

ELECTRONIC AUTHENTICATION SYSTEM AND PROCESS USING THE SAME

[0001] The present patent application relates to an electronic authentication system for financial auditing or accounting. The electronic authentication system is also
5 known as electronic authentication device or apparatus. The present application further relates one or more electronic authentication processes using the electronic authentication system.

[0002] Personnel authentication for auditing financial or accounting documents (e.g.
10 statement of account) is important because personnel authentication attests a signature, seal, stamp, certificate or written note on a financial document to be genuine and/or authorized. An authenticated financial document or personnel provide recognized validity by many authorities, organizations, jurisdictions or countries. Currently, auditing of financial documents is mostly done manually and
15 paper-based. Often, authorized personnel are required to sign and/or stamp on relevant financial documents as proof of authenticity and approval. The manual and paper-based authentication process is known to be sluggish or human attention demanding, in addition to rampant problems of forgery, interception and/or unlawful alternation. In some situations, there are unlicensed auditors (known as bogus
20 auditors/accountants) who provide audit work with/without complying with audit standards. SMEs (Small and Medium-Sized Enterprises) do not know how to differentiate between genuine/authentic auditors and bogus auditors/accountants. Hence, these SMEs are exposed to great financial risk by engaging those feign auditing professionals.

[0003] The present patent application aims to provide one or more new and useful electronic authentication systems or tools for financial auditing. The present patent application further aims to provide one or more new and useful methods or processes for financial auditing. Essential features of the patent application are
5 provided by one or more independent claims, whilst advantageous features are presented by their dependent claims respectively.

[0004] As a first aspect, the present application provides an electronic authentication system. The electronic authentication system comprises a computing server and a
10 communicating unit further connected to the computing server for communicating with at least one external electronic device via an external communication network. The computing server further comprises a non-transitory machine-readable storage unit configured to store a series of instructions to perform an authentication process; and a processing unit (e.g. microprocessor, microcontroller) connected to the non-
15 transitory machine-readable storage unit for processing the series of instructions. In particular, the computing server is configured to authenticate the at least one communication device in order to authenticate communication between the at least one external electronic device and the electronic authentication system. Authentication or its variation (e.g. authenticate, authentic) means to prove that
20 something or someone is real, true, authorized or what people say it is. For example, in some instances of financial auditing, to authenticate an auditor means to check or verify if the auditor is authorized by a client for auditing, the auditor is a licensed professional and/or the auditor is duly accredited (e.g. authorized, delegated) by a licensed auditor in one or more relevant jurisdictions. For example, a third party out
25 of the licensed professional's organisation is authorised to conduct auditing job

partially or fully on behalf of the licensed auditor. Alternatively, a subordinate of the licensed professional or auditor is delegated by the licensed auditor to carry out the auditing job partially or fully.

5 [0005] The one or more external electronic devices optionally comprise a first external electronic device (i.e. first external communication device, first personal communication device, first electronic device) for an auditor (also known as preparer) to initiate a confirmation request; a second electronic device (i.e. second external communication device, second personal communication device, second
10 electronic device) for a client (also known as authorizer) to authorize the confirmation request, and a third electronic device (i.e. third external communication device, third personal communication device, third electronic device) for a responder to respond to the confirmation request. The first electronic device, the second electronic and the third electronic device are configured to register at the computing
15 server with their unique identities (IDs) respectively. The confirmation request includes but not limited to trade and non-trade for debtors/creators; transactions with related parties; balances, transactions, remunerations, shareholdings, etc. for directors; resolutions and minutes passed, share capital, etc. for secretary; confirmation for investments for shareholding; inventories held at third parties'
20 premises; hire purchase or other leasing arrangements; and legal issues for lawyers.

[0006] The series of instructions optionally comprise an artificial intelligence (AI) algorithm for automatically causing the computing server to perform the authentication process. Therefore, the electronic authentication system is configured
25 at a dominating position of the authentication process for preventing any malicious

person from interfering with the authentication process. Accordingly, the processing unit optionally has an artificial intelligence (AI) accelerator for accelerating the artificial intelligence (AI) algorithm for various artificial intelligence applications, such as artificial neural networks and machine learning. In some implementations, the AI
5 accelerator comprises one or more Graphics Processing Units (GPUs) for image manipulator which shares a similar mathematical basis with neural networks. The GPUs may further comprise neural network specific hardware (such as tensor cores) for further accelerating the AI applications. In some implementations, the AI accelerator comprises reconfigurable devices (such as field-programmable gate
10 arrays (FPGA)) especially for deep learning frameworks which continue to evolve. In particular, the electronic authentication system may comprise an artificial intelligence (AI) algorithm for automatically performing the electronic authentication process.

[0007] The computing server optionally has a database configured to store
15 information of the client. Similarly, the computing server may also have databases configured to store information of the auditor, the authorizer, the responder and/or another party respectively. The databases are independent to each other. Alternatively, the computing server may have a single database configured to store information of the client, the auditor and the responder. The database management
20 system (DBMS) is optionally configured to automatically update the information of the client. The computing server may automatically retrieve and collect latest information of the client from trustable external sources, such as government websites, official company websites and professional organizations. The artificial intelligence (AI) algorithm may be trained to identify whether the external sources are
25 latest and genuine by sharing computation capacity of the artificial intelligence (AI)

processor. Similarly, the information of the auditor and the responder may also be updated from trustable external sources, or another source. For example, the database is updated by the artificial intelligence (AI) algorithm (also known as AI Engine) of the computing server by obtaining, compiling, analysing, organizing, 5 verifying, editing and/or storing information from external sources, such as social media platforms of the auditor, the authorizer and the responder, such as blogs, business networks, social gaming, etc.

[0008] The confirmation request is optionally sent exclusively to the second electronic 10 device (i.e. second communication device) according to the information of the client. The client may authorize the confirmation request by using the second communication device only. Meanwhile, the client also cannot forward the confirmation request to any other electronic devices or communication devices. The computing server is optionally configured to warn the auditor if authorization of the 15 confirmation request is not sent from the second communication device. The auditor then may inform the client through the computing server. Alternatively, the client can authorize his/her subordinate for further action. Once the client forwards the request to his/her subordinates, this action is deemed to be part of "authorization". Accordingly, both the external electronic devices (e.g. personal electronic device, 20 personalized computing device, mobile phone, Personal Computer) of the client and his/her subordinates are registered and/or authenticated by the computing server.

[0009] The computing server is optionally configured to notify the responder to respond to the confirmation request in a timely manner. The computing server may 25 also set up a score system to each specific responder, known as credit scoring

system. The score system may include multiple parameters, such as responding time and responding rate. The higher the score, the better service the responder would be likely to provide to the confirmation request. The score system may allow an authenticated auditor to mark trustworthiness or credit of a responder by identifying
5 the responder's personal electronic device. In detail, the authenticated auditor can take alternative procedures to test and ensure the responder to be authentic. Records or scores of the responder in the score system may be recorded, updated or analysed.

- 10 [0010] "Another auditor" can refer to the same procedure & vote up/down or he/she can proceed with other alternative procedures to prove authenticity & trustworthiness.

[0011] The computing server is optionally configured to store an authentication report after the authentication process, such as in a non-volatile memory of the computing
15 server. The authentication report is approachable to the auditor such that the auditor may download the authentication report via the external communication network for completing the authentication process.

[0012] As a second aspect, the present application discloses an electronic
20 authentication process for financial auditing by using the electronic authentication system described in the first aspect. The electronic authentication process comprises a first step of collecting authentication information of at least one external electronic device from an external source to an electronic authentication system; a second step of authenticating the at least one external electronic device by communicating with
25 the at least one external electronic device by utilizing the authentication information;

and a third step of providing the authorization information of the at least one external electronic device to a third party.

[0013] The electronic authentication process may further comprise a step of
5 collecting authentication information of a first external electronic device and a second external electronic device from the external source; and a following step of authenticating the first external electronic device and the second external electronic device for authenticating communication between the first external electronic device and the second external electronic device.

10

[0014] The electronic authentication process may further comprise a step of authenticating a third external electronic device; and a following step of providing authentication information of the third external electronic device to the first external electronic device, the second external electronic device or both after authenticating
15 the third external electronic device.

[0015] The electronic authentication process may further comprise a step of initiating a confirmation request from the first electronic device of an auditor to the electronic authentication system; a second step of authorizing the confirmation request from
20 the second electronic device of a client to the electronic authentication system; and a third step of responding the confirmation request from the third electronic device of a responder to the electronic authentication system. The first electronic device, the second electronic device and the third electronic device are configured to register at the electronic authentication system. Accordingly, only the first electronic device, the
25 second electronic device and the third electronic devices can get access to the

electronic authentication system. Before the initiating step, the electronic authentication process starts with the auditor triggers a task assignment which is to be completed by the responder. The auditor obtains instructions and authorization from the client, before triggering the task assignment. The task assignment requires
5 the auditor to obtain a confirmation from the client before the task assignment is executed. Thus, the confirmation request is generated in the electronic authentication process. The task assignment includes but not limited to assurance service, payment transaction, document verification or other related task assignment which requires an approval from the client.

10

[0016] The electronic authentication process optionally comprises an additional step of checking information of the client with the second electronic device before sending the confirmation request to the second electronic device. This step is preferably conducted by the electronic authentication system (such as using the artificial
15 intelligence (AI) algorithm) for preventing any external interference and/or proving authentic.

20

[0017] The electronic authentication process may further comprise an additional step of updating the information of the client stored in a computing server of the electronic authentication system. As mentioned in the first aspect, the computing server may automatically retrieve and collect latest information of the client from trustable external sources with the artificial intelligence (AI) algorithm. Similarly, the electronic authentication process may also comprise additional steps of updating the information of the auditor and the responder, the authorizer respectively.

25

[0018] The electronic authentication process may further comprise an additional step of warning the auditor if authorization of the confirmation request is not sent from the second communication device. The auditor then may then notify the client through the electronic authentication system.

5

[0019] The electronic authentication process may further comprise an additional step of notifying the responder to respond to the confirmation request in a timely manner. As mentioned in the first aspect, each specific responder would be scored according to responding time, responding rate and other parameters.

10

[0020] According to a third aspect, the present patent application provides an electronic authentication system for financial auditing. The electronic authentication system comprises a computing server that has a non-transitory machine-readable storage unit configured to store a series of instructions to perform an authentication
15 process; a processing unit connected to the non-transitory machine-readable storage unit for processing the series of instructions automatically; and a communicating unit further connected to the processing unit for communicating with an external electronic device via an external communication network. In computing, the computing server is also known as a server that is installed with one or more
20 computer programs in order to provide functionality for other programs and electronic devices, sometimes called "clients". The non-transitory machine-readable storage unit is also known as memory or computer memory for storing data or information in a computer or related computer hardware device, such as semiconductor memory (Metal–Oxide–Semiconductor memory). Often, the non-
25 transitory machine-readable storage unit includes flash memory (e.g. Solid-State

Drive or Memory) and ROM, PROM, EPROM and EEPROM memory. The processing unit includes a computer processor, a CPU (Central Processing Unit), a GPU (Graphics Processing Unit), a microcontroller, and a Reduced Instruction Set Computer (RISC) microprocessor. The communicating unit includes networking

5 hardware (also known as network equipment or computer networking devices), which are electronic components required for communication and interaction between devices on a computer network. For example, the communicating unit includes mobile data communication components (e.g. Subscriber Identity Module card) that are configured to communicate with communications system or

10 communication system for telecommunication, whether 2G (second-generation cellular network), 3G (third generation of wireless mobile telecommunications technology), 4G (fourth generation of broadband cellular network technology), 5G (fifth generation technology standard for cellular networks) or more advanced telecommunication protocols. The communication unit possibly includes examples

15 such as a network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or other physical network interfaces), which is a computer hardware component that connects the computing server to a computer network.

20 [0021] The computing server is operable or configured to authenticate a first external electronic device of a first user or a Requestor and a second external electronic device of a second user or Responder in order to authenticate communication or electronic communication between the first external electronic device and the second external electronic device. The first external electronic device or the second

25 electronic device are communication devices outside or independently operated

from the electronic authentication system. In an auditing process, the Requestor is often known as a client whose accounting records are required to be audited. The Responder is a business partner (e.g. supplier) who has financial transaction with the client and the financial transaction is required to be audited by a licensed auditor.

5

[0022] The computing server is optionally configured to authenticate the first external electronic device and/or the second external electronic device via reciprocal exchange of authorized electronic signals (e.g. network packet, data packet, messages, emails, electronic document) between or among the computing server

10 and one of the two external electronic devices.

[0023] The electronic authentication system may be configured to authenticate the first external electronic device and the second external electronic device independently or separately in order to achieve back-to-back auditing. Hence, the

15 first external electronic device and the second external electronic device are individually verified for trusted communication between the first external electronic device and the second external electronic device.

[0024] The computing server is possible configured to authenticate a third external

20 electronic device of a third user as a client that communicatively connected to the computing server for communicating with the first external electronic device and/or the second external electronic device. Once each of the first external electronic device, the second external electronic device and the third external electronic device are individually or collectively authenticated, electronic communication between any

25 of these devices (e.g. SMS message, email, WhatsApp message, LINE message,

Telegram message, etc.) becomes trustworthy. An auditing process that utilizes these devices may become efficient, reliable and confidential.

[0025] Each component of the electronic authentication system, the computing
5 server, the first external electronic device, the second external electronic device and
the third external electronic device can be a commonly available electronic device,
such as a computer or a smartphone. The computer or smartphone may be
personalized according to particular technical specification and/or personal
preference. For example, the computer is assigned with a unique IP address and/or
10 MAC address, whilst the smartphone is configured by a Subscriber Identity Module
(SIM) card and/or Bluetooth Device Address (BD_ADDR). The computer and/or
smartphone is possibly configured to obtain user interfaces and software
applications for the convenience of operation by users, including auditors, clients
(e.g. Directors of a company), Responders (e.g. licensed and authorized
15 accountant).

[0026] The non-transitory machine-readable storage unit is further possibly
configured to store, record or remember audio identification signals, video
identification signals or data, biometric identification signals, gesture identification
20 signals, geographical location signals, unique identifiers of the first electronic device,
the second electronic device or both. In other words, the non-transitory machine-
readable storage unit keeps records of electronic credentials that identify the
electronic authentication system, the first external electronic device, the second
external electronic device and the third external electronic device. For example, the
25 first external electronic device is a smartphone with a camera and a fingerprint

sensor so that biometric identification signals of a user of the smartphone are instantaneously captured and possibly stored for authentication in real-time. In other words, authenticity of the user (e.g. Responder) is verified by a personalized electronic device of the user.

5

[0027] The electronic credentials include three types, namely, something a user know (i.e. type 1), something a user have (i.e. type 2) and something the user is (i.e. type 3). The type 1 includes passwords, PINs, Authentic Pin Number (APN), combinations, code words, or secret handshakes, geographical location (e.g. GPS
10 signals). Anything that the user can remember and then type, say, do, perform, or otherwise recall when needed falls into this category. The type 2 includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices. A token device produces a time-based PIN or computes a response from a challenge number issued by the server. The type 3 includes any part of the
15 human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification. Two or more of the above types can be combined to authenticate the electronic authentication system, the first electronic device, the second electronic device or a combination of the devices, which is also known as multi-factor authentication.

20

[0028] In some cases, the unique identifiers comprises an electronic identity, identity information or simply identity (e.g. electronic address) of one of the first electronic device and the second electronic device. For example, the electronic identity includes MAC (media access control address) address, IP address (e.g. IPv4, IPv6)

according to TCP/IP protocol, a telephone number, a WeChat ID and their extensions.

[0029] The electronic authentication system may be configured to communicate with
5 one of the first electronic device and the second electronic device or both via multiple
electronic communication network (e.g. 1-to-1 telephone call, conference call,
WeChat, WhatsApp, Internet, Wi-Fi, Bluetooth, etc.). The non-transitory machine-
readable storage unit can be configured to store, modify, update, and/or delete
authentication information of the first electronic device and/or the second electronic
10 device so that electronic identifies or credentials can be kept up-to-date. For
example, the non-transitory machine-readable storage unit is operable to update
store, modify, update and/or delete authentication information of the first electronic
device and/or the second electronic device periodically or regularly, whether with a
secure database automatically. The secure database includes an official database
15 that holds authoritative and authentic data, which can only be read but cannot be
modified by the electronic authentication system, the computing server, the first
external electronic device, the second external electronic device and the third
external electronic device. For example, the secure database holds official records
of licensed auditors, directors and shareholders of business entities and official
20 representatives of companies, possibly including their telephone numbers, email
addresses and other electronic credentials.

[0030] In some cases, the electronic authentication system, the first electronic
device, the second external electronic device and/or the third external electronic
25 device are/is operable to revoke authentication information of the electronic

authentication system such that the authentication information of the electronic authentication system is no longer verifiable by the second electronic device. For example, when an auditor retires, his electronic credentials (e.g. digital credential) are removed from the non-transitory machine-readable storage unit, preventing
5 unauthorized or illegal usage of his electronic credentials or license.

[0031] The external electronic device of a first user or a Requestor sometimes is configured to communicate authentication information or digital credentials (e.g. telephone number, digital identification, password, digital key) of the electronic
10 authentication system with the second external electronic device for authenticating the electronic authentication system by the first electronic device and/or the second electronic device.

[0032] The electronic authentication system can be configured to authenticate with
15 the first electronic device, the second electronic device and the third electronic device sequentially simultaneously, separately or in combination of any of these forms/manners. For example, the electronic authentication system is configured to authenticate with the electronic device after authenticating with the second electronic device.

20

[0033] In some instances, the electronic authentication system is configured to give a predetermined scope of authorization by the first electronic device, the second electronic device or the third external electronic device with consent (e.g. time duration, network drive accessibility, the number of devices or users, geographical
25 location, size of data, number of files, frequency or number of access, number of

electronic devices to be accessed, number software applications to be accessed, fields of data or table to be accessed). For example, the third external electronic device of a client authorizes the first external electronic device of an auditor to access financial records of the third electronic device of a Responder for the latest
5 financial year or financial transaction records with the client only, but not any other financial records.

[0034] In some cases, the electronic authentication system is configured to accredit (e.g. approve delegation of authentication) from one of the first external electronic
10 device, the second external electronic device and the third electronic device to another internal or external electronic device (e.g. access rights). Often, each of the client, the auditor and the responder has many subordinates or colleagues with their own electronic devices. For example, a subordinate who is authorized and authenticated by the client, the auditor or the responder is able to represent his
15 superior for conducting authenticated communication with other parties or other electronic devices.

[0035] The electronic authentication system may be configured to authenticating one or more delegate electronic devices accredited (e.g. authorized, delegate) and/or
20 authenticated by the first external electronic device (i.e. also known as first electronic device or the first external device), the second external electronic device (i.e. also known as second electronic device or second external device), the third external electronic device (i.e. also known as third electronic device or third external device) or a combination of any of these devices.

[0036] The electronic authentication system can possibly be operable to be authenticated by the first electronic device, the second electronic device, third external electronic device or vice versa, whether within a predetermined period or permanently. In other words, mutual authentication between electronic devices are
5 feasible or allowable.

[0037] When necessary, the electronic authentication system is configured to authenticate the first external electronic device, the second external electronic device, the third external electronic device or a combination of any of these devices
10 via encrypted electronic communication. Encryption of authentication process or electronic devices facilitates reliable and confidential electronic correspondence. Whether encrypted or not, the electronic authentication system is configured to communicate with the first external electronic device, the second external electronic device and the third external electronic device continually, continuously and/or
15 automatically till completion of authentication.

[0038] Often, the electronic authentication system is configured to communicate with a cloud computing device (known as computer cloud) for using physical or virtual computing resource of a remote computer (e.g. data storage, processor), such as
20 by using Microsoft Azure, Alibaba Cloud and/or Amazon Web Services (AWS) as a cloud computing service via the communication unit (e.g. internet connection). In fact, any component of the electronic authentication system, the first external electronic device, the second external electronic device and the third external electronic device can be connected to one or more external clouds, computer
25 clouds, computing servers, servers or cloud computers.

[0039] The electronic authentication system can be operable to modify or configure the cloud computing device (also known as computer cloud) for supervised learning. For example, the cloud computing device is configured to capture data of multiple authentication processes so that the electronic authentication system is optimized or become "intelligent" for swift and reliable authentication, improving over time.

[0040] The electronic authentication system may be operable to embed authentication information of the electronic authentication system into an electronic report (e.g. auditing report) which may be accessed by the first external electronic device, the second external electronic device, the third external electronic device or a combination of any of these devices. For example, hyperlink, barcodes (QR code) and/or electronic file can be embedded into financial records for the ease of transmission or authentication.

15

[0041] The electronic authentication system is possibly configured to transfer, store, modify, update and/or verify authentication information of the first external electronic device to the second external electronic device or vice versa. For example, if an auditor leaves an auditing firm, his electronic credentials of his mobile phone is replaced by another set of electronic credentials of a replacement staff.

20

[0042] Sometimes, the electronic authentication system is uniquely accessible by an auditor (via biometric recognition of the electronic authentication system) who is registered with a secure database (e.g. official register, auditors or directors, court records of bankrupted personnel), which cannot be altered by the first electronic

25

device, the second electronic device, third electronic device or the electronic authentication system.

[0043] The secure database or external secure database is accessible and/or
5 readable (known as verifiable) by the first external electronic device, the second external electronic device, the third external electronic device and/or the electronic authentication system, but cannot be changed by any of them (i.e. the first electronic device, the second electronic device, third external electronic device and the electronic authentication system). For example, the authentication device may be
10 authenticated by the first external electronic device, the second external electronic device or both via ACS mPAC mechanism so that only external electronic devices of licensed auditors or associates authorized by a licensed auditor mechanism can be authenticated by the electronic authentication system, which means only intended account users are allowed to send confirmation. Usually, electronic
15 identification and/or electronic address of the first external electronic device, the second external electronic device and/or the third communication device are/is stored, recorded, registered or kept by the computing server or the non-transitory machine-readable storage unit.

20 [0044] The series of instructions preferably comprise one or more artificial neural networks (e.g. deep feedforward neural network, deep recurrent neural networks) and/or Artificial Intelligence (AI) algorithms for automatically causing the computing server to perform the authentication process. The AI algorithm may accurately process, verify and authenticate identities of the at least one external communication
25 device. The at least one external communication device is personalized (temporarily

or permanently) by a user (e.g. the auditor, the client and the responder) so that personal identity of the user is verified and/or authenticated by via authentication of the electronic identities of the at least one external communication device, particularly at scale if a plurality of cases are conducted by the electronic authentication system. For example, identification documents (e.g. identity cards, citizen cards, passports and driving licenses) are scanned and/or recorded for authentication depending on various elements of the identification documents. The elements include confirmation of genuine microprint text and security threads, validation of special paper and ink, comparison between OCR and barcodes and magnetic strips, data validity tests, and biometrics or facial recognition to link an individual to an ID credential. In contrast to trained humans, the electronic authentication system with the AI algorithm may be trained to detect these elements of the identification documents for differentiating fraudulent identifications from genuine identifications.

15

[0045] Often, the identification documents have complicated natures such as wear and tear, physical damages or impairments, manufacturing errors or defects, minor design changes or even variations in production depending on where and how the identification documents were produced. Therefore, the AI algorithm optionally comprises a semi-supervised learning model that would include the identification documents with these complicated variations. The AI algorithm may also have a feedback loop into which new data are fed. The feedback loop tests that the outcomes are consistent and improving. The outcomes are then fed into the AI algorithm so that the AI algorithm continues to learn and adjust.

25

[0046] The identification documents may comprise biometric identities (such as facial recognition or voice recognition), which are implemented as a more stringent security protocol. Accordingly, the AI algorithm optionally comprises a deep learning model to mimic the way human neurons process extremely difficult information such as faces and languages. The deep learning model learns to match images on the identification documents to faces of the users by looking for certain patterns of basic features of the faces (e.g. eyes, mouths, noses) and complex shapes of the faces (e.g. complete faces and distinctive shapes), and then returns outputs to indicate whether the images match the faces of the users.

10

[0047] Preferably, the artificial intelligence (AI) algorithm comprises a machine learning model, algorithm and/or software for the authentication process. The machine learning model may adopt various technologies, including but not limited to supervised learning, unsupervised learning, semi-supervised learning, ensemble learning, deep learning, reinforcement learning, regression, classification or clustering, outlier detection, metric learning and causality analysis. Examples of the machine learning model, algorithm or software includes CNTK, Deeplearning4j, ELKI, Keras, Caffe, ML.NET, Mahout, Mallet, mlpack, KNIME, Amazon Machine Learning, Angoss KnowledgeSTUDIO, Azure Machine Learning, Ayasdi, IBM Data Science Experience, Google Prediction API, IBM SPSS Modeler, KXEN Modeler, LIONSolver, Mathematica, MATLAB, Microsoft Azure, Neural Designer, NeuroSolutions, Oracle Data Mining, Oracle AI Platform Cloud Service, RCASE, SAS Enterprise Miner, SequenceL, Splunk and STATISTICA Data Miner.

15
20

[0048] Embodiments of the relevant invention or present application provide the processing unit that has an artificial intelligence (AI) accelerator for accelerating the artificial intelligence (AI) algorithm. Particularly, the artificial intelligence (AI) algorithm is configured to record, recognize, analyse, update patterns of authentication by the first external electronic device, the second external electronic device and/or the third external electronic device in order to facilitate reliable and efficient authentication. With increasing number of external electronic devices and authentication actions/processes, the AI algorithm can recognize genuine users or their personalized computing devices (e.g. external electronic device), and refuse authentication of bogus auditors.

[0049] The computing server is configured to hold a database configured to store information (e.g. personal data) of the client. Raw data of the information may come from various sources, such as historical records from business transactions, either inter-business deals (e.g. purchases, exchanges, banking or stock) or intra-business operations (e.g. management of in-house wares and assets), video and pictures from digital media (e.g. scanners, video cameras, digital cameras, smartphones, radio stations, television channels and film studios), textual reports and memos from companies and individuals, and even data from the World Wide Web repositories. The raw data is gathered in various forms from the various sources, such as numerical measurements, textual documents, spatial data, multimedia channels and hypertext documents.

[0050] Accordingly, the database may comprise one or more relational databases, object-relational databases and object-oriented databases, transactional databases,

unstructured and semi-structured repositories (such as the World Wide Web), advanced databases (such as spatial databases), multimedia databases, time-series databases and textual databases, and even flat files for storing the amalgam of raw data.

5

[0051] The artificial intelligence (AI) algorithm is optionally configured to increase or adjust its trust of authenticating the first external electronic device when noticing past successful authentication of the first external electronic device, the second external electronic device, the third external electronic device and/or the electronic authentication system for communication with other external electronic devices. For example, the artificial intelligence (AI) algorithm is sometimes configured to increase its trust of authenticating the first external electronic device when noticing past successful authentication of both the first external electronic device and the second external electronic device for communication with other external electronic devices.

10

15 The artificial intelligence (AI) algorithm is preferably configured to increase its trust of authenticating the first external electronic device when noticing past successful authentication of the first external electronic device, the second external electronic device and the third external electronic device for communication with other external electronic devices. In some cases, the artificial intelligence (AI) algorithm is

20 configured to refuse authentication if an identity of the first electronic device is not authorized.

[0052] Preferably, the computing server further comprises a database management system (DBMS) for managing the information. The database management system

25 (DBMS) needs not only to collect the raw data, but also to analyse the raw data

which are stored in disparate structures for information retrieval. The database management system (DBMS) is sometimes configured to extract knowledge from the information. The database management system (DBMS) may also conduct knowledge discovery databases (KDD) process for extracting non-trivial and
5 potentially useful, but implicit and previously unknown information from the raw data stored in the database.

[0053] Firstly, the database management system (DBMS) sets up a data warehouse by data cleaning for removing noise data and irrelevant data from the raw data, and
10 then conducts data integration for combining the raw data of heterogeneous formats into a single format. In other words, the data warehouse centralizes the raw data from various sources into a common repository. Therefore, the database management system (DBMS) may have a higher efficiency by retrieving the relevant data from the data warehouse, instead of obtaining the relevant data from multiple
15 resources respectively. In addition, data warehouse may comprise a multi-dimensional data cube structure of which ordinary cells are configured to store values of aggregate measurements and special cells are configured to store summations along dimensions. Each dimension of the multi-dimensional data cube structure contains a hierarchy of values for one attribute. In particular, the multi-
20 dimensional data cube structure is suitable for On-Line Analytical Processing (OLAP) for fast interactive querying and analysis of data at different conceptual levels.

[0054] Secondly, the Data Base Management System (DBMS) conducts data
25 selection for retrieving relevant data from the data warehouse in response to a

specific query and data transformation for appropriately consolidating the relevant data.

[0055] Thirdly, the database management system (DBMS) conducts data mining
5 (also known as data dredging or pattern discovery) for discovering potentially useful patterns from the consolidated data. The data mining is a critical step and may deploy various methods for assisting the discovery process. The data mining comprises descriptive data mining for describing general properties of the existing raw data and predictive data mining for attempting to predict based on inference of
10 the existing raw data. In particular, a compressive pattern discovery may be conducted by combining the data mining and the OLAP which are complementary in nature, i.e. the data mining conducts a bottom-up analysis while the OLAP conducts a top-down analysis. The OLAP may further comprise multi-dimensional OLAP (MOLAP), relational OLAP (ROLAP), hybrid OLAP (HOLAP) or any
15 combination thereof.

[0056] Finally, the database management system (DBMS) conducts data evaluation for identifying interesting patterns (i.e. knowledge) from the potentially useful patterns and knowledge presentation for visually representing and interpreting the
20 knowledge to the users (such as the auditors, the clients or any third party).

[0057] The data mining is particularly applicable to the World Wide Web which is the most heterogeneous and dynamic repository. Since the raw data in the World Wide Web are organized as interconnected documents, the World Wide Web comprises
25 three major components, i.e. content of the Web for available documents, structure

of the Web for hyperlinks and relationships between the available documents, and usage of the Web for description of how and when the available documents are accessed. Accordingly, the data mining in the World Wide Web comprises web content mining, web structure mining and web usage mining.

5

[0058] Preferably, the database management system (DBMS) is configured to automatically update the information of users and/or their personalized electronic devices, including clients, responders and auditors. In addition to the trustable external sources, the database management system (DBMS) may also
10 automatically update the information from other external sources since the data warehouse is able to not only update the information consistently from the raw data but also secure the database regardless of the external resources.

[0059] Embodiments of the relevant invention provide the database management
15 system (DBMS) with a cloud Application Programming Interface (API) for providing inter-cloud compatibility. The cloud-based electronic authentication system may comprise multiple clouds which have different managing mechanisms for storing and updating data from various sources. Since the data from multiple clouds may be integrated into a unified platform during authentication, the database management
20 system (DBMS) comprises the cloud Application Programming Interface (API) as a computing interface between the multiple clouds for providing inter-cloud compatibility to the data.

[0060] In some implementations, the cloud API has an in-process APIs as a set of
25 net-based APIs accessible to plugins that enable direct interaction between the

multiple clouds. In some implementations, the cloud API has a remote APIs including web-services (SOAP or REST), remote calls (Sun RPC, Java RMI) and application dependent protocols (FTP, SNMP). The remote API is based on HTTP and SHTTP protocols which are suitable for GET, PUT, POST and DELETE requests. In addition, the cloud API has a two-stage API access control mechanism using a role based access control model in which access is provided to users based on roles assigned to the users. In other words, each user is assigned with a specific role and thus serves as a connecting layer between the user and the permissions assigned to the user.

10

[0061] Preferably, the database management system (DBMS) comprises a big data-based authentication framework for combining a “something-you-do” model as a fourth type of electronic credential (i.e. type 4) and applications of big data technology in authentication. More preferably, the database management system (DBMS) comprises a blockchain protocol for verifying the information. The blockchain (i.e. block chain) protocol decentralizes ownership of credentials and thus offers a universally available protocol for verifying the information of the users (i.e. the auditors, the clients and the responders). Security of the information stored in the blockchain is derived from a proof of work problem which is design to take a large amount of computational power to complete such that a single person may work for years but a network of computers may take only a few minutes to complete. The blockchain protocol comprises a shared ledger for storing the information; and the shared ledger can be downloaded by the users for retrieving the stored information.

25

[0062] The blockchain protocol builds up an immutable chain of data based on consensus, distribution and trustless of the blockchain for guaranteeing security of the information. Firstly, the public ledger is chosen by consensus of all the users who agree on a longest chain as a recognized chain of the blockchain protocol. The longest chain cannot be mathematically altered by any individual user since all the users would add new blocks to the recognized chain much faster than the individual user to construct a new longest chain as a new recognized chain, due to nature of the work problem. Therefore, fake information cannot be made up by any individual user to the database management system (DBMS). Secondly, the trustless character of the blockchain protocol makes a third party unnecessary to authenticate the information; and any malicious party or careless party is prevented to intentionally or accidentally authenticate fake information into the database management system (DBMS). Thirdly, the public ledger is stored by all users and thus distributed all over the blockchain protocol. In traditional cryptography, a single point of truth could be a certificate authority, and a malicious attacker could replace stored keys with his or her own keys for masquerading users if certificate authority is breached in the traditional cryptography. In contrast, the malicious attacker would have to breach every member machine of each user since the public ledger is distributed in each member machine in the blockchain protocol.

20

[0063] The blockchain protocol assigns a blockchain ID which is essentially a block of data on the recognized chain that can be verified. In particular, the blockchain protocol comprises an Elliptic Curve Digital Signature Algorithm (ECDSA) for binding a public key by default and then transferring ownership of the private key to the user when a blockchain ID is added to the blockchain protocol. Therefore, only the user

25

is allowed to sign a signature that can be verified against the public key stored in the blockchain protocol. As a decentralized source of authentication, the blockchain protocol essentially becomes a single-sign-on portal that may be accessed by any app while not owned by any single entity. The blockchain protocol would only have
5 to request a digital signature and a blockchain ID from a user who requests access to the Database Management System (DBMS) by confirming that the signature is valid and that the user's blockchain ID verifies who the user say who he or she is.

[0064] In addition, the blockchain protocol may be further integrated with current
10 multiple-factor authentication methods. The blockchain protocol would serve as an extra layer of security to the electronic authentication system while not scrap habits of the users who are familiar with the multiple-factor authentication methods. For example, a common two-factor authentication method may send a code over short message service (SMS) which is well-known as insecure, since a potential attacker
15 could sniff messages in addition to spoofing the sender of the message. For another example, current special two-factor authentication methods (such as Google Authenticator) may be secure, but owners of the special two-factor authentication methods have access to all two-factor codes which maybe leaked out when the owners are breached. The blockchain protocol would solve both the security concern
20 and the owner concern by distributing the two-factor codes over the recognized chains.

[0065] The computing server or the electronic authentication system is configured to send an alert signal (i.e. a WhatsApp message or an email) to any of the first

external electronic device, the second external electronic device and the third external electronic device.

[0066] According to a fourth aspect, the present application provides an electronic authentication process for financial auditing. The electronic authentication process comprises a first step of authenticating a first external electronic device; a second step of authenticating a second external electronic device; and a third step of providing authorization information of the first external electronic device and the second external electronic device to each other for authorizing electronic communication between the first external electronic device and the second external electronic device after authenticating the first external electronic device and the second external electronic device. Some of these steps may be changed in sequence, combined or separated. For example, the first and second steps can possibly be combined so that the first external electronic device and the second external electronic device can be authenticated in a reverse order or together.

[0067] The electronic authentication process may further comprise a step of authenticating a third external electronic device; and another following step of providing authorization information of the third external electronic device to the first external electronic device, the second external electronic device or both after authenticating the third external electronic device. The electronic authentication process optionally further comprises a step of initiating a confirmation request from the first external electronic device of an auditor to an electronic authentication system; a step of authorizing the confirmation request from the second external electronic device of a client to the computing server; and a step of responding the

confirmation request from the third external electronic device of a responder to the computing server. The first external electronic device, the second external electronic device, the third external electronic device or a combination of any of these devices are possibly configured to be authenticated by the electronic authentication system.

5

[0068] Embodiments of the electronic authentication process further comprise a step of authenticating electronic identity of the second external electronic device before sending the confirmation request to the second external electronic device. The embodiments preferably further comprise a step of updating electronic authentication system with the electronic identity of the second external electronic device. The embodiments may further comprise a step of sending warning signals to the electronic authentication system, the first external electronic device, the second external electronic device, the third external electronic device or a combination of any of these devices in case of failure of authentication. The

10

15

embodiments may additionally comprise a step of authenticating the first external electronic device, the second external electronic device or both via reciprocal exchange of authorized electronic signals between the computing server and one of the two external electronic devices.

20 [0069] Preferably, the electronic authentication process may further comprise a step of communicating with the first electronic device, the second electronic device or both via the electronic communication network. Sometimes, the electronic authentication process further comprises a step of giving a predetermined scope of authorization to the first electronic device, the second electronic device, the third

25

external electronic device or a combination of any of these devices. When required,

the electronic authentication process further comprises a step of accrediting (e.g. approving delegation of authentication) from one of the first external electronic device, the second external electronic device, the third external electronic device to another electronic device. In some cases, the electronic authentication process

5 further comprises a step of communicating with the first electronic device, the second electronic device, the third external electronic device, a cloud computing device or a combination of any of these devices continually, continuously or automatically. In some instances, the electronic authentication process further comprises a step of embedding authentication information of the electronic

10 authentication system into an electronic report which could accessed by the first electronic device, the second electronic device, the third external electronic device or the cloud computing device.

[0070] Other embodiments of the application offer the electronic authentication

15 process that further comprises a step of causing the computing server to perform an authentication process by an artificial intelligence (AI) algorithm automatically. The other embodiments can further comprise a step of incorporating a machine learning model for the authentication process. The other embodiments optionally include the electronic authentication process that further comprises a step of incorporating a

20 database management system (DBMS) for managing the electronic authentication process, another step of including cloud Application Programming Interface (API) for providing inter-cloud compatibility, or both.

[0071] According to a fifth aspect, the present application provides a non-transitory,

25 computer-readable medium storing one or more instructions executable by an

electronic authentication system to perform authentication process to external electronic devices for financial auditing. The process comprises following steps, namely a first step of authenticating a first external electronic device; a second step of authenticating a second external electronic device; and a third step of providing
5 authorization information of the first external electronic device and the second external electronic device to each other for authorizing electronic communication between the first external electronic device and the second external electronic device after authenticating the first external electronic device and the second external electronic device. Some of these method steps may be combined, divided,
10 changed in sequence (e.g. reversed).

[0072] The accompanying figures (Figs.) illustrate embodiments and serve to explain principles of the disclosed embodiments. It is to be understood, however, that these figures are presented for purposes of illustration only, and not for defining limits of
15 relevant applications.

- Fig. 1 illustrates a diagram of a known manual authentication process;
- Fig. 2 illustrates a diagram of an electronic authentication process and its corresponding electronic authentication system;
- Fig. 3 illustrates a diagram of a cloud-based electronic authentication system;
- 20 Fig. 4 illustrates a diagram of a client communication device of the cloud-based electronic authentication system;
- Fig. 5 illustrates a diagram of a computing server (either a local server or a remote server) of the cloud-based electronic authentication system;
- Fig. 6 illustrates an exploded view of a cloud service architecture of the cloud-
25 based electronic authentication system;

- Fig. 7 illustrates an overview of an authentication procedure of the electronic authentication process;
- Fig. 8 illustrates a diagram of an Artificial Intelligent (AI) platform of the cloud-based electronic authentication system;
- 5 Fig. 9 illustrates an electronic authentication system for authenticating a single external electronic device; and
- Fig. 10 illustrates that the computing server comprising a communicating unit for communicating with external electric devices.
- 10 [0073] Fig. 1 illustrates a diagram of an existing manual authentication process 100. Three independent parties are involved in the existing manual authentication process 100, i.e. an auditor (also known as preparer) 102, a client (also known as authorizer) 104 and a responder 106. The auditor 102 is a licensed auditor, accountant or with other equivalent qualifications to initiate a confirmation request
- 15 108. The client 104 is an authentic recipient (such as directors or other high-level managers) who authorizes the confirmation request 108. The responder 106 is capable of responding the confirmation request 108. The authentication process 100 comprises a first step 110 of sending by the auditor 102 the confirmation request 108 via a deliver method, such as post of a hardcopy of the confirmation request
- 20 108 or email of a softcopy of the confirmation request 108; a second step 112 of authorizing by the client 104 the confirmation request 108 and sending the authorization back to the auditor 102 also via the deliver method; a third step 114 of sending by the auditor 102 the confirmation request 108 to the responder 106 via the deliver method; a fourth step 116 of signing by the responder 106 the
- 25 confirmation request 108 and sending the signature back to the auditor 102 via the

deliver method; and a fifth step 118 of preparing an authentication report 120 and complete the authentication process 100.

[0074] The known or existing manual authentication process 100 has several
5 significant disadvantages. Firstly, the existing manual authentication process 100 cannot identify whether the auditor 102 is a licensed auditor or accountant; and thus cannot prevent an unlicensed auditor or bogus accountant from malicious actions. Since the auditor 102 has a controlling power over the existing manual authentication process 100, the unlicensed auditor or bogus accountant would bring
10 immeasurable harm to the client 104 and/or the responder 106 and cause a massive decrease in a response rate of the existing manual authentication process 100. Secondly, the existing manual authentication process 100 cannot identify whether the client 104 is the authentic recipient (such as directors or other high-level managers) at the client 104 who has the right to authorize the confirmation request
15 108. Since the deliver method cannot prevent another person (such as a clerk or low-level manger) who does not have the authorization right at the client 104 from getting access to the confirmation request 108, the existing manual authentication process 100 may be easily intercepted and/or manipulated maliciously. Thirdly, the existing manual authentication process 100 cannot identify whether the responder
20 106 is a capable responder or genuine owner and whether the responder 106 has the capacity to respond the confirmation request 108, which would defeat purpose of authentication. Fourthly, the deliver method is too slow which may take about 2 to 6 weeks for the first step 110 and the second step 112 and about another 4 to 6 weeks for the third step 114 and the fourth step 116 of the existing manual
25 authentication process 100. Last but not the least, the responder 116 may either

intentionally or unintentionally ignore the confirmation request 108, the existing manual authentication process 100 cannot urge the responder 106 to act in a timely manner.

5 [0075] Fig. 2 illustrates a diagram of an electronic authentication process 200 and its corresponding electronic authentication system 201. Similarly, three independent parties are involved, i.e. an auditor (also known as preparer) 202, a client (also known as authorizer) 204 and a responder 206 in relation to an electronic confirmation request 208. In addition, the electronic authentication system 201 has

10 a computing server 210 and a communication network 212 which are communicatively connected. In particular, the auditor 202, the client 204 and the responder 206 respectively have a first external electronic device (also known as an auditor communication device) 214, a second external electronic device (also known as a client communication device) 216, a third external electronic device (also known

15 as a responder communication device) 218, all of which are also communicatively connected to the communication network 212. The communication devices 214-218 may be also known as mobile station, mobile terminal, subscriber station, remote station, user terminal, terminal, subscriber unit, access terminal, etc. The communication devices 214-218 (particularly the client communication device 216

20 and the responder communication device 218) are mobile or portable devices, including but not limited to laptop, mobile phone, cordless telephone, pager, personal digital assistant, enterprise digital assistant, smartphone or other small computing handheld device with a display screen and input/output interface. In particular, the responder communication device 218 should be capable of executing

25 instructions given by the computing server 210. Therefore, the communication

devices 214-218 may exchange information with the computing server 210. In addition, all the information exchange via the communication network 212 is encrypted such that the information would not be intercepted by any unauthorized receiver. In some implementations, Hypertext Transfer Protocol Secure (HTTPS) is adopted as the encryption method for guaranteeing security of data transmission. HTTPS is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computing network such as the Internet. Communication protocol of HTTPS is encrypted using Transport Layer Security (TLS) or Secure Sockets Layer (SSL). For authentication purpose, HTTPS requires a trusted third party to sign server side digital certificates. However, full authenticated HTTPS connections to the communication network 212 may incur high costs, similar to other secured corporate information systems on the World Wide Web, such as some proprietary accounting software packages.

[0076] In contrast to the deliver method in the existing manual authentication process 100, various electronic authentication means may be adopted in the electronic authentication process 200 to identify the auditor 202, the client 204 and the responder 206, such as authentic pin number (APN), biometric verification, peripheral device recognition, computer recognition or any other authentication mean which allows the computing server 210 to recognize and verify the genuine auditor 202, the client 204 and the responder 206. For example, the client 204 receives an APN from the computing server 210 for completing authorization of the electronic confirmation request 208 by keying in the APN into a pre-determined web portal within the client communication device 216. The APN may be sent to the client 204 in various ways, such as short message service (SMS), social medium

programs or applications (such as WhatsApp or WeChat), specific programs or applications, or in other dynamic modes to the client communication device 216. For another example, the electronic authentication means may be provided in the social medium applications or specific applications without receiving APN, where electronic

5 credentials of the client 204 is transmitted to the computing server 210. Alternatively, the electronic authentication means may be directly embedded in the client communication device 216 which would transmit electronic credentials of the client 204 to the computing server 210, In contrast to the traditional delivering method in which post of a hardcopy or email of a softcopy of the confirmation request 108 may

10 be forwarded to other persons (such as a secretary of the client 204) without any restriction, the electronic authentication means is not easily forwarded or disclosed to any communication device other than the specific client communication device 216. For example, the electronic authentication means sends an encrypted electronic link to the communication devices 214-218 only after an intended recipient

15 as the auditor 202, the client 204 or the responder 206 has been authenticated. If the encrypted electronic link is forwarded to another electronic device, the electronic link will automatically become invalid and meanwhile an electronic warning signal would be sent to the computing server 210. Since the encrypted electronic link includes electronic identities or credentials of the intended electronic device, such

20 as MAC (Media Access Control) address of the intended electronic device, the encrypted electronic link become invalid when sent to another electronic device. Meanwhile, the communication devices 214-218 may also be respectively pre-assigned with a unique ID in numeric, alphabetic or alphanumeric form. The unique ID is registered in the computing server 210 for identifying each of the

25 communication devices 214-218. Therefore, the electronic authentication process

200 may provide a better authentication of auditor 202, the client 204 and the responder 206 by combining the electronic authentication means and the unique ID of the communication devices 214-218.

5 [0077] As shown in Fig. 2, the electronic authentication process 200 comprises a first step 220 of sending by the auditor 202 the electronic confirmation request 208 from the auditor communication device 214 to the computing server 210 via the communication network 212; a second step 222 of sending automatically by the computing server 210 the electronic confirmation request 208 to the client 204 via
10 the communication network 212; a third step 224 of authorizing by the client 204 the electronic confirmation request 208 and then sending the authorization back to the computing server 210 via the communication network 212; a fourth step 226 of sending automatically by the computing server 210 the electronic confirmation request 208 to the responder 206 via the communication network 212 after the
15 computing server 210 checks the authorization; a fifth step 228 of signing by the responder 206 the electronic confirmation request 208 and sending the signature and/or confirmation back to the computing server 210 via the communication network 212; and a sixth step 230 of downloading an authentication report 232 by the auditor 202 from the computing server 210 via the communication network 212
20 and then completing the electronic authentication process 200. In contrast to the auditor 102 in the existing manual authentication process 100, the computing server 210 has a dominate position in the electronic authentication process 200 for preventing any malicious inference from the auditor 202 or any other person. In addition, the authentication report 232 is prepared automatically by the computing
25 server 210 for avoiding any human error that may be easily made by the auditor 202.

[0078] In the first step 220, the computing server 210 would automatically identify the auditor 202 using any of the electronic authentication means at the time or later when the auditor 202 initiates the electronic confirmation request 208. In other words, only the authenticated auditor 202 is allowed to use the electronic authentication system 201. Moreover, the electronic authentication system (also known as Authentic Practitioner Solution) can operate independently or cooperatively with other hardware or software systems. For example, suitable APIs (application program interfaces) may be provided for exchanging data with office suites (e.g. Microsoft Outlook®) for the convenience of auditing, accounting or other professionals.

[0079] In particular, the computing server 210 may have a database configured to store information of the auditor 202 before the electronic authentication process 200. The auditor 202 is required to submit its information (such as the auditor or accountant's license) to the computing server 210 along with the electronic confirmation request 208. The computing server 210 thus compares the stored information with submitted information of the auditor 202 for figuring out whether the auditor 202 is genuine. The computing server 210 may retrieve and collect the information of the auditor 202 from external sources (such as professional organizations of licensed accounts) for updating the stored information of the auditor 202. In addition, the computing server 210 may also check whether the electronic confirmation request 208 is sent from the auditor communication device 214 with the unique ID. Since only licensed auditor or accountant is made accessible to the

auditor communication device 210 (such as his or her personal phone), the first issue of unlicensed auditor or bogus accountant is solved.

[0080] In the second step 222 and the fourth step 226, the computing server 210
5 would send the electronic confirmation request 208 to the client communication device 216 and the responder communication device 218, respectively. Since the client communication device 216 and the responder communication device 218 are also only accessible to the client 204 and the responder 206 respectively, the client 204 and the responder 206 are guaranteed as genuine authorizer and the capable
10 respondent. Therefore, the second issue and the third issue stated above with the existing manual authentication process 100 are solved.

[0081] In the third step 224 and the fifth step 228, the computing server 210 would automatically identify the client 204 and the responder 206 using any of the
15 electronic authentication means at the time when the client 206 and the responder 206 send authorization and response to the electronic confirmation request 208, respectively. Similarly, the computing server 210 may have databases configured to store information of the client 204 and the responder 206 before the electronic authentication process 200. The client 204 and the responder 206 are required to
20 submit their information to the computing server 210 along with sending authorization and response to the electronic confirmation request 208, respectively. The computing server 210 thus compares the stored information with submitted information of the client 204 and the responder 206 respectively for figuring out whether the client 204 and the responder 206 are genuine. The computing server
25 210 may retrieve and collect the information of the client 204 and the responder 206

from external sources (such as client official websites, trustable third parties including stock exchange announcements if the client is publicly listed, or professional organizations of responders) for updating the stored information of the client 204 and the responder 206. In particular, a set of rules may be stored in the
5 computing server 210 for rating responding service provided by the responder 206, especially response time of the responder 206 which is determined as a time interval between the fourth step 226 and the fifth step 228.

[0082] The authentication of the client 204 and/or the responder 206 may be proved
10 in a three-tier hierarchical mechanism. In the first tier (also known as an absolute tier), the client 204 and/or the responder 206 is proved to be absolutely capable. In other words, the first tier has only two results, i.e. "YES" for a capable client and/or responder; and "NO" for an incapable client and/or responder. The first tier may adopt any possible means to prove authentication of the client 204 and/or the
15 responder 206. For example, the computing server 210 automatically collect information from official sources or government organizations (such as Companies Commission of Malaysia (CCM) or Accounting and Corporate Regulatory Authority (ACRA) of Singapore). However, the official sources or government organizations may be slow to update the information or impossible to provide information of some
20 specific client 204 and/or responders 206. Therefore, the computing server 210 also collects information from other auditors 202 who vouch specific client 204 and/or responders 206 are authentic. In this way, updated information or additional information of the specific client 204 and/or responder 206 are also included in the computing server 210 for making a comprehensive database of the client and/or
25 responders 206.

[0083] In the second tier (also known as relative tier), the client 204 and/or the responder 206 is proved to be relatively capable. In some implementations, an artificial intelligence (AI) weighted method is used to calculate relative capability for enhancing credibility of the client 204 and/or the responder 206. For example, multiple confirmation cases may be referred to the same responder 206 by multiple auditor 202. If one of the multiple auditors 202 has authenticated or confirmed the responder 206 and then provided remarks or scores in relation to the responder 206 in the computing server 210 accordingly, others of the multiple auditors 202 may give more credits to the same responder 206 in their respective confirmation cases. In some implementations, the auditor 202 may call the client 204 to confirm the authentic recipient (such as directors or other high-level managers) and his or her phone number are correct. Then the authentic receipt and his or her phone number are recorded in the computing server 210. It is understood that other commonly known manners of confirming the responder 206 or other intended recipients are also within scope of the subject invention. For example, the auditor 202 may make a visit to the responder 206 by himself or herself and then confirm with the responder 206 face-to-face. Thus, the auditor 202 may refer to or vouch a specific responder 204 if his or her authentication could be found in the computing sever 210 in a later confirmation case. Of course, the auditor 202 may choose to adopt his or her convenient method to authenticate the responder 206 and then confirm with record of the responder 206 in the computing server 210.

[0084] In the third tier (also known as weightage tier), the computing server 210 optionally adopts technologies of data analysis or data mining to find out any

indication or evidence of authentication of the client 204 and/or the responder 206 (such as a specific company or an intended receipt). In some implementations, the computing server 210 sets up an artificial intelligence (AI) frame to automatically conduct the data analysis or data mining. The AI frame significantly enhances
5 efficiency of data analysis and data mining by carefully designing AI algorithm and logic reasoning.

[0085] In the authentication process, various models may be adopted, including “something-you-know” model (i.e. type 1), “something-you-have” model (i.e. type 2),
10 “something-you-are” model (i.e. type 3) as well as “something-you-do” model (i.e. type 4). The “something-you-know” model includes passwords, PINs, Authentic Pin Number (APN), code words, secret handshakes, geographical location (e.g. GPS signals), and any other methods of authentication a user creates. The “something-you-have” model includes smartcards, cell phones (i.e. mobile phones), security
15 tokens, and any other methods of authentication a user has. The “something-you-are” model is based on biometric traits such as fingerprints, retina scan, palm prints, facial recognition, speech recognition and walking posture. All the three authentication models may be susceptible to breach. While the “something-you-do” model is based on dynamic biometrics and behavioural patterns, such as voice
20 patterns, handwritings and typing rhythms. In addition, multiple-factor authentication model may be also adopted by combining any two or more of the four models above.

[0086] In particular, the “something-you-do” mode (i.e. type 4) may be combined with big data technology for forming a big data-based authentication framework for
25 leveraging characteristics of the big data, i.e. volume, velocity and variety into the

authentication process. Beforehand, big data is established about a user by gathering his or her behaviours and information, such as logs, events, telephone records, alerts, customer transaction, web page text, GPS tracking, network flows, social data, blogs, tweets and chats. The big data-based authentication framework

5 comprises three components: a data security-based analytics (DSA), a big data-driven authentication (BDA) tool, and software as a service (SaaS) authentication tool. The DSA leverages large scale data processing engines (such as Spark and Hadoop) to provide real-time identification of data with security potentials for capturing and analysing big datasets in real-time. The BDA tool then manages to

10 cluster outcomes of the DSA into human dynamic based information for creating security profiles based on actions and behaviours of humans. The BDA tool has a just-in-time human dynamic authentication engine (JitHDA) for generating random set challenging questions one of which relate to actions performed by a user. The randomness creates a certain level of uncertainty for preventing any attacker from

15 acquiring knowledge about which question relates to the certain user. The SaaS authentication tool finally promotes the authentication service from the cloud.

[0087] Fig. 3 illustrates a diagram of a cloud-based electronic authentication system 600 for performing the electronic authentication process 200. The cloud-based

20 electronic authentication system 600 has an authentication application 602 which is implemented as cloud application architecture 604. Other components of the cloud-based electronic authentication system 600 are communicatively connected to the cloud application architecture 604, including a local server 606, multiple client communication devices (such as a first client communication device 608 and a

25 second client communication device 610), and a cloud service architecture 612. In

particular, the local server 606 has a local non-volatile memory such that information may be transmitted between the local server 606 and the cloud application architecture 604 in a two-way configuration, i.e. the information may be uploaded to and downloaded from the cloud application architecture 604; while the client communication devices 608, 610 and the cloud service architecture 612 may work in a two-way configuration, i.e. information could be either uploaded to or downloaded from the cloud application architecture 604. The cloud service architecture 612 further comprises a service database 614, a service server 616 and an artificial intelligence (AI) cloud processor 618, all of which are communicatively connected with the cloud service architecture 612 in a two-way configuration. The artificial intelligence (AI) cloud processor 618 is configured dedicatedly to run an artificial intelligence (AI) algorithm for performing the electronic authentication process 200 automatically and wisely. For example, the artificial intelligence (AI) algorithm may identify duplicated responders that have been recorded in the authentication application 602; and then merge the duplicated responders into a single responder. For another example, the artificial intelligence (AI) algorithm has a learning capability as to identify behaviours of a specific responder from his or her past experiences and then determine types and frequencies of reminders sent to the responder for reminding the specific responder to respond in a timely manner.

20

[0088] Fig. 4 illustrates a diagram of the client communication device 608, 610 the cloud-based electronic authentication system 600 with multiple units, including an interface 620 (such as a screen) for the client 204 to interact with the client communication device 608, 610; a main memory 622 for storing the instructions; a processor 624 (such as central processing unit (CPU)) for executing the stored

25

instructions; a Random Access Memory (RAM) 626 for exchanging data between the main memory 622 and the processor 624; a storage 628 for permanently storing information; and other peripheral units such as an input device 630 configured to enable user to input information, digitalize the input information and provide the

5 digitalized input information to the client communication device 608 and an output device 632 configured to provide the user with an output generated by the client communication device 608. Examples of the input-and/or output devices 630, 632 include a monitor, a speaker, a printer, a projector, a keyboard, a pointing device, a scanner, a personal digital assistant, a microphone and other electronic devices. It

10 will be appreciated by that the term 'user' as used herein relates to any entity including a person (i.e., human being), or a virtual personal assistant (an autonomous program or a bot) using a device and/or system described herein.

[0089] Fig. 5 illustrates a diagram of the local server 606 of the cloud-based

15 electronic authentication system 600. The local server 606 relates to a structure and/or module that include(s) programmable and/or non-programmable components configured to store, process and/or share information. The local server 606 includes one or more data processing facilities for the storing, processing and/or sharing data and/or setting instruction. Furthermore, the local server 606 includes

20 hardware, software, firmware or a combination of these, suitable for storing and processing various information and services accessed by the one or more user using the one or more computing device (such as the client communication devices 608, 610). Optionally, the local server 606 includes any arrangement of physical or virtual computational entities capable of enhancing information to perform various

25 computational tasks. Furthermore, it should be appreciated that the local server 606

may be both single hardware server and/or a plurality of hardware servers operating in a parallel or distributed architecture. Optionally, the local server 606 is implemented as a computer program that provides various services to other devices, modules or apparatus. For example, the local client 606 has a main memory 634 for

5 storing the instructions; a processor 636 (such as central processing unit (CPU)) for executing the stored instructions; a Random Access Memory (RAM) 638 for exchanging data between the main memory 634 and the processor 636; a storage 640 for permanently storing information; and peripheral devices 650 for a user to communicate with the local server 606, including but not limited to a handheld device

10 642 (such as hand phone or tablet), a printing device 644 (such as printer), a workstation 646, and a personal computer 648 (such as desktop or laptop). It will be appreciated by that the term 'user' as used herein relates to any entity including a person (i.e., human being), or a virtual personal assistant (an autonomous program or a bot) using a device and/or system described herein.

15

[0090] Fig. 6 illustrates an exploded view of the cloud service architecture 612 of the cloud-based electronic authentication system 600. The cloud service architecture 612 has a processing unit 652, a memory unit 654 including multiple instructions and an artificial intelligent (AI) algorithm 656, and a database 658.

20

[0091] Fig. 7 illustrates an overview of an authentication procedure 1700 of the electronic authentication process 200. The authentication procedure 1700 includes a data processing platform 1702 including logical modules 1704 implemented as an application tier-Intelligent risk algorithm module (IRA), 1710 as OMM App, 1712 as

25 Overall Materiality Module Database, 1714 as Cognition AI, 1716 as audit strategy

(AS), 1718 as business environment (BE), 1720 as internal control (IC), 1722 as management meeting (MM), 1724 as preliminary analytical review (AR), 1726 as risk consideration (RC), 1728 as assertion risk assessment (AS), 1730 as financial statement assessment (FS), 1732 as performance materiality (PM), 1734 as audit
5 program (AP), and a database 1706. Further, the authentication procedure 1700 also includes a sequence showing the plurality of events numbered as 1 as start (ST), 2 as overall materiality (OM), 3 as business environment (BE), 4 as internal control (IC), 5 as management meeting (MM), 6 as preliminary analytical review (AR), 7 as risk consideration (RC), 8 as audit strategy (AS), 9 as financial statement
10 assessment (FS), 10 as risk response summary (RR), 12 as risk response implementation (RRI). It will be appreciated logical modules 1704 implemented as an application tier-Intelligent risk algorithm module (IRA), 1710 as OMM App, 1712 as Overall Materiality Module Database, 1714 as Cognition AI, 1716 as audit strategy (AS), 1718 as business environment (BE), 1720 as internal control (IC),
15 1722 as management meeting (MM), 1724 as preliminary analytical review (AR), 1726 as risk consideration (RC), 1728 as assertion risk assessment (AS), 1730 as financial statement assessment (FS), 1732 as performance materiality (PM), 1734 as audit program (AP) requests multiple inputs from the user and at the events in the sequence, namely the 1 as start (ST), 2 as overall materiality (OM), 3 as
20 business environment (BE), 4 as internal control (IC), 5 as management meeting (MM), 6 as preliminary analytical review (AR), 7 as risk consideration (RC), 8 as audit strategy (AS), 9 as financial statement assessment (FS), 10 as risk response summary (RR), the user provides its inputs. Subsequently, a data processing platform 1702 depicted as server arrangement in the electronic authentication
25 process 200 at the event A provides report describe the performance materiality

(PM) of the entity, at the event B provides report describe the audit program (AP) for the entity, at the event C provides report describe the sample size (SS) for the entity, and at the event 11 provides report describe the audit planning memo (APM) for the entity and at 12 provides report describing the risk response implementation (RRI).

5

[0092] Fig. 8 illustrates a diagram of an artificial intelligent (AI) platform 700 of the cloud-based electronic authentication system 600. The artificial intelligent (AI) platform 700 has a traffic manger 710, such as a DNS-based traffic load balancer. Multiple users 720 are communicatively connected to the traffic manger 710. The traffic manger 710 enables the user to distribute traffic optimally to services across global regions. The traffic manager 710 uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. An endpoint is any Internet-facing service hosted inside or outside of the artificial intelligent (AI) platform 700. The traffic manager 710 provides a range of traffic-routing methods and endpoint monitoring options to suit different application 730 needs and automatic failover models. Therefore, the traffic manger 710 provides significant advantages to the artificial intelligent (AI) platform 700, such as increasing application availability, improving application performance, performing service maintenance without downtime, combining hybrid applications 730 and distributing traffic for complex deployments. The applications 730 may include a mobile application 732 and a web application 734. The applications 730 are designed for providing multiple services 740, including a natural language processing service 742, an index search service 744, and a SQL database 746. The services 740 is optionally provided through a cloud computer service 750 (such as artificial intelligence (AI) operating desk) for getting access to the application 730.

25

[0093] In one implementation, Microsoft Azure (also known as Window Azure) is adopted as the artificial intelligent (AI) platform 700. Microsoft Azure provides application services, cloud services, SQL database services and search services.

5 The application services include S3 at max of 10 instances, 7GB RAM, processor with 4 cores, and storage of 50GB; the cloud services include standard D3_V2 having 14GB RAM, a processor with 4 cores, storage of 200GB SSD, and high-speed network (network 4); the SQL database services include S4 DTU with a max size of 200, max concurrent 400, and storage of 250GB; and the search services

10 include standard S1 DTU, storage of 25GB with max of 300GB documents per service, and 50 indexes per service. It is appreciated to note that other artificial intelligent (AI) platforms are also applicable to the electronic authentication process, including but not limited to Google AI platform, TensorFlow, Rainbird, Infosys Nia, Wipro HOLMES, Dialogflow, Premonition, Ayasdi, MindMeld, Meya, KAI, Vital A.I.,

15 Receptiviti, Watson Studio, Lumiata, and Infrd.

[0094] Fig. 9 illustrates an electronic authentication system 201 for authenticating a single external electronic device 214, which is another embodiment of the relevant invention. In the present case, the electronic authentication system 201 includes a

20 computing server 210 (i.e. server) in a data centre, which is also connected to an external telecommunication network 212. An auditor 202 has a Personal Computer 214 that is remotely connected to the computing server 210. The Personal Computer is alternatively known as the auditor communication device 214. In use, the auditor logs into the Personal Computer 214 such that the Personal Computer 214 becomes

25 personalised. Though physical components or structure of the Personal Computer

214 is not changed, the Personal Computer 214 becomes a personal electronic device that is uniquely accessed and identified with the auditor 202. After logging in (logging on, signing in, or signing on), the auditor 202 gains access to the Personal Computer 214 by identifying and authenticating the auditor himself. For example,

5 the auditor scans his thumbprints (i.e. fingerprints), irises and/or retinas by the Personal Computer 214 such that the auditor 202 enters his user account of the Personal Computer 214. The Personal Computer 214 becomes personalised by the auditor 202 because predetermined applications and user interfaces become available to the auditor 202. The auditor 202 is enabled to access one or more email

10 accounts, messages (e.g. WhatsApp messages, LINE messages, Telegram messages) and network drives or folders, which are not available to others, which are uniquely identified and accessible by the auditor 202. The Personal Computer 214 thus becomes an external electronic device, a personalised electronic device, a personal electronic communication device, an external communication device, a

15 personal communication device or a portable electronic device, which is communicatively connected to the computing server 210 via the communication network 212.

[0095] Since a database of the computing server 210 holds the latest and past

20 records of licensed auditors and their electronic identities (e.g. telephone number, email address), the computing server 210 is able to communicate to a designated auditor according to registered electronic identities of the designated auditor by electronic communication via the multiple electronic identities. For example, the computing server 210 sends an OTP (One Time Password) or APN (Authentic Pin

25 Number) text message via SMS (short message service) to a registered mobile

number of the designated auditor and waits for a verification message from the designated auditor 202 via another form of electronic message, such as by email or WhatsApp. The OTP or APN would be then entered into the electronic authentication system 201 for authenticating purposes. If the OTP or APN is received from the other
5 form of electronic message to be identical to the OTP or ATP, the computing server 210 recognises and authenticates the Personal Computer 214, which is uniquely accessed & utilised by the auditor 202. Otherwise (e.g. OTP or APN via SMS and WhatsApp not matching), the computing server 210 rejects authentication of the Personal Computer 214 and refuses access by the Personal Computer 214. The
10 computing server 210 further sends alert or alarm message to an operator of the computing server 210 for further actions.

[0096] Since the computing server 210 periodically downloads and updates its database on licensed auditors, the database holds electronic identities of the
15 licensed auditors. The computing server 210 has an internet bot (i.e. web robot, robot or bot) that further collects, compares and verifies electronic identities of the licensed auditors progressively. Accordingly, the computing server 210 can easily recognise bogus auditors or unlicensed auditors if their electronic identities do not match with those on the database. Of course, the database further holds electronic
20 identities of people who are authorised and/or delegated by the licensed auditor 202. The computer server 210 becomes a filter that automatically rejects fake auditors.

[0097] Fig. 10 illustrates that the computing server (local sever) 210 comprises a communicating unit 1800 for communicating with the external electric devices 216,
25 218. Referring to Fig. 10, the communicating unit (also known as communication

unit) 1800 includes a control logic 1802, a memory 1804, a medium access control (MAC) unit 1806 and a DMA (direct memory access) interface 1808, which is connected to a bus interface (PCI) 1810 of the computing server 210. the control logic 1802 is one or more programmable processors that run compiled-code
5 firmware. The DMA interface (i.e. DMA unit) 1808 is directed by the on-board control logic 1802 to read and write data between the local NIC memory 1804 and the host's memory. The medium access unit 1806 interacts with the control logic 1802 to receive frames into local buffer storage and to send frames from local buffer storage out onto a network 1812 (e.g. full-duplex ethernet link). The memory 1804 is used
10 for temporary storage of frames, buffer descriptors, and other control data. The media access control unit 1806 is connected to the network 1812 (e.g. telecommunication network, telecommunication voice network, telecommunication text network) via an internal or external modem, optionally via infrared (IrDA), Bluetooth, a USB cable and/or a serial cable. Moreover, the computing server 210
15 optionally communicates with the external electronic devices 216, 218 via external service providers, such as Nokia PC Suite and a SMS Sender of Microsoft, which enables Windows users to send SMS messages via a GSM mobile phone from the computing server 210.

20 [0098] In terms of geographical locations of the computing server 210 and external electronic devices 216, 218, the network 1812 includes Remote Data Entry Stations (RJES); Local Area Network (LAN); Wide Area Network (WAN); Metropolitan Area Network (MAN); Distributed Data Processing Network (DDPN); and Gateways. In terms of communication technologies and media used, the network 1812 includes
25 Public Switched Data Network (PSDN); Public Switched Telephone Network

(PSTN); and Integrated Service Data Network (ISDN). In addition, the network 212 may be provided by common carriers, specialized common carriers or value added carriers.

- 5 [0099] Since digitized signals instead of electric signals are transmitted in the network 212, the digitized signals are optionally firstly converted into analogue electrical signals which are then transmitted via conventional voice telecommunication links. In this case, a MOdulator–DEModulator (MODEM) is used to fulfil a modulation process for converting digital signals into analogue signals. A
- 10 demodulator recovers the digitized data from the analogue electrical signals. In other implementations, an Integrated Service Digital Network (ISDN) is developed for handling all telecommunications requirements (i.e. voice, data, telemetry, facsimile and video) with the external electronic devices 216, 218.
- 15 [0100] Alternatively speaking, the electronic authentication system 201 is configured to take following steps automatically. In a first step, the electronic authentication system 201 takes a step of verification and/or accreditation, which verifies whether an auditor is authentic by either possessing a valid auditing licence, or accredited (e.g. authorised or delegated) by a licenced auditor. The electronic authentication
- 20 system 201 has internet bots, AI (artificial intelligence) algorithms and/or artificial neural networks to access online databases of regulatory and/or professional bodies (also known secure database) so that its database of licensed auditors become reliable, up-to-date and complete. Suspicious activities or access to the electronic authentication system 201 are monitored, reviewed, compiled and reported to
- 25 authorised personnel. Members of the public, such as directors of SMEs can easily

identify whether the auditor is authenticated through system, whether by email or other messages from the electronic authentication system 201, if subscribed. The electronic authentication system 201 provides API (Application programming interface) to software vendors to further enhance authentication performance, such as by increasing access by more users, providing more reliability and credibility.

[0101] In the application, unless specified otherwise, the terms "comprising", "comprise", and grammatical variants thereof, intended to represent "open" or "inclusive" language such that they include recited elements but also permit inclusion of additional, non-explicitly recited elements.

[0102] As used herein, the term "about", in the context of concentrations of components of the formulations, typically means +/- 5% of the stated value, more typically +/- 4% of the stated value, more typically +/- 3% of the stated value, more typically, +/- 2% of the stated value, even more typically +/- 1% of the stated value, and even more typically +/- 0.5% of the stated value.

[0103] Throughout this disclosure, certain embodiments may be disclosed in a range format. The description in range format is merely for convenience and brevity and should not be construed as an inflexible limitation on the scope of the disclosed ranges. Accordingly, the description of a range should be considered to have specifically disclosed all the possible sub-ranges as well as individual numerical values within that range. For example, description of a range such as from 1 to 6 should be considered to have specifically disclosed sub-ranges such as from 1 to 3, from 1 to 4, from 1 to 5, from 2 to 4, from 2 to 6, from 3 to 6 etc., as well as individual

numbers within that range, for example, 1, 2, 3, 4, 5, and 6. This applies regardless of the breadth of the range.

[0104] It will be apparent that various other modifications and adaptations of the
5 application will be apparent to the person skilled in the art after reading the foregoing disclosure without departing from the spirit and scope of the application and it is intended that all such modifications and adaptations come within the scope of the appended claims.

Reference Numerals

	100	existing manual authentication process or existing manual confirmation process;
5	102	auditor;
	104	client;
	106	responder;
	108	confirmation request;
	110	first step;
10	112	second step;
	114	third step;
	116	fourth step;
	118	fifth step;
	120	authentication report;
15	200	electronic authentication process;
	201	electronic authentication system;
	202	auditor;
	204	client or authorizer;
	206	responder;
20	208	electronic confirmation request;
	210	computing server;
	212	communication network;
	214	first external electronic device or auditor communication device;
	216	second external electronic device or client communication device;
25	218	third external electronic device or responder communication device;

	220	first step;
	222	second step;
	224	third step;
	226	fourth step;
5	228	fifth step;
	230	sixth step;
	232	authentication report;
	600	cloud-based electronic authentication system;
	602	authentication application;
10	604	cloud application architecture;
	606	local server;
	608	first client communication device;
	610	second client communication device;
	612	cloud service architecture;
15	614	service database;
	616	service server;
	618	artificial intelligence (AI) cloud processor;
	620	interface;
	622	main memory;
20	624	processor;
	626	Random Access Memory (RAM);
	628	storage;
	630	input device;
	632	output device;
25	634	main memory;

	636	processor;
	638	Random Access Memory (RAM);
	640	storage;
	642	handheld device;
5	644	printing device;
	646	workstation;
	648	personal computer;
	650	peripheral device;
	652	processing unit;
10	654	memory unit;
	656	artificial intelligent (AI) algorithm;
	658	database;
	700	artificial intelligent (AI) platform;
	710	traffic manager;
15	720	users;
	730	application;
	732	mobile application;
	734	web application;
	740	services;
20	742	natural language processing service;
	744	index search service;
	746	SQL database;
	750	cloud computer service;
	1700	authentication procedure;
25	1702	data processing platform;

	1704	logical modules;
	1706	database;
	1710	OMM App;
	1712	Overall Materiality Module Database;
5	1714	Cognition AI;
	1716	define audit strategy (AS);
	1718	understanding business environment (BE);
	1720	internal control (IC);
	1722	management meeting (MM);
10	1724	preliminary analytical review (AR);
	1726	risk consideration (RC);
	1728	assertion risk assessment (AS);
	1730	financial statement assessment (FS);
	1732	performance materiality (PM);
15	1734	audit program (AP);
	1800	communication unit
	1802	Control logic
	1804	memory
	1806	media Access unit
20	1808	DMA interface

	event number 1	start (ST);
	event number 2	overall materiality (OM);
	event number 3	business environment (BE);
25	event number 4	internal control (IC);

	event number 5	management meeting (MM).
	event number 6	preliminary analytical review (AR);
	event number 7	risk consideration (RC);
	event number 8	audit strategy (AS);
5	event number 9	financial statement assessment (FS);
	event number 10	risk response summary (RR);
	event number 12	risk response implementation (RRI);