR) communications. Cellular systems embody technologies such as, but not limited to, 3G, 5G (such as WiMax and LTE), and 5G (short and long wavelength).
- **[0133]** Parallel communications, such as, but not limited to, LPT ports.
- **[0134]** Serial communications, such as, but not limited to, RS-232 and USB.
- **[0135]** Fiber Optic communications, such as, but not limited to, Single-mode optical fiber (SMF) and Multimode optical fiber (MMF).
- **[0136]** Power Line and wireless communications

**[0137]** The aforementioned network may comprise a plurality of layouts, such as, but not limited to, bus network such as ethernet, star network such as Wi-Fi, ring network, mesh network, fully connected network, and tree network. The network can be characterized by its physical capacity or its organizational purpose. Use of the network, including user authorization and access rights, differ accordingly. The characterization may include, but not limited to nanoscale network, Personal Area Network (PAN), Local Area Network (LAN), Home Area Network (HAN), Storage Area Network (SAN), Campus Area Network (CAN), backbone network, Metropolitan Area Network (MAN), Wide Area Network (WAN), enterprise private network, Virtual Private Network (VPN), and Global Area Network (GAN).

**[0138]** Consistent with the embodiments of the present disclosure, the aforementioned computing device **500** may employ the sensors sub-module **563** as a subset of the I/O **560**. The sensors sub-module **563** comprises at least one of the devices, modules, and subsystems whose purpose is to detect events or changes in its environment and send the information to the computing device **500**. Sensors are sensitive to the measured property, are not sensitive to any property not measured, but may be encountered in its application, and do not significantly influence the measured property. The sensors sub-module **563** may comprise a plurality of digital devices and analog devices, wherein if an analog device is used, an Analog to Digital (A-to-D) converter must be employed to interface the said device with the computing device **500**. The sensors may be subject to a plurality of deviations that limit sensor accuracy. The sensors sub-module **563** may comprise a plurality of embodiments, such as, but not limited to, chemical sensors, automotive sensors, acoustic/sound/vibration sensors, electric current/electric potential/magnetic/radio sensors, environmental/weather/moisture/humidity sensors, flow/fluid velocity sensors, ionizing radiation/particle sensors, navigation sensors, position/angle/displacement/distance/speed/acceleration sensors, imaging/optical/light sensors, pressure sensors, force/density/level sensors, thermal/temperature sensors, and proximity/presence sensors. It should be understood by a person having ordinary skill in the art that the ensuing are non-limiting examples of the aforementioned sensors:

**[0139]** Chemical sensors, such as, but not limited to, breathalyzer, carbon dioxide sensor, carbon monoxide/smoke detector, catalytic bead sensor, chemical field-effect transistor, chemiresistor, electrochemical gas sensor, electronic nose, electrolyte-insulator-semiconductor sensor, energy-dispersive X-ray spectroscopy, fluorescent chloride sensors, holographic sensor, hydrocarbon dew point analyzer, hydrogen sensor, hydrogen sulfide sensor, infrared point sensor, ion-selective electrode, nondispersive infrared sensor, microwave chemistry sensor, nitrogen oxide sensor, olfactometer, optode, oxygen sensor, ozone monitor, pellistor, pH glass electrode, potentiometric sensor, redox electrode, zinc oxide nanorod sensor, and biosensors (such as nano-sensors).

**[0140]** Automotive sensors, such as, but not limited to, air flow meter/mass airflow sensor, air-fuel ratio meter, AFR sensor, blind spot monitor, engine coolant/exhaust gas/cylinder head/transmission fluid temperature sensor, hall effect sensor, wheel/automatic transmission/turbine/vehicle speed sensor, airbag sensors, brake fluid/engine crankcase/fuel/oil/tire pressure sensor, camshaft/crankshaft/throttle position sensor, fuel/oil level sensor, knock sensor, light sensor, MAP sensor, oxygen sensor (o2), parking sensor, radar sensor, torque sensor, variable reluctance sensor, and water-in-fuel sensor.

- **[0141]** Acoustic, sound and vibration sensors, such as, but not limited to, microphone, lace sensor (guitar pickup), seismometer, sound locator, geophone, and hydrophone.
- **[0142]** Electric current, electric potential, magnetic, and radio sensors, such as, but not limited to, current sensor,

Daly detector, electroscope, electron multiplier, faraday cup, galvanometer, hall effect sensor, hall probe, magnetic anomaly detector, magnetometer, magnetoresistance, MEMS magnetic field sensor, metal detector, planar hall sensor, radio direction finder, and voltage detector.

**[0143]** Environmental, weather, moisture, and humidity sensors, such as, but not limited to, actinometer, air pollution sensor, bedwetting alarm, ceilometer, dew warning, electrochemical gas sensor, fish counter, frequency domain sensor, gas detector, hook gauge evaporimeter, humistor, hygrometer, leaf sensor, lysimeter, pyranometer, pyrgeometer, psychrometer, rain gauge, rain sensor, seismometers, SNOTEL, snow gauge, soil moisture sensor, stream gauge, and tide gauge.

**[0144]** Flow and fluid velocity sensors, such as, but not limited to, air flow meter, anemometer, flow sensor, gas meter, mass flow sensor, and water meter.

**[0145]** Ionizing radiation and particle sensors, such as, but not limited to, cloud chamber, Geiger counter, Geiger-Muller tube, ionization chamber, neutron detection, proportional counter, scintillation counter, semiconductor detector, and thermos-luminescent dosimeter.

**[0146]** Navigation sensors, such as, but not limited to, air speed indicator, altimeter, attitude indicator, depth gauge, fluxgate compass, gyroscope, inertial navigation system, inertial reference unit, magnetic compass, MHD sensor, ring laser gyroscope, turn coordinator, variometer, vibrating structure gyroscope, and yaw rate sensor.

**[0147]** Position, angle, displacement, distance, speed, and acceleration sensors, such as, but not limited to, accelerometer, displacement sensor, flex sensor, free fall sensor, gravimeter, impact sensor, laser rangefinder, LIDAR, odometer, photoelectric sensor, position sensor such as, but not limited to, GPS or Glonass, angular rate sensor, shock detector, ultrasonic sensor, tilt sensor, tachometer, ultra-wideband radar, variable reluctance sensor, and velocity receiver.

**[0148]** Imaging, optical and light sensors, such as, but not limited to, CMOS sensor, LiDAR, multi-spectral light sensor, colorimeter, contact image sensor, electro-optical sensor, infra-red sensor, kinetic inductance detector, LED as light sensor, light-addressable potentiometric sensor, Nichols radiometer, fiber-optic sensors, optical position sensor, thermopile laser sensor, photodetector, photodiode, photomultiplier tubes, phototransistor, photoelectric sensor, photoionization detector, photomultiplier, photoresistor, photoswitch, phototube, scintillometer, Shack-Hartmann, single-photon avalanche diode, superconducting nanowire single-photon detector, transition edge sensor, visible light photon counter, and wavefront sensor.

**[0149]** Pressure sensors, such as, but not limited to, barograph, barometer, boost gauge, bourdon gauge, hot filament ionization gauge, ionization gauge, McLeod gauge, Oscillating U-tube, permanent downhole gauge, piezometer, Pirani gauge, pressure sensor, pressure gauge, tactile sensor, and time pressure gauge.

**[0150]** Force, Density, and Level sensors, such as, but not limited to, bhangmeter, hydrometer, force gauge or force sensor, level sensor, load cell, magnetic level or nuclear density sensor or strain gauge, piezo capacitive pressure sensor, piezoelectric sensor, torque sensor, and viscometer.

**[0151]** Thermal and temperature sensors, such as, but not limited to, bolometer, bimetallic strip, calorimeter, exhaust gas temperature gauge, flame detection/pyrometer, Gardon gauge, Golay cell, heat flux sensor, microbolometer, microwave radiometer, net radiometer, infrared/quartz/resistance thermometer, silicon bandgap temperature sensor, thermistor, and thermocouple.

**[0152]** Proximity and presence sensors, such as, but not limited to, alarm sensor, doppler radar, motion detector, occupancy sensor, proximity sensor, passive infrared sensor, reed switch, stud finder, triangulation sensor, touch switch, and wired glove.

**[0153]** Consistent with the embodiments of the present disclosure, the aforementioned computing device **500** may employ the peripherals sub-module **562** as a subset of the I/O **560**. The peripheral sub-module **565** comprises ancillary devices used to put information into and get information out of the computing device **500**. There are **3** categories of devices comprising the peripheral sub-module **565**, which exist based on their relationship with the computing device **500**, input devices, output devices, and input/output devices. Input devices send at least one of data and instructions to the computing device **500**. Input devices can be categorized based on, but not limited to:

**[0154]** Modality of input, such as, but not limited to, mechanical motion, audio, visual, and tactile.

**[0155]** Whether the input is discrete, such as but not limited to, pressing a key, or continuous such as, but not limited to position of a mouse.

**[0156]** The number of degrees of freedom involved, such as, but not limited to, two-dimensional mice vs three-dimensional mice used for Computer-Aided Design (CAD) applications.

**[0157]** Output devices provide output from the computing device **500**. Output devices convert electronically generated information into a form that can be presented to humans. Input/output devices that perform both input and output functions. It should be understood by a person having ordinary skill in the art that the ensuing are non-limiting embodiments of the aforementioned peripheral sub-module **565**:

Input Devices

**[0158]** Human Interface Devices (HID), such as, but not limited to, pointing device (e.g., mouse, touchpad, joystick, touchscreen, game controller/gamepad, remote, light pen, light gun, Wii remote, jog dial, shuttle, and knob), keyboard, graphics tablet, digital pen, gesture recognition devices, magnetic ink character recognition, Sip-and-Puff (SNP) device, and Language Acquisition Device (LAD).

**[0159]** High degree of freedom devices, that require up to six degrees of freedom such as, but not limited to, camera gimbals, Cave Automatic Virtual Environment (CAVE), and virtual reality systems.

**[0160]** Video Input devices are used to digitize images or video from the outside world into the computing device **500**. The information can be stored in a multitude of formats depending on the user's requirement. Examples of types of video input devices include, but

not limited to, digital camera, digital camcorder, portable media player, webcam, Microsoft Kinect, image scanner, fingerprint scanner, barcode reader, 3D scanner, laser rangefinder, eye gaze tracker, computed tomography, magnetic resonance imaging, positron emission tomography, medical ultrasonography, TV tuner, and iris scanner.

**[0161]** Audio input devices are used to capture sound. In some cases, an audio output device can be used as an input device, in order to capture produced sound. Audio input devices allow a user to send audio signals to the computing device **500** for at least one of processing, recording, and carrying out commands. Devices such as microphones allow users to speak to the computer in order to record a voice message or navigate software. Aside from recording, audio input devices are also used with speech recognition software. Examples of types of audio input devices include, but not limited to microphone, Musical Instrument Digital Interface (MIDI) devices such as, but not limited to a keyboard, and headset.

**[0162]** Data Acquisition (DAQ) devices convert at least one of analog signals and physical parameters to digital values for processing by the computing device **500**. Examples of DAQ devices may include, but not limited to, Analog to Digital Converter (ADC), data logger, signal conditioning circuitry, multiplexer, and Time to Digital Converter (TDC).

**[0163]** Output Devices may further comprise, but not be limited to:

**[0164]** Display devices, which convert electrical information into visual form, such as, but not limited to, monitor, TV, projector, and Computer Output Microfilm (COM). Display devices can use a plurality of underlying technologies, such as, but not limited to, Cathode-Ray Tube (CRT), Thin-Film Transistor (TFT), Liquid Crystal Display (LCD), Organic Light-Emitting Diode (OLED), MicroLED, E Ink Display (ePaper) and Refreshable Braille Display (Braille Terminal).

**[0165]** Printers, such as, but not limited to, inkjet printers, laser printers, 3D printers, solid ink printers and plotters.

**[0166]** Audio and Video (AV) devices, such as, but not limited to, speakers, headphones, amplifiers and lights, which include lamps, strobes, DJ lighting, stage lighting, architectural lighting, special effect lighting, and lasers.

**[0167]** Other devices such as Digital to Analog Converter (DAC)

**[0168]** Input/Output Devices may further comprise, but not be limited to, touchscreens, networking device (e.g., devices disclosed in network **562** sub-module), data storage device (non-volatile storage **561**), facsimile (FAX), and graphics/sound cards.

**[0169]** All rights including copyrights in the code included herein are vested in and the property of the Applicant. The Applicant retains and reserves all rights in the code included herein, and grants permission to reproduce the material only in connection with reproduction of the granted patent and for no other purpose.

**[0170]** While the specification includes examples, the disclosure's scope is indicated by the following claims. Furthermore, while the specification has been described in language specific to structural features and/or methodological acts, the claims are not limited to the features or acts described above. Rather, the specific features and acts described above are disclosed as examples for embodiments of the disclosure.

**[0171]** Insofar as the description above and the accompanying drawing disclose any additional subject matter that is not within the scope of the claims below, the disclosures are not dedicated to the public and the right to file one or more applications to claims such additional disclosures is reserved.

The following is claimed:

**1**. A system for an automated real-time intrusion detection based on predictive analytics of intrusion-related data, comprising:

a processor of an intrusion detection (ID) node configured to host a machine learning (ML) module and connected to at least one captured data source entity node over a network; and

a memory on which are stored machine-readable instructions that when executed by the processor, cause the processor to:

acquire intrusion-related captured data from the at least one captured data source entity node;

parse the captured data to derive a plurality of key features;

query a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features;

generate at least one feature vector based on the plurality of key features and the local historical intrusions'-related data;

provide the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict;

continuously monitor incoming captured data to determine if at least one variable of the incoming captured data deviates from a value of previous intrusions'-related data by a margin exceeding a pre-set threshold value; and

responsive to the at least one variable of the incoming captured data deviating from the value of previous intrusions'-related data by the margin exceeding the pre-set threshold value, generate an updated feature vector based on the incoming captured data and generate an updated intrusion detection verdict based on at least one updated intrusion detection parameter produced by the predictive model in response to the updated feature vector.

**2**. The system of claim **1**, wherein the instructions further cause the processor to derive a language indicator from the captured data comprising audio data and to parse the audio data based on the language indicator to derive a plurality of key language features.

**3**. The system of claim **2**, wherein the instructions further cause the processor to generate the feature vector based on the plurality of key features combined with the key language features and the local historical intrusions'-related data.

**4**. The system of claim **1**, wherein the instructions further cause the processor to retrieve remote historical intrusions'-related data from at least one remote intrusions' database based on the local historical intrusions'-related data, wherein the remote historical intrusions'-related data is collected at third-party security entities.

5. The system of claim 4, wherein the instructions further cause the processor to generate the at least one feature vector based on the plurality of key features, the local historical intrusions'-related data combined with the remote historical intrusions'-related data.

6. The system of claim 1, wherein the instructions further cause the processor to parse the captured data to derive a plurality of key features comprising intruder behavioral variables comprising movements and speech parameters.

7. The system of claim 1, wherein the instructions further cause the processor to record the at least one intrusion detection parameter on a blockchain ledger along with the key features retrieved from the captured data.

8. The system of claim 7, wherein the instructions further cause the processor to retrieve the at least one intrusion detection parameter from the blockchain responsive to a consensus among the ID node and at least one security entity node.

9. The system of claim 8, wherein the instructions further cause the processor to execute a smart contract to record data reflecting generation of the intrusion detection verdict associated with the captured data and at least one security entity node on the blockchain for future audits.

10. The system of claim 1, wherein the instructions further cause the processor to map the at least one intrusion detection parameter to at least one intruder behavior reference rule.

11. A method for an automated real-time intrusion detection based on predictive analytics of intrusion-related data, comprising:

acquiring, by an intrusion detector (ID) node configured to host a machine learning (ML) module, intrusion-related captured data from at least one captured data source entity node;

parsing, by the ID node, the captured data to derive a plurality of key features;

querying, by the ID node, a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features;

generating, by the ID node, at least one feature vector based on the plurality of key features and the local historical intrusions'-related data;

providing, by the ID node, the at least one feature vector to the ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict;

continuously monitoring, by the ID node, incoming captured data to determine if at least one variable of the incoming captured data deviates from a value of previous intrusions'-related data by a margin exceeding a pre-set threshold value; and

responsive to the at least one variable of the incoming captured data deviating from the value of previous intrusions'-related data by the margin exceeding the pre-set threshold value, generating an updated feature vector based on the incoming captured data and generate an updated intrusion detection verdict based on at least one updated intrusion detection parameter produced by the predictive model in response to the updated feature vector.

12. The method of claim 11, further comprising deriving a language indicator from the captured data comprising audio data, parsing the audio data based on the language indicator to derive a plurality of key language features and generating the feature vector based on the plurality of key features combined with the key language features and the local historical intrusions'-related data.

13. The method of claim 11, further comprising executing a smart contract to record data reflecting generation of the intrusion detection verdict associated with the captured data and at least one security entity node on the blockchain for future audits.

14. A non-transitory computer-readable medium comprising instructions, that when read by a processor, cause the processor to perform:

acquiring intrusion-related captured data from at least one captured data source entity node;

parsing the captured data to derive a plurality of key features;

querying a local intrusions' database to retrieve local historical intrusions'-related data associated with previous intrusion detection parameters based on the plurality of key features;

generating at least one feature vector based on the plurality of key features and the local historical intrusions'-related data; and

providing the at least one feature vector to a machine learning module ML module for generating a predictive model configured to produce at least one intrusion detection parameter for generation of an intrusion detection verdict;

continuously monitoring incoming captured data to determine if at least one variable of the incoming captured data deviates from a value of previous intrusions'-related data by a margin exceeding a pre-set threshold value; and

responsive to the at least one variable of the incoming captured data deviating from the value of previous intrusions'-related data by the margin exceeding the pre-set threshold value, generating an updated feature vector based on the incoming captured data and generate an updated intrusion detection verdict based on at least one updated intrusion detection parameter produced by the predictive model in response to the updated feature vector.

15. The non-transitory computer readable medium of claim 14, further comprising deriving a language indicator from the captured data comprising audio data, parsing the audio data based on the language indicator to derive a plurality of key language features and generating the feature vector based on the plurality of key features combined with the key language features and the local historical intrusions'-related data.

16. The non-transitory computer readable medium of claim 14, further comprising executing a smart contract to record data reflecting generation of the intrusion detection verdict associated with the captured data and at least one security entity node on the blockchain for future audits.

17. The non-transitory computer readable medium of claim 14, further comprising mapping the at least one intrusion detection parameter to at least one intruder behavior reference rule.

18. The non-transitory computer readable medium of claim 14, further comprising retrieving remote historical intrusions'-related data from at least one remote intrusions' database based on the local historical intrusions'-related

data, wherein the remote historical intrusions'-related data is collected at third-party security entities.

**19**. The non-transitory computer readable medium of claim **18**, further comprising generating the at least one feature vector based on the plurality of key features, the local historical intrusions'-related data combined with the remote historical intrusions'-related data.

**20**. The non-transitory computer readable medium of claim **14**, further comprising recording the at least one intrusion detection parameter on a blockchain ledger along with the key features retrieved from the captured data.

* * * * *