feedback information to the secure intelligent agent 103. Additionally, the functions of the specialized dedicated hardware processors of the secure intelligent operational agent 104 may be distributed among many hardware processors or integrated or consolidated into fewer hardware processors.

[0019] The secure intelligent operational agent 104, in some exemplary embodiments, receives massive amounts of secure digital data from the secure cloud based specialized intelligent historical agent 101 in an extremely short period of time. Such secure digital data may be received by the secure intelligent operational agent 104 as triggered by the secure intelligent operational agent 104 determining a digital data element, determining a list based upon the determined digital data element and requesting members of the list (comprising secure digital data) from the secure cloud based specialized intelligent historical agent 101. Accordingly, bandwidth and processing between the secure intelligent operational agent 104 and the secure cloud based specialized intelligent historical agent 101 maybe optimized through dedicated hardware, including processors, wired and/or wireless channels, circuits, switches, firewalls, data compressors, data scrubbers and the like.

[0020] The data transmissions to and from the secure intelligent operational agent 104, according to various exemplary embodiments, are highly valuable and/or sensitive. Accordingly, numerous measures may be taken including use of hardware based encryption and/or decryption of the transmissions, use of a dedicated wired and/or wireless channels for transmissions, use of specialized hardware circuitry and/or switches for transmissions.

[0021] In a further exemplary embodiment, the data transmissions to and from the secure intelligent operational agent 104 may comprise actual or true transmissions and decoy or false transmissions to deter or throw-off any outside agency intercepting, recording, observing or otherwise interfering with such transmissions.

[0032] A neural network may comprise a neural network base and its underlying algorithms in tandem with a neural network usable data set. The neural network usable data set may function as a data feeder for the neural network base to calculate and/or otherwise interact with.

[0033] In various exemplary embodiments, feeding of a data point may be performed by the neural network iteratively requesting to process the next data point in the usable data set.

[0034] Data points, according to many exemplary embodiments, may include but are not limited to performance data and historical data that the neuro network has access to as part of its useable data set.

[0035] Also shown in FIG. 1 are optional data transfer corridors 106A-106D. According to further exemplary embodiments, one or more optional data transfer corridors may be installed at certain locations in the intelligent networked architecture. The optional data transfer corridors are hardware-based secure, high speed data transfer corridors, each having specialized processors and switches. The optional data transfer corridors facilitate the unilateral or bilateral transfer of massive amounts of data especially in those situations where the extremely quick transfer of massive amounts of data is required.

[0036] FIGS. 2A-2B represent a flowchart of an exemplary method 200 for intelligent networked architecture, processing and execution.

[0037] At step 201, a secure intelligent agent determines a first digital data element. In some exemplary embodiments, the first digital data element may include a resource. In further exemplary embodiments, other factors may represent the first digital data element.

[0038] At step 202, the secure intelligent agent determines a second digital data element. In some exemplary embodiments, the second digital data element is a

period. In further exemplary embodiments, other factors may represent the fourth digital data element. This step may also be performed by the hardware based random number generator machine, either as a separate step or as part of optional step 204.

[0044] At step 207, the intelligent agent directs (via its circuitry over a secure network) the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents that may be load balanced to send secure digital data for the first, second, third and fourth digital data elements to a plurality of secure cloud based specialized insight servers and/or virtual insight machines. In some embodiments, security of such activity may be established through a virtual private network ("VPN").

[0045] According to many exemplary embodiments, the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents function in parallel to divide the data to be transferred to the plurality of cloud based specialized insight servers and/or virtual insight machines, copy the secure digital data, proportion the copied secure digital data among a series of secure channels and transmit the data to the plurality of specialized insight servers and/or virtual insight machines.

[0046] At step 208, the intelligent agent determines a fifth digital data element. According to various exemplary embodiments, a performance metric is the fifth digital data element. In further exemplary embodiments, other factors may represent the fifth digital data element. This step may also be performed by the hardware based random number generator machine, either as a separate step or as part of optional step 204.

[0047] At step 209, the intelligent agent determines a sixth digital data element. According to various exemplary embodiments, a condition is the sixth digital data element. In further exemplary embodiments, other factors may represent the sixth

digital data element. This step may also be performed by the hardware based random number generator machine, either as a separate step or as part of optional step 204.

[0048] At step 210, the intelligent agent determines a seventh digital data element. According to various exemplary embodiments, an allocation amount is the seventh digital data element. In further exemplary embodiments, other factors may represent the seventh digital data element.

[0049] At step 211, the intelligent agent directs (via its circuitry over a secure network) the secure cloud of specialized insight servers and/or virtual insight machines to transform the secure digital data for the first, second, third and fourth digital data elements pursuant to the fifth, sixth and seventh digital data elements.

[0050] According to many exemplary embodiments, data transformation is optimized by one way secure digital data delivery across expandable computing resources. This includes not transmitting back the secure digital data for the first through seventh digital data elements to their origins. Instead, the fast destruction of this data is performed so as to speed up the transformation of a subsequent run.

[0051] At step 212, the intelligent agent determines an eighth digital data element. According to one exemplary embodiment, a percentage representing a percentage of the transformed results that should be selected is the eighth digital data element. In further exemplary embodiments, other factors may represent the eighth digital data element.

[0052] At optional step 213, the intelligent agent determines a ninth digital data element. According to one exemplary embodiment, an upper and/or lower outlier factor, representing a particular percentage of the highest and/or lowest of the transformation results to remove before performing step 212 is the ninth digital data element.

digital data that resides in the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents. In comparison to systems to where both data sets reside in the same machine, the intelligent operational agent can more quickly match a strategy to a current condition and make a deployment.

[0056] According to further exemplary embodiments, a scrubbed situational deployment trigger such as exemplary scrubbed situational deployment trigger 107 (FIG. 1) is the transformed product produced at step 214. As described herein, most if not all of the secure digital data employed to generate the scrubbed situational deployment trigger 107 has been scrubbed by the clearing of the secure digital data from the secure cloud based specialized insight servers and/or the virtual insight machines 105 (FIG. 1). The scrubbed situational deployment trigger 107 comprises the names/identifiers of strategies determined at step 214 so that the strategies may be quickly recalled from the secure cloud based specialized intelligent historical agent 101 (FIG. 1) upon the occurrence of a particular current condition. In many exemplary embodiments, the scrubbed situational deployment trigger 107 also comprises digital data elements one through nine. After it is generated, the scrubbed situational deployment trigger 107 is transmitted from the secure cloud based specialized insight servers and/or the virtual insight machines 105 to the secure intelligent operational agent 104. As described in connection with step 215, upon the occurrence of a particular current condition (e.g. the tenth digital data element) that is the same as or approximates the condition for which the scrubbed situational deployment trigger 107 was produced (e.g. the six digital data element), the scrubbed situational deployment trigger 107 will cause the transmission of the named/identified strategies from the secure cloud based specialized intelligent historical agent 101 for execution at the activity server 102 (FIG. 1).

[0057] At step 215 the intelligent operational agent determines a tenth digital data element and executes a test deployment strategy.

digital data element is a look back period. Look back periods may include without limitation the last two seasons, last month, last ten years, last thirty years, last two years, or last 5000 patients, etc. The fifth digital data element is a performance metric. Performance metrics may include, without limitation, yards per carry, hours billed, risk adjusted performance, miles per gallon, disease free months. The sixth digital data element is a condition. Conditions may include, without limitation, snow, recession, bear market, record (high or low) gas prices, lung adenocarcinoma, or a drought. The seventh digital data element is an allocation amount. Allocation amounts may include, without limitation, number of players, workers, dollars, vehicles, drugs, computing resources or contracts. The eighth digital data element is a percentage for selection. Percentages for selection may include, without limitation, top 10%, top 2%, top 1%, top 4%, or top 30%. The ninth digital data element is an outlier percentage to remove from a top and/or bottom of a data set before executing selection pursuant to the eighth digital data element. Outlier percentages may include, without limitation, top 1% and bottom 1%, top 5% and bottom 1%, not applicable or doesn't apply ("N/A"), top 2% or bottom 10%. The tenth digital data element is a current condition. Current conditions may include, without limitation, snow, recession, bear market, record (high or low) gas prices, lung adenocarcinoma, or a drought.

[0063] FIGS. 4A-4B represent an exemplary method 400 of the application of intelligent networked architecture, processing and execution.

[0064] At step 401, a secure intelligent agent determines a first digital data element. In some exemplary embodiments, the first digital data element may include a resource. For example, resources may include metals, energies, currencies, softs, grains, meats, and interest rates.

[0065] Here, for example, equities may be selected as the first digital data element.

[0083] At step 407, the intelligent agent directs (via its circuitry over a secure network) the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents that may be load balanced to send secure digital data for the first, second, third and fourth digital data elements to a plurality of secure cloud based specialized insight servers and/or virtual insight machines. In some embodiments, security of such activity may be established through a virtual private network ("VPN").

[0084] Here, for example, the past 10 years of transaction data (on a transaction by transaction basis) for each of the bots that trade GM as well as the past 10 years of market price data (on a minute by minute basis) is the secure digital data for the first, second, third and fourth digital data elements that the intelligent agent determines and directs the transmission between cloud resources.

[0085] Here, for example, transaction information for the 160,000 bots and copies of the bots are transmitted. Load balancing of the servers may also be performed as directed by the intelligent agent or another specialized machine.

[0086] At step 408, the intelligent agent determines a fifth digital data element. According to various exemplary embodiments, a performance metric is the fifth digital data element. This step may also be performed by the hardware based random number generation machine, either as a separate step or as part of optional step 404. Here, for example, risk adjusted performance is determined by the intelligent agent as the fifth digital data element.

[0087] According to some exemplary embodiments, bots or trading algorithms may be grouped together in each market by each performance metric. A group of bots filtered by average drawdown is focused on risk/safety. A group of bots filtered by MAR is focused on risk-adjusted returns since risk now taken into account (unlike CAGR).

on such steps as the determination of strategy and execution of trades. For example, in addition to an optimal strategy, non-optimal strategies may purposely be added in the same string or digital data environment of the optimal strategy to confuse any unwanted hackers intercepting such information. As another example, in addition to a desired trade to be executed, undesired trades may purposely be added in the same string or digital data environment of the desired trade to confuse any unwanted hackers intercepting such information. Further, the desired trade may receive funding for execution, whereas the undesired trades may not receive funding for execution.

[00105] FIGS. 5A-5B represent another example of the application of intelligent networked architecture, processing and execution.

[00106] At step 501, a secure intelligent agent determines a first digital data element. In some exemplary embodiments, the first digital data element may include a resource.

[00107] Here, the resource is a large collection of biological drugs.

[00108] At step 502, the secure intelligent agent determines a second digital data element. In some exemplary embodiments, the second digital data element is a segment for the resource.

[00109] Here, the segment for the resource are monoclonal antibody ("Mab") based biological drugs.

[00110] At step 503, the secure intelligent agent determines a third digital data element. In various exemplary embodiments, the third digital data element is an item on the segment.

[00111] Here, the item on the segment are monoclonal antibody ("Mab") based drugs for treating cancer.

[00112] At optional step 504, steps 501 through 503 (i.e. intelligent determination of the first, second and/or third digital data elements) may be performed by a

digital data element. In further exemplary embodiments, other factors may represent the seventh digital data element.

[00125] Here, the allocation amount is the amount of computing resources that may be used in performing step 511.

[00126] At step 511, the intelligent agent directs (via its circuitry over a secure network) the secure cloud of specialized insight servers and/or virtual insight machines to transform the secure digital data for the first, second, third and fourth digital data elements pursuant to the fifth, sixth and seventh digital data elements.

[00127] According to many exemplary embodiments, data transformation is optimized by one way secure digital data delivery across expandable computing resources. This includes not transmitting back the secure digital data for the first through sixth digital data elements to their origins. Instead, the fast destruction of this data is performed so as to speed up the transformation of a subsequent run.

[00128] According to exemplary embodiments, the secure cloud of specialized insight servers and/or virtual insight machines analyze the secure digital data for the last 50,000 patients treated with monoclonal antibody based biological drugs for adenocarcinoma of the lung, with a particular gene sequence to determine the drug(s) that maximized disease free months.

[00129] Additionally, the genomic data of this patient population will be analyzed for commonalities and differences, especially as it relates to the specific treatment(s) received. This includes analyzing gene sequences from lung tissue biopsies, taking into account cell types. Additionally, determinations may be made about "cocktail" treatments where based on the analysis, a plurality of monoclonal antibody based biological drugs would appear to have additive impact with respect to the particular performance metric selected. Such cocktail treatments may also include suggested treatments based on information obtained by analyzing the medical histories, such as dietary and exercise patterns.

and/or virtual intelligent historical agents was copied before the transmission, this data still resides in the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents. The scrubbed names and/or identifiers is transformed into a list that may also include specification of digital data elements one through eight. The list is then securely transmitted to an intelligent operational agent.

[00134] The functioning of the intelligent operational agent, according to various exemplary embodiments, is enhanced by being focused on matching strategies to current conditions by being focused on such and not being hindered by having to consume time and resources in managing and processing the corresponding secure digital data that resides in the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents. In comparison to systems to where both data sets reside in the same machine, the intelligent operational agent can more quickly match a strategy to a current condition and make a deployment.

[00135] According to further exemplary embodiments, a scrubbed situational deployment trigger such as exemplary scrubbed situational deployment trigger 107 (FIG. 1) is the transformed product produced at step 514. As described herein, most if not all of the secure digital data employed to generate the scrubbed situational deployment trigger 107 has been scrubbed by the clearing of the secure digital data from the secure cloud based specialized insight servers and/or the virtual insight machines 105 (FIG. 1). The scrubbed situational deployment trigger 107 comprises the names/identifiers of strategies determined at step 514 so that the strategies may be quickly recalled from the secure cloud based specialized intelligent historical agent 101 (FIG. 1) upon the occurrence of a particular current condition. In many exemplary embodiments, the scrubbed situational deployment trigger 107 also comprises digital data elements one through nine. After it is generated, the scrubbed situational deployment trigger 107 is transmitted from the secure cloud based

specialized insight servers and/or the virtual insight machines 105 to the secure intelligent operational agent 104. As described in connection with step 515, upon the occurrence of a particular current condition (e.g. the tenth digital data element) that is the same as or approximates the condition for which the scrubbed situational deployment trigger 107 was produced (e.g. the six digital data element), the scrubbed situational deployment trigger 107 will cause the transmission of the named/identified strategies from the secure cloud based specialized intelligent historical agent 101 for execution at the activity server 102 (FIG. 1).

[00136] According to one exemplary embodiment, the further transformation produces a list of names and/or identifiers of optimal treatment strategies.

[00137] The scrubbed situational deployment trigger 107 comprises the names/identifiers of strategies determined at step 514 (e.g. monoclonal antibody ("Mab" based drugs) so that the associated information may be quickly recalled from the secure cloud based specialized intelligent historical agent 101 (FIG. 1) upon the occurrence of a particular current condition.

[00138] At step 515 the intelligent operational agent determines a tenth digital data element and executes a deployment strategy.

[00139] According to various exemplary embodiments, the tenth digital data element is a current condition. In some embodiments, the current condition may be similar to the sixth digital data element, a condition. Accordingly, the intelligent operational agent may access the list of names and/or identifiers corresponding to the sixth digital data element. Upon receiving a request from the intelligent operational agent, the secure cloud of specialized intelligent historical agents and/or virtual historical intelligent agents will function in parallel to send the secure digital data to the intelligent operational agent. The intelligent operational agent will then deploy the transferred data in a setting such as that exemplified by the activity server 102 (FIG. 1).

[00140] According to further exemplary embodiments, the intelligent operational agent may transmit to the activity server one or more decoy strings in the same string to confuse any unwanted hackers attempting to intercept such information. The activity server would only actually deploy the actual strategy.

[00141] Here, for example, the activity server may be connected to a gene sequencer at a cancer treatment center. The sequencer may be sequencing the DNA of a lung cancer biopsy tissue specimen. The scrubbed situational deployment trigger 107 at the secure intelligent operational agent 104 will be deployed based upon the occurrence of a particular current condition (e.g. the tenth digital data element being adenocarcinoma of the lung, with a particular gene sequence) that is the same as or approximates the condition for which the scrubbed situational deployment trigger 107 was produced (e.g. the six digital data element being adenocarcinoma of the lung, with a particular gene sequence), the scrubbed situational deployment trigger 107 causing the transmission of the associated information (e.g. genomic data and medical histories) from the secure cloud based specialized intelligent historical agent 101 for execution at the activity server 102 (FIG. 1) in the form of generating a personalized treatment plan.

[00142] While various embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation. The descriptions are not intended to limit the scope of the technology to the particular forms set forth herein. Thus, the breadth and scope of a preferred embodiment should not be limited by any of the above-described exemplary embodiments. It should be understood that the above description is illustrative and not restrictive. To the contrary, the present descriptions are intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the technology as defined by the appended claims and otherwise appreciated by one of ordinary skill in the art. The scope of the technology should,

CLAIMS

What is claimed:

1. An intelligent networked architecture comprising:

an intelligent agent having a specialized hardware processor, the intelligent agent configured to automatically determine a first, a second, a third, a fourth, a fifth, a sixth, a seventh and an eighth digital data element, the intelligent agent configured to utilize a random number generator machine to optimize variables for processing runs;

a secure cloud of a plurality of specialized intelligent historical agents, each of the plurality of specialized intelligent historical agents having a specialized hardware processor and a memory further comprising secure digital data corresponding to the first, the second, the third and the fourth digital data elements, the plurality of specialized intelligent historical agents configured to copy and divide the secure digital data into parallel segments based on the optimized variables;

a plurality of secure cloud based specialized insight servers, each of the plurality of secure cloud based specialized insight servers having a specialized hardware processor, the plurality of secure cloud based specialized insight servers configured to receive from the secure cloud of the plurality of specialized intelligent historical agents the secure digital data corresponding to the first, the second, the third and the fourth digital data elements and configured to transform the secure digital data corresponding to the first, the second, the third and the fourth digital data elements as directed by the fifth, the sixth, the seventh and the

eighth digital data elements into a scrubbed situational deployment trigger, the scrubbed situational deployment trigger being a reduced size version of the secure digital data, wherein a complete version of the secure digital data is retained by the plurality of specialized intelligent historical agents; and

an intelligent operational agent having a specialized hardware processor, the intelligent operational agent configured to receive the scrubbed situational deployment trigger and cause the plurality of specialized intelligent historical agents to transmit the complete version of the secure digital data to the plurality of secure cloud based specialized insight servers.

2. The intelligent networked architecture of claim 1, wherein the intelligent operational agent is configured to determine a tenth digital data element, and configured to deploy the scrubbed situational deployment trigger based on the tenth digital data element.

3. The intelligent networked architecture of claim 1, further comprising a load balancer having a specialized hardware processor, the load balancer configured to distribute the secure digital data received by the plurality of secure cloud based specialized insight servers.

4. The intelligent networked architecture of claim 3, wherein the load balancer is further configured to distribute processing of the secure digital data received by the plurality of secure cloud based specialized insight servers.

5. The intelligent networked architecture of claim 1, wherein the first digital data element, the second digital data element, and the third digital data element are randomly generated by a hardware based random number generator.

6. The intelligent networked architecture of claim 1, wherein the first digital data element, the second digital data element, the third digital data element and the fourth digital data element are randomly generated by a hardware based random number generator.

7. The intelligent networked architecture of claim 1, wherein the first digital data element is a resource.

8. The intelligent networked architecture of claim 1, wherein the second digital data element is a resource segment.

9. The intelligent networked architecture of claim 8, wherein the third digital data element is an item on the resource segment.

10. The intelligent networked architecture of claim 1, wherein the fourth digital data element is a look back period.

11. The intelligent networked architecture of claim 1, wherein the fifth digital data element is a performance metric.

12. The intelligent networked architecture of claim 1, wherein the sixth digital data element is a condition.

13. The intelligent networked architecture of claim 1, wherein the seventh digital data element is an allocation amount.

14. The intelligent networked architecture of claim 1, wherein the eighth digital data element is a percentage for selection.

15. The intelligent networked architecture of claim 14, wherein a ninth digital data element is a percentage to remove from a population before executing the percentage for the selection.

16. The intelligent networked architecture of claim 1, wherein a tenth digital data element is a current condition.

17. A system, comprising:

a secure intelligent agent comprising a random number generator machine, the secure intelligent agent being configured to:

receive a first set comprising a plurality of digital data elements including a first, a second, a third, and a fourth digital data element from one of a plurality of specialized intelligent historical agents, the plurality of digital data elements being associated with a time value;

utilize the random number generator machine to optimize variables for processing runs; and

instruct the plurality of specialized intelligent historical agents to:

copy and divide secure digital data for the first set into parallel segments based on the optimized variables;

retain the secure digital data for the first set;

transmit a copied version of the secure digital data for the first set to a plurality of insight servers over secure channels;

wherein the plurality of insight servers are configured to:

transform the copied version of the secure digital data for the first set using a second set comprising additional digital data elements including a fifth, a sixth, a seventh and an eighth digital data element to generate a massive amount of data output; and

scrub the massive amount of data output to:

reduce a size of the massive amount of data output; and generate a scrubbed situational deployment trigger that is a reduced size version of the copied version of the secure digital data for the first set, the scrubbed situational deployment trigger being provisioned to a secure intelligent operational agent.

18. The system according to claim 17, wherein the plurality of specialized intelligent historical agents are configured to perform rapid destruction of the first set and the second set to increase a speed of each subsequent processing run of the processing runs.

19. The system according to claim 17, further comprising a plurality of hardware-based secure, high data transfer corridors, each having specialized processors and switches to facilitate unilateral or bilateral transfer of the secure digital data between any of the secure intelligent agent, the plurality of specialized intelligent historical agents, and the plurality of insight servers.

20. The system according to claim 17, wherein the plurality of insight servers transmits the scrubbed situational deployment trigger to the secure intelligent operational agent, the secure intelligent operational agent being configured to transmit the secure digital data retained by the plurality of specialized intelligent historical agents to the plurality of insight servers when at least one condition specified in the scrubbed situational deployment trigger is met.