

**SECURE INTELLIGENT NETWORKED ARCHITECTURE, PROCESSING AND
EXECUTION**

FIELD OF THE TECHNOLOGY

[0001] The embodiments disclosed herein are related to secure intelligent networked architecture, processing and execution.

SUMMARY

[0002] Provided herein are exemplary systems and methods for secure intelligent networked architecture, processing and execution.

[0003] Exemplary embodiments include 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; a secure cloud of a plurality of specialized intelligent historical agents, each historical agent 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; a plurality of secure cloud based specialized insight servers, each insight server 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 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; and an intelligent operational agent having a specialized hardware processor, the intelligent operational agent configured to receive the scrubbed situational deployment trigger.

[0004] Further exemplary embodiments include the intelligent operational agent configured to determine a tenth digital element, and configured to deploy the scrubbed situational deployment trigger based on the tenth digital element. The intelligent networked architecture may further comprise 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. The load balancer may be further configured to distribute processing of the secure digital data by the plurality of secure cloud based specialized insight servers.

[0005] Some exemplary embodiments include the first digital data element, the second digital data element, and the third digital data element randomly generated by a hardware based random number generator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 is a diagram of an exemplary system for secure intelligent networked architecture, processing and execution.

[0007] FIGS. 2A-2B represent a flowchart of an exemplary method for intelligent networked architecture, processing and execution.

[0008] FIG. 3 is a table of exemplary digital data elements for secure intelligent networked architecture, processing and execution.

[0009] FIGS. 4A-4B represent a flowchart of an exemplary method for intelligent networked architecture, processing and execution.

[0010] FIGS. 5A-5B represent a flowchart of an exemplary method for intelligent networked architecture, processing and execution.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0011] FIG. 1 is a diagram of an exemplary system for secure intelligent networked architecture, processing and execution.

[0012] The exemplary system 100 as shown in FIG. 1 includes a secure cloud based specialized intelligent historical agent 101, activity server 102, secure intelligent agent 103, optional hardware based random number generator machine 103A, secure intelligent operational agent 104, secure cloud based specialized insight servers and/or virtual insight machines 105, optional data transfer corridors 106A-106D, and scrubbed situational deployment trigger 107.

[0013] According to various exemplary embodiments, the secure cloud based specialized intelligent historical agent 101 is a non-generic computing device comprising non-generic computing components. It may comprise specialized dedicated processors configured to seek, copy and transmit massive amounts of secure digital data from the secure cloud based specialized intelligent historical agent 101 to the secure cloud based specialized insight servers and/or virtual insight machines 105.

[0014] In some embodiments, the secure cloud based specialized intelligent historical agent 101 is situated behind a firewall (not shown). In some embodiments, the secure cloud based specialized intelligent historical agent 101 encrypts the secure digital data before storing it and decrypts the secure digital data before copying and transmitting it to the secure cloud based specialized insight servers and/or virtual insight machines 105. The decrypting may be performed as a separate step in advance of copying and transmitting to increase the speed in which the specialized dedicated processors may copy and transmit the secure digital data. According to further embodiments, the specialized dedicated processors may copy as a separate step the secure digital data before transmitting it to increase the speed in which the

specialized dedicated processors retrieve and transmit the secure digital data. In even further embodiments, the secure cloud based specialized intelligent historical agent 101 may, without human involvement, automatically search, retrieve, and encrypt new data to update stored secure digital data.

[0015] The activity server 102, according to exemplary embodiments, is a third party server with activity influenced by numerous external agents, factors and conditions. The activity server 102 receives secure instructions from the secure intelligent operational agent 104 and the activity server 102 transmits digital data as influenced by the numerous external agents, factors and conditions to the secure intelligent operational agent 104. In some exemplary embodiments, the activity server 102 is associated with one or more sports teams, companies, markets, exchanges, firms or associations. In further exemplary embodiments, one way or two way communication between the activity server 102 and the secure intelligent operational agent 104 may be over a dedicated secure wired channel or over a dedicated secured wireless channel, with or without encryption/decryption and with or without a firewall separating the two.

[0016] The secure intelligent agent 103, according to some exemplary embodiments (although not limited to), is a non-generic computing device comprising non-generic computing components. It may comprise specialized dedicated hardware processors to determine and transmit digital data elements to the secure cloud based specialized intelligent historical agent 101. In further exemplary embodiments, the secure intelligent agent 103 comprises a specialized device having circuitry, load balancing, and specialized hardware processors, and artificial intelligence, including machine learning. Numerous determination steps by the secure intelligent agent 103 as described herein may be made by an automatic machine determination without human involvement, including being based on a previous outcome or feedback (e.g. an automatic feedback loop) provided by the

secure intelligent networked architecture, processing and/or execution as described herein.

[0017] The optional hardware based random number generator machine 103A, according to various exemplary embodiments, may determine and/or transmit one or more digital data elements to the secure intelligent agent 103, to the secure cloud based specialized intelligent historical agent 101 and/or to the secure cloud based specialized insight servers and/or virtual insight machines 105.

[0018] The secure intelligent operational agent 104, according to various exemplary embodiments, is a non-generic computing device comprising non-generic computing components. It may comprise specialized dedicated hardware processors to determine and transmit one or more digital data elements to the secure cloud based specialized intelligent historical agent 101. The secure intelligent operational agent 104 may comprise specialized dedicated hardware processors to determine and transmit new data to update secure digital data in the secure cloud based specialized intelligent historical agent 101. The secure intelligent operational agent 104 may comprise specialized dedicated hardware processors to determine, request and receive secure digital data from the secure cloud based specialized intelligent historical agent 101. The secure intelligent operational agent 104 may comprise specialized dedicated hardware processors to determine and transmit secure instructions to the activity server 102. The secure intelligent operational agent 104, may comprise specialized dedicated hardware processors to receive from the activity server 102 digital data as influenced by the numerous external agents, factors and conditions. The secure intelligent operational agent 104 may comprise specialized dedicated hardware processors to receive transformed data, files, and/or visually perceptible elements from the secure cloud based specialized insight servers and/or virtual insight machines 105. The secure intelligent operational agent 104 may comprise specialized dedicated hardware processors to determine and transmit

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 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.

[0022] The secure cloud based specialized insight servers and/or virtual insight machines 105, according to various exemplary embodiments, receive secure digital data from the secure cloud based specialized intelligent historical agent 101. The secure cloud based specialized insight servers and/or virtual insight machines 105, according to various exemplary embodiments, receive at least one digital data element from the secure intelligent agent 103. The secure cloud based specialized insight servers and/or virtual insight machines 105, according to various exemplary embodiments, utilize massive sophisticated computing resources as described herein to produce transformed digital data, files, scrubbed files and/or visually perceptible digital data elements. One such transformation product produced is the scrubbed situational deployment trigger 107 that is transmitted to the secure intelligent operational agent 104.

[0023] In certain exemplary embodiments, the secure cloud based specialized insight servers and/or virtual insight machines 105 further comprise a master virtual machine server including a single secure cloud resource responsible for generating all of or most of the herein described virtual machines.

[0024] According to various exemplary embodiments, a virtual machine may comprise an emulation of a particular computer system. Virtual machines operate based on the computer architecture and functions of a real or hypothetical computer, and their implementations may involve specialized hardware, software, or a combination of both.

[0025] In further exemplary embodiments, a CloudManager is configured to a cluster of cloud computing instances for processing large amounts of data. The CloudManager serves as the user interface to handle the ordering and cancelling of virtual computing instances. Additionally, the CloudManager may allow for detailed customization of the virtual machines. For example, Random Access Memory ("RAM"), processor speed, number of processors, network details,

security/encryption, and/or memory may be detailed for each virtual machine and/or all virtual machines. Once the cluster of cloud computing instances is ordered and running, the CloudManager is "listening" for idle machines and "assigning" any idle machine processing responsibilities.

[0026] A cloud-based computing environment is a resource that typically combines the computational power of a large grouping of processors and/or that combines the storage capacity of a large grouping of computer memories or storage devices.

[0027] For example, 150 8-core virtual machines may be utilized to process hundreds of billions of calculations in three to four hours.

[0028] Additionally, each virtual machine may transform historical data and performance data into a neural network usable data set. In some exemplary embodiments, a neural network usable data set comprises an aggregation of data points organized into one or more sets.

[0029] For example, for a particular time period, such as each day (or each minute, hour, month, year(s), decades, etc.), for any particular item, the historical data and performance data are grouped together as a data set.

[0030] According to further embodiments, each virtual machine may create a neural network base. The neural network base, along with the neural network usable data set forms a neural network. Creating a neural network base, according to some exemplary embodiments, includes processing a layer of input data and then processing that data algorithmically to compare the output of algorithms against known output.

[0031] A neural network base may comprise a set of algorithms used to approximate against data inputs. These algorithms are able to store tested values within itself and store an error rate.

[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 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

segment for the resource. In further exemplary embodiments, other factors may represent the second digital data element.

[0039] At step 203, the secure intelligent agent determines a third digital data element. In various exemplary embodiments, the third digital data element is an item on the determined segment. In further exemplary embodiments, other factors may represent the third digital data element.

[0040] At optional step 204, steps 201 through 203 (i.e. intelligent determination of the first, second and/or third digital data elements) may be performed by a hardware based random number generator machine that comprises part of the intelligent agent.

[0041] Optional step 204, according to many exemplary embodiments, improves the functioning of the exemplary system by optimizing the number of runs that can be performed in a limited period of time. That is, in most exemplary embodiments, the information generated has a time value. As time lapses, the value of the information decreases. Additionally, given the massive amount of data to be processed in a limited period of time, it is important that the time be used as effectively as possible. Therefore employing random number generation to drive the variables for the runs is far more effective than having a human drive the variables for the runs, as human involvement would likely lead to redundancy, bias and other inefficiencies, as often a desired goal is to maximize the number of runs that may be performed in a limited period of time.

[0042] At step 205, the intelligent agent accesses (via its circuitry over a secure network to a secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents that may be load balanced) secure digital data for the first, second and third digital data elements.

[0043] At step 206, the intelligent agent determines a fourth digital data element. In some exemplary embodiments, the fourth digital data element is a look back

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 nor 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.

[0053] At step 214, the intelligent agent directs (via its circuitry over a secure network) the secure cloud of specialized insight servers and/or virtual insight machines to further transform the transformation results generated at step 211 pursuant to step 212 and optionally, step 213. According to one exemplary embodiment, the further transformation results in a list of names and/or identifiers of portions of the transformed results, but not the portions themselves.

[0054] In many exemplary embodiments, the transformation results generated at step 211 pursuant to step 212 and optionally, step 213 represent a massive amount of data. At step 214, computing performance is improved by scrubbing or clearing the data transferred from the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents from names and/or identifiers of parts of that data. The names and/or identifiers are based on the output or outcome of the transformation performed at step 211 pursuant to step 212 and optionally, step 213. The amount of data represented by the names and/or identifiers is extremely small when compared to the secure digital data transferred from the secure cloud of specialized historical agents and/or virtual historical intelligent agents. Because the data transferred from the secure cloud of specialized intelligent historical agents 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.

[0055] 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.

[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 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 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.

[0058] 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 test deploy the transferred data in a setting such as that exemplified by the activity server 102 (FIG. 1).

[0059] 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.

[0060] At step 216, if the test deployment strategy performed at step 215 was successful, the intelligent operational agent will actually execute the deployment strategy.

[0061] FIG. 3 is a table of exemplary digital data elements for secure intelligent networked architecture, processing and execution.

[0062] Shown in table 300 of FIG. 3 are ten exemplary digital data elements, including the corresponding name of each of the digital data elements. The first digital data element is a resource. Resources may include football players, workers, equities, vehicles, biological based drugs and the like. The second digital data element is a resource segment. Resource segments may include college football, lawyers, New York Stock Exchange ("NYSE"), trucks, monoclonal antibodies ("Mabs") and such. The third digital data element is an item. Items may include running backs, patent lawyers, GM stock, Ford trucks, cancer Mabs, etc. The fourth

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 one example 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.

[0066] At step 402, 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. For example, segments may include the Chicago Mercantile Exchange ("CME"), New York Mercantile Exchange ("NYMEX") and/or the Intercontinental Exchange ("ICE").

[0067] Here, for example, the New York Stock Exchange ("NYSE") may be selected as the second digital data element.

[0068] At step 403, the secure intelligent agent determines a third digital data element. In various exemplary embodiments, the third digital data element is an item on the determined segment. For example, items may include gold ("GC"), crude oil ("CL"), and/or the S&P 500 ("ES").

[0069] Here, for example, General Motors ("GM") stock may be selected as the third digital data element.

[0070] At optional step 404, steps 401 through 403 (i.e. intelligent determination of the first, second and/or third digital data elements) may be performed by a hardware based random number generator machine that comprises part of the intelligent agent.

[0071] At step 405, the intelligent agent accesses (via its circuitry over a secure network to a secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents that may be load balanced) secure digital data for the first, second and third digital data elements. For example, the secure digital data for the first, second and third digital data elements may be trading strategies, including algorithms or bots.

[0072] According to some exemplary embodiments, data processing may be managed using simultaneous requests without the need to have multiple copies of programs executing within any single intelligent agent (e.g. "multithreading").

[0073] Here, for example, an entire population (or optionally a segment of the entire population) of algorithms or bots that trade GM stock on the NYSE market is the secure digital data. For example, data for 160,000 bots (or more) are selected. These bots may be generated per U.S. Non Provisional Application Serial No. 14/642,569 filed on March 9, 2015 titled "Systems and Methods for Generating and Selecting Trading Algorithms for Big Data Trading in Financial Markets," which is hereby incorporated by reference, or the bots may be generated by other systems and methods.

[0074] According to certain exemplary embodiments, a trading algorithm, a trading strategy or a bot comprises a technical indicator, an evaluation bar characteristic and an item.

[0075] A technical indicator at the most basic level is a series of data points that are derived by applying a formula to price data of an item. Technical indicators provide a unique perspective on the strength and direction of the underlying price action of the item. Exemplary technical indicators include, but not by way of limitation, relative strength index ("RSI"), average directional index, stochastics, money flow index, moving average convergence-divergence, etc.

[0076] A bar is comprised of an opening price, a closing price, intervening prices, volume and trading activity across a period of time for an item. For example, the price of gold may open at \$800 per ounce on an exchange at 9:00 AM and close at \$900 per ounce on the same exchange at 5:00 PM on the same day. This may represent one bar.

[0077] Evaluation bar characteristics may be based on time, tick, volume, or market activity. For example, time (e.g., second, minute, hour, day, month etc.), and/or tick (trades at the exchange, e.g., x number of trades) and/or volume (e.g., one, ten, two-hundred, one-thousand etc. contracts), and/or market-activity (e.g., 0.5%, 1%, 1.5%, 2% etc. market move).

[0078] Items may include futures (e.g., S&P, Euro, gold, crude, cotton, soybeans, 10-yr notes, lean hogs, etc.), stocks (e.g., PG, GE, AAPL, GOOG, FB, etc.), bonds (e.g., US Gov. bonds, Eurodollar, etc.), and forex (e.g., EURUSD euro to the dollar, etc.).

[0079] Here, for example, the relative strength index (“RSI”) may be selected as a technical indicator. Every thirty seconds may be selected as an evaluation bar characteristic. The price of gold may be selected as the tradable item. Accordingly, a bot may comprise deciding whether to buy, sell or hold based on calculating the RSI of the price of gold every 31 seconds while the relevant market is open.

[0080] A secure cloud of specialized historical intelligent historical agents and/or virtual intelligent historical agents, according to some exemplary embodiments, may comprise trading algorithms, trading strategies or “bots” that meet minimum standards.

[0081] In some embodiments, minimum standards refer to anything that is trade worthy. Minimum standards vary for different preliminary tests. For example, if the strategy is to look for safe trading algorithms, filtering criteria focus on safety (minimal losses) in unfavorable market conditions such as volatile or bearish market periods. If the strategy is to look for high performing trading algorithms, filtering criteria focus on superior returns such as any trading algorithm with a high annual return (i.e., greater than 50% return).

[0082] At step 406, the intelligent agent determines a fourth digital data element. In some exemplary embodiments, the fourth digital data element is a look back 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 generation machine, either as a separate step or as part of optional step 404. Here, for example, the intelligent agent may determine a look back period of 10 years as the fourth 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).

[0088] According to other exemplary embodiments, multiple performance metrics may be selected at step 408. Such performance metrics may include, however, not limited to: Compounded Annual Growth Rate (CAGR), Time Weighted Rate of Return (TWRR), Holding Period Return (HPR), Jensen's Alpha, Underwater Volume Index (UVI), Abovewater Volume Index (AVI), Average Drawdown, Maximum Drawdown, MAR Ratio, Total Decision Points, Trades Per Million, Best 12 Months, Worst 12 Months, Return Retracement Ratio, Sortino Ratio, Sharpe Ratio, Percent in the Market, Total Number of Trades, Average Trade Length, Average Trades Per Day, Average Trades Per Week, Average Trades Per Month, Percent Return in the Last Week, Percent Return in the Last 4 Weeks, Number of trades in the Last Week, Number of trades in the Last 4 Weeks, Commission, Slippage, Time Spent Long in the Market, Time Spent Short in the Market, Average Profit / Loss per Day, Average Profit / Loss per Week, Average Profit / Loss per Month, K-Ratio, and/or RINA Index.

[0089] At step 409, 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 generation machine, either as a separate step or as part of optional step 404. Here, for example, a bear market condition may be selected as the sixth digital data element, so that the risk adjusted performance for each of the bots trading GM stock is calculated for the bear markets that took place during the last 10 years. According to other exemplary embodiments, market conditions may also include cyclical bull, cyclical bear, volatile and/or ranging.

[0090] At step 410, 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. Here, the allocation amount is a number of contracts to deploy.

[0091] According to other exemplary embodiments, the allocation amount may be to a single strategy, a group of strategies, and/or to multiple groups of strategies. For example, the maximum number of contracts a grouping of strategies will trade may be set and the grouping of strategies will systematically trade based on the strategies' signals. In another example, a fixed percentage of total equity or total value may represent an allocation amount. Accordingly, with a \$1,000,000 total value, the maximum number contracts may be set so that the margin to equity ratio is 10%. The maximum number of contracts traded will change as the equity changes and as the margin on a given contract adjusts. In another example, risk based allocation may be used. Here, based on a risk metric, contracts are allocated to the best risk-return ratio in real time. In yet a further example, a machine learning algorithm allocation may be used. In this case, based on the machine learning algorithm, contract allocation will be distributed to the highest expectancy score.

[0092] At step 411, 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. In one exemplary embodiment, the transformation will result in visually perceptible elements. In further exemplary embodiments, other factors may represent the transformation result.

[0093] Here, for example, visually perceptible elements may represent performance of the 160,000 bots based upon the determined performance metric and market condition. For example, based upon the past transaction history for each bot on a minute by minute basis, a visually perceptible element representing the risk

adjusted performance for each of the bots trading GM stock is calculated for the bear markets that took place during the last 10 years.

[0094] Here, for example, if a bot made 20 transactions over the last 10 years, these transactions can be evaluated in order to calculate a performance metric. Other information about the bot may be determined based on observing the bot's minute by minute performance against its transaction history, including trade by trade metrics, compound annual growth rate (CAGR), underwater volume index (UVI), drawdown evaluation metrics, etc.

[0095] Performance metrics may include total profit over 1 year, percentage of profitable trades over a time period, how much was gained or lost in each trade, percentage of profitable trades in a bear or bull market, correlation to other indexes, ratio of profitable trades to cover largest loss, etc. For instance, % of profitable trades ($= \text{profitable trades} / \text{total number of trades}$) may be used as performance metrics.

[0096] According to other exemplary embodiments, performance metrics may also include maximum drawdown, average drawdown, max peak to trough time, average peak to trough time, max peak to peak time, average peak to peak time, pain to gain ration, sortino ratio, sharpe ratio, and/or return retracement ratio.

[0097] At step 412, 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. According to one exemplary embodiment, a percentage representing what percent of the bot population should be selected for active trading based upon step 411 is the eighth digital data element. Here, for example, for the plurality of specialized servers each having an insight engine, 1% is determined, meaning that the top 1% of the 160,000 bots should be selected based the risk adjusted return for trading GM stock (regardless of frequency) for the bear markets during past 10 years, resulting in a strategic trading portfolio of 1600 selected bots. According to another

exemplary embodiment, a predetermined minimum threshold may be set as the eighth digital element. In this case, bots meeting and/or exceeding such a threshold are selected.

[0098] At optional step 413, 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 412 is the 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 performing bots to remove before performing step 412 is the eighth digital data element. For example, the intelligent agent may employ multiple statistical regression methods to systematically determine which bots perform outside of a mean of a particular population. Such methods may include, but are not limited to grouping methods (e.g. ignoring the top 5% based on the selected performance metric and grouping the first 100 and 300 of the remaining bots), elimination methods (standardization or normalization of populations through elimination of the top and bottom 5% of bots outside of a statistical mean), using statistical measures DFITTS and/or DFBETAS to identify outliers, or mathematical calculations such as standard error and standard deviation. In further exemplary embodiments, other factors may represent the eighth digital data element.

[0099] At step 414, the intelligent agent directs (via its circuitry over a secure network) the secure cloud of specialized insight servers and/or virtual insight machines to further transform the transformation results generated at step 411 pursuant to step 412 and optionally, step 413. According to one exemplary embodiment, the further transformation results in a list of names/identifiers of the bots in each strategic trading portfolio (and not the bots themselves). The list may include the variables defined by the intelligent agent during the run as well as the

resulting performance metric(s) for each bot and for the strategic trading portfolio. The list may also include a market condition for the strategic trading portfolio. The list may be transmitted to an intelligent operational agent for further analysis.

[00100] At step 415 the intelligent operational agent determines a tenth digital data element and executes a test deployment strategy.

[00101] 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 test deploy the transferred data in a setting such as that exemplified by the activity server 102 (FIG. 1).

[00102] 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.

[00103] At step 416, if the test deployment strategy performed at step 415 was successful, the intelligent operational agent will actually execute the deployment strategy.

[00104] The exemplary systems and methods described herein may be performed in a secure computing environment including the use of firewalls and encryption technology. Given the potentially high value of the information being generated, and the potential magnitude of the resulting investment decisions, measures may be taken to perform some or all of the steps herein in a secure manner, with emphasis

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 is 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

hardware based random number generator machine that comprises part of the intelligent agent.

[00113] Optional step 504, according to many exemplary embodiments, improves the functioning of the exemplary system by optimizing the number of runs that can be performed in a limited period of time. That is, in most exemplary embodiments, the information generated has a time value. As time lapses, the value of the information decreases. Additionally, given the massive amount of data to be processed in a limited period of time, it is important that the time be used as effectively as possible. Therefore employing random number generation to drive the variables for the runs is far more effective than having a human drive the variables for the runs, as human involvement would likely lead to redundancy, bias and other inefficiencies, as often a desired goal is to maximize the number of runs that may be performed in a limited period of time.

[00114] At step 505, the intelligent agent accesses (via its circuitry over a secure network to a secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents) secure digital data for the first, second and third digital data elements.

[00115] At step 506, the intelligent agent determines a fourth digital data element. In some exemplary embodiments, the fourth digital data element is a look back period. This step may also be performed by a hardware based random number generation machine, either as a separate step or as part of optional step 504.

[00116] Here, the look back period is represented by the last 50,000 patients seen or treated with monoclonal antibody ("Mab") based drugs for cancer.

[00117] At step 507, 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 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").

[00118] 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.

[00119] Here, the secure digital data includes the medical histories and genomic data for the last 50,000 patients seen or treated with monoclonal antibody ("Mab") based drugs for cancer.

[00120] At step 508, 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 generation machine, either as a separate step or as part of optional step 504.

[00121] Here, the number of disease free months is the performance metric.

[00122] At step 509, the intelligent agent determines a sixth digital data element. According to various exemplary embodiments, a condition is the sixth 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 504.

[00123] Here, the condition is adenocarcinoma of the lung, with a particular gene sequence.

[00124] At step 510, 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.

[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 nor 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.

[00130] At step 512, 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.

[00131] At optional step 513, 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 512 is the ninth digital data element.

[00132] At step 514, the intelligent agent directs (via its circuitry over a secure network) the secure cloud of specialized insight servers and/or virtual insight machines to further transform the transformation results generated at step 511 pursuant to step 512 and optionally, step 513. According to one exemplary embodiment, the further transformation results in a list of names and/or identifiers of portions of the transformed results, but not the portions themselves.

[00133] In many exemplary embodiments, the transformation results generated at step 511 pursuant to step 512 and optionally, step 513 represent a massive amount of data. At step 514, computing performance is improved by scrubbing or clearing the data transferred from the secure cloud of specialized intelligent historical agents and/or virtual intelligent historical agents from names and/or identifiers of parts of that data. The names and/or identifiers are based on the output or outcome of the transformation performed at step 511 pursuant to step 512 and optionally, step 513. The amount of data represented by the names and/or identifiers is extremely small when compared to the secure digital data transferred from the secure cloud of specialized historical agents and/or virtual historical intelligent agents. Because the data transferred from the secure cloud of specialized intelligent historical agents

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 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 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 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 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,

therefore, be determined not with reference to the above description, but instead should be determined with reference to the appended claims along with their full scope of equivalents.