SYSTEM AND METHOD FOR COMPLAINT AND REPUTATION MANAGEMENT IN A MULTI-PARTY DATA MARKETPLACE

CROSS-REFERENCE TO RELATED APPLICATIONS AND PRIORITY

[0001] This application is a Singapore National Stage Filing of International Application No. PCT/IB2017/051005, filed on February 22, 2017, which application claims priority from Indian Provisional Patent Application No. 201621006133, filed on February 22nd, 2016, the entirety of which is hereby incorporated by reference.

TECHNICAL FIELD

[0002] The present application generally relates to complaint and reputation management in an online transaction. More particularly, but not specifically, the invention is related to method and system for providing complaint and reputation management in a multi-party data marketplace.

BACKGROUND

[0003] A huge amount of data is available for multiple uses. A lot of business require such data for smooth operation of their business. It is not always feasible to gather or analyze such kind of data. To facilitate this condition, the concept of a data marketplace is getting very popular day by day. A data marketplace is an online platform where users may buy, sell, trade, and/or otherwise transact personal data or any other data captured from other sources with other users for agreed upon compensation and other predefined terms and condition.

[0004] In the data marketplace, multiple users are involved simultaneously. The data involved in the transaction in the marketplace could be confidential data. There are a lot of things dependent on the reputation of the users. On the similar lines as of any other online marketplace, the data marketplace has also issues related to the complaint and reputation management. The participants, buyers and sellers, can raise complaint against

any of the other participant involves in a transaction. Thus, it is very necessary to have a robust and automated complaint and reputation management system in the data marketplace.

[0005] Most of the existing solutions for managing the complaints and reputation are customer centric and cater to multiple small individual buyers and single seller (i.e. B-to-C). Complaint is normally raised for a particular service or product offered by the seller. Data marketplace is normally a B-to-B setup, where large organizations may buy or lease data for analysis and infer business related outcomes.

[0006] In addition to that, the scale on which existing systems operate are small and simple. Few proposed solutions which are available for such kind of setup are very rigid as they do not support tunable reputation and liability calculation with respect to complaint. There are few prior art which talk about data as an asset but none of them tackle the issue of aggregation of reputation or liabilities in case of mergers or acquisitions. None of them protects seller's concern in case of an abusive buyer. Most of the existing systems are either customer oriented i.e. they only capture a buyers concern or they don't consider the various stakeholder involved in a single transaction or the distributed nature of the data storage and usage. One other lacking feature is that they don't capture and consider the dynamism of the data and its impact on the complaint management and reputation calculation.

SUMMARY

[0007] The following presents a simplified summary of some embodiments of the disclosure in order to provide a basic understanding of the embodiments. This summary is not an extensive overview of the embodiments. It is not intended to identify key/critical elements of the embodiments or to delineate the scope of the embodiments. Its sole purpose is to present some embodiments in a simplified form as a prelude to the more detailed description that is presented below.

[0008] In view of the foregoing, an embodiment herein provides a system for complaint and reputation management of users in a data marketplace. The system comprises a user interface, a memory and a processor in communication with the

memory. The user interface for accessing the data marketplace by the users for a data transaction. The processor further configured to perform the steps of: calculating an initial reputation score of each of the users using a reputation calculation module if the user is a new user, else; retrieving and updating the reputation score of the user from a reputation bank; updating the reputation score of the user if there is a complaint against the user, wherein the reputation score is updated after verification as per a first set of predefined conditions; checking if there is an influencer in the data transaction; checking if there is an insider trading in the data transaction, wherein updating the reputation score of each of the users if there is at least one of influencer or insider trading in the data transaction after verification as per a second set of predefined conditions; checking if there is the user inactive in the data marketplace, wherein decaying the reputation score of the user if it is inactive in the data marketplace for more than a specified inactivity time period; gathering a set of insights from the data transaction for future transactions; and updating the final reputation score of each of the users in the reputation bank.

[0009] Another embodiment provides a processor implemented method for complaint and reputation management of users in a data marketplace. Initially, the data marketplace is accessed by the users for a data transaction using the user interface. At the next step, an initial reputation score is calculated for each of the users using a reputation calculation module if the user is a new user, else. The reputation score of the user is retrieved and updated from a reputation bank. In the next step the reputation score of the user is updated if there is a complaint against the user, wherein the reputation score is updated after verification as per a first set of predefined conditions. Then it is checked if there is an influencer in the data transaction. It is also checked if there is an insider trading in the data transaction, wherein the reputation score of each of the users is updated if there is at least one of influencer or insider trading in the data transaction after verification as per a second set of predefined conditions. In the next step it is checked if there is the user inactive in the data marketplace, wherein the reputation score of the user is decayed if it is inactive in the data marketplace for more than the specified inactivity time period. A set of insights are then gathered from the data transaction for future transactions. And finally, the final reputation score of each of the users is updated in the reputation bank.

[0010] Another embodiment provides a non-transitory computer-readable medium having embodied thereon a computer program for complaint and reputation management of users in a data marketplace. Initially, the data marketplace is accessed by the users for a data transaction using the user interface. At the next step, an initial reputation score is calculated for each of the users using a reputation calculation module if the user is a new user, else. The reputation score of the user is retrieved and updated from a reputation bank. In the next step the reputation score of the user is updated if there is a complaint against the user, wherein the reputation score is updated after verification as per a first set of predefined conditions. Then it is checked if there is an influencer in the data transaction. It is also checked if there is an insider trading in the data transaction, wherein the reputation score of each of the users is updated if there is at least one of influencer or insider trading in the data transaction after verification as per a second set of predefined conditions. In the next step it is checked if there is the user inactive in the data marketplace, wherein the reputation score of the user is decayed if it is inactive in the data marketplace for more than the specified inactivity time period. A set of insights are then gathered from the data transaction for future transactions. And finally, the final reputation score of each of the users is updated in the reputation bank.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The embodiments herein will be better understood from the following detailed description with reference to the drawings, in which:

[0012] Fig. 1 shows a block diagram of a system for providing complaint and reputation management in a multi-party data marketplace in accordance with an embodiment of the disclosure;

[0013] Fig. 2 shows a vector representation of reputation of a specific feature in accordance with an embodiment of the disclosure;

[0014] Fig. 3A, 3B, 3C shows a flow chart illustrating the steps involved in managing complaint and reputation of the party in a multi-party data marketplace in accordance with another embodiment of the disclosure;

[0015] Fig. 4A, 4B, 4C shows a flowchart illustrating the steps involved in

managing the reputation and complaint filed by the buyer in the data market place in accordance with another embodiment of the disclosure;

[0016] Fig. 5A, 5B, 5C, 5D shows a flowchart illustrating the steps involved in managing the reputation and complaint filed by the seller in the data market place in accordance with another embodiment of the disclosure; and

[0017] Fig. 6A, 6B, 6C, 6D, 6E shows a flowchart illustrating the steps involved in managing the reputation of the seller or the buyer in the data market place in accordance with another embodiment of the disclosure.

DETAILED DESCRIPTION

[0018] The embodiments herein and the various features and advantageous details thereof are explained more fully with reference to the non-limiting embodiments that are illustrated in the accompanying drawings and detailed in the following description. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein may be practiced and to further enable those of skill in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

[0019] Referring now to the drawings, and more particularly to Fig. 1, where similar reference characters denote corresponding features consistently throughout the figures, there are shown preferred embodiments and these embodiments are described in the context of the following exemplary system and/or method.

[0020] Fig. 1 illustrates a schematic block diagram of a system 100 for providing complaint and reputation management in a multi-party data marketplace according to an embodiment of the disclosure. The multi-party data marketplace can involve a plurality of users or a plurality of parties. It should be appreciated that the terms users and parties can be used replaceable in the disclosure. The plurality of parties comprises a plurality of seller parties and a plurality of buyer parties. It should be appreciated that for the sake of convenience, the plurality of buyer parties and the plurality of seller parties herein after will be referred as a set of buyers and a set of sellers respectively. The system 100 keeps track of the concerns of both the buyers and the sellers involved in a data transaction or

the distributed nature of the data storage and usage. According to an embodiment of the invention, the system 100 is managed by a central independent entity which keeps track of available data, their characteristics, their quoted worth, their availability, volume, rate of creation and consumption and various other meta-information about it. The central independent entity may also be referred as a platform provider.

[0021] According to an embodiment of the disclosure, the system 100 uses data as commodity or resource. It should be appreciated that the data can be static or dynamic. The data is perishable and whose worth might decay or improve with the time. The data can be used as a tradable entity for buying other data points, services, reputation points or resolving any disputes related to an existing complaint. In similar terms as any other commodity, the data can also have a value based on the demand, this can be measured in terms of data credit score. Thus, maintaining high quality data repository means having higher data credit score. The reputation and liability of the parties can be updated based on the complaints involving the parties, for example, consideration of peer and trust network, history of peering and transaction, automatic decay of reputation and liability in case of inactive participants. In an example, the system 100 also handles any kind collusion between external or internal entities/parties/participants.

[0022] According to an embodiment of the disclosure, the system 100 includes a database 102, a processor 104. The processor 104 further comprising a reputation calculation module 106, a loss minimization module 108, a multiparty verification and dispute resolution module 110, an influencer detection module 112, an insider trading detection module 114, an inactivity monitoring module 116, a complaint and reputation decay calculation module 118, a reputation lending module 120, a trust calculation module 122 and an active guidance module 124. It should be appreciated that the processor 104 may also include other modules for performing various functions of the data marketplace. The database 102 is configured to store all the information involved during the data transaction. The database 102 may also include a reputation bank 126 for storing reputation scores of the parties. The system 100 classify the users using the data marketplace based on various criteria.

[0023] The system 100 also includes a user interface 128 for accessing the data marketplace by the users. The user interface 128 can include a variety of software and

hardware interfaces, for example, a web interface, a graphical user interface, and the like and can facilitate multiple communications within a wide variety of networks N/W and protocol types, including wired networks, for example, LAN, cable, etc., and wireless networks, such as WLAN, cellular, or satellite. In an embodiment, the user interface device(s) can include one or more ports for connecting a number of devices to one another or to another server.

[0024] According to an embodiment of the disclosure, the reputation of the user is used as an asset to the person, while the complaints against the buyers or sellers is referred as the liability. In another example, the reputation can also be used as the asset to the organization in B-B setup. The reputation is calculated by the reputation calculation module 106. The reputation calculation module 106 calculates a reputation score of the parties. The reputation calculation module 106 calculates party's reputation score as a function of various parameters such as history, affiliation, quality, corpus size, trust, delivery time, market reach, payment time, request frequency, complaints and peer network. These parameters are constantly changing based on newly identified patterns in the market. Depending upon the party's role i.e. buyer or seller, a set of parameters can be picked from the above mentioned various parameters. This will help in incorporating meta-information about the party while calculating its reputation score. For example, for a seller, history and peer information can be used for figuring any collaboration with malicious party and hence lower reputation score. Although a higher existing reputation, and collaboration with malicious / new party may depict / convey a risk taking aggressive party in the data marketplace.

[0025] In an example, the reputation score of the parties can be calculated as follows. The combined reputation formula is provided as shown below:

Feature set for a buyer and a seller:

$A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *and* $B = \{\beta_1, \beta_2, \ldots, \beta_m\}$

Where, A *is feature set for a* ***seller*** *and* B *is feature set for* ***buyer***

Also, ζ_A & ζ_B *is the karma point earned by an entity between time* $(\tau - 1, \tau)$

Damping constant (λ)

$\lambda_{\alpha_k} = f(\alpha_k), Where, \alpha_k \in A$

$\lambda_{\beta_j} = f(\beta_j), Where, \beta_j \in \mathrm{B}$

$Also, \quad 0 < \lambda \leq 1$

Change constant (δ)

$\delta_A = \lambda_A * size(data)/\max(data)$

$\delta_B = \lambda_B * size(data)/\max(data)$

Reputation at time τ for a seller:

$R_{A_\tau} = (1 - \delta_A) * F_{\mathrm{A}_{\tau-1}} + \delta_A$

Penalty at time τ for a seller:

$R_{A_\tau} = (1 - \delta_A) * F_{\mathrm{A}_{\tau-1}}$

$Where, \boldsymbol{F_{\mathrm{A}_{\tau-1}}} = f(\mathrm{A}, \tau - 1) + \zeta_A$

Reputation at time τ for a buyer:

$R_{B_\tau} = (1 - \delta_B) * F_{B_{\tau-1}} + \delta_B$

Penalty at time τ for a buyer:

$R_{B_\tau} = (1 - \delta_B) * F_{B_{\tau-1}}$

$Where, \boldsymbol{F_{\mathrm{B}_{\tau-1}}} = f(\mathrm{B}, \tau - 1) + \zeta_B$

Total reputation of an entity at time τ:

$R_\tau = R_{\tau_S} + R_{\tau_B}$

[0026] The reputation can also be represented as an N dimensional Vector as shown below

Feature set for a buyer and a seller:

$\mathrm{A} = \{\overrightarrow{\alpha_1}, \overrightarrow{\alpha_2}, \ldots, \overrightarrow{\alpha_n}\}$ *and* $\mathrm{B} = \{\overrightarrow{\beta_1}, \overrightarrow{\beta_2}, \ldots, \overrightarrow{\beta_m}\}$

Where, A *is feature set for a* ***seller*** *and* B *is feature set for* ***buyer***

Also, ζ_A & ζ_B *is the karma point earned by an entity between time* $(\tau - 1, \tau)$

Now consider that a reputation for a specific feature can be represented as a vector itself as shown in Fig. 2,

So, this implies that

$\boldsymbol{\alpha_k} = \alpha_{k_x} + \alpha_{k_y}$ *, and*

$\boldsymbol{\beta_k} = \beta_{k_x} + \beta_{k_y}$

Damping constant (λ)

$\lambda_{\alpha_k} = f(\alpha_k), Where, \alpha_k \in A$

$\lambda_{\beta_j} = f(\beta_j), Where, \beta_j \in B$

$Also, \quad 0 < \lambda \leq 1$

Change constant (δ)

$\delta_{\alpha_k} = \lambda_{\alpha_k} * size(data)/\max(data)$

$\delta_{\beta_k} = \lambda_{\beta_k} * size(data)/\max(data)$

Reputation at time τ for feature α_k of seller:

$R_{\alpha_{k_x}}(\tau) = (1 - \delta_{\alpha_k}) * F_{\alpha_{k_x}}(\tau) + \delta_{\alpha_k}$

$Where, \boldsymbol{F}_{\alpha_{k_x}}(\tau) = f(\alpha_{k_x}, \tau - 1) + \zeta_A$

Penalty at time τ for feature α_k of seller:

$R_{\alpha_{k_y}}(\tau) = (1 - \delta_{\alpha_k}) * F_{\alpha_{k_y}}(\tau)$

$Where, \boldsymbol{F}_{\alpha_{k_y}}(\tau) = f(\alpha_{k_y}, \tau - 1) + \zeta_A$

Total reputation for feature α_k *at time* τ

$\overrightarrow{R_{\alpha_k}}(\tau) = \overrightarrow{R_{\alpha_{k_x}}}(\tau) + \overrightarrow{R_{\alpha_{k_y}}}(\tau)$

Total reputation of seller at time τ

$$\overrightarrow{\boldsymbol{R_A}} = \overrightarrow{R_{\alpha_1}} + \overrightarrow{R_{\alpha_2}} + \cdots + \overrightarrow{R_{\alpha_n}} = \sum_{i=1}^{n} \overrightarrow{R_{\alpha_i}}$$

$Or, \|\boldsymbol{R_A}\| = \|R_{\alpha_1}\| + \|R_{\alpha_2}\| + \cdots + \|R_{\alpha_n}\|$

Similarly, Total reputation of buyer at time τ

$$\overrightarrow{\boldsymbol{R_B}} = \overrightarrow{\boldsymbol{R_{\beta_1}}} + \overrightarrow{\boldsymbol{R_{\beta_2}}} + \cdots + \overrightarrow{\boldsymbol{R_{\beta_m}}} = \sum_{j=1}^{m} \overrightarrow{\boldsymbol{R_{\beta_j}}}$$

$Or, \|\boldsymbol{R_B}\| = \|R_{\beta_1}\| + \|R_{\beta_2}\| + \cdots + \|R_{\beta_m}\|$

Total reputation of an entity at time τ

$\vec{R} = \overrightarrow{R_A} + \overrightarrow{R_B}$

$Or, \|\boldsymbol{R}\| = \|R_A\| + \|R_B\|$

[0027] According to an embodiment of the disclosure, the system 100 also takes care of the scenario where the buyer is malicious/mischievous and does not use the provided content as per the signed SLA. Depending on the impacted/misused data points

the buyer's reputation score will be recalculated on predetermined intervals or relief given to the seller in case of a complaint submitted by the malicious/mischievous party.

[0028] According to an embodiment of the disclosure, the system 100 also maintains the historical records of complaints, their symptoms and their remediation. All this will be classified as per certain topic modelling technique like Latent Dirichlet Allocation (LDA) or information retrieval technique like tf-idf frequency for easy searching and querying. In case of a new complaint the system 100 will provide or suggest possible remediation techniques from its past experience. This will help in reducing false positives and fix turnaround time.

[0029] The system 100 also provides distributed complaint management and reporting. In the data marketplace, the buyer and the seller might have data repositories on virtually, logically or physically distributed nodes. In such a scenario there will be cases of single/multiple node failure while sending (for seller) or processing (for buyer). The present disclosure provides a technique for complaint resolution by capturing the information about the replica nodes in service level agreement (SLA) and associated cost/incentive models for doing that. This will help in continuous data flow to buyer and an incentive model for seller to maintain its reputation and occasional extra revenue. Apart from this the technique will only calculate the differential impact on reputation as per the number of dysfunctional nodes. For instance, a seller will have higher reputation for maintaining redundancy as buyers will have unrestricted flow of data. Again they may be penalized for any delay in delivery of the data points.

[0030] According to an embodiment of the disclosure, the system 100 also includes the loss minimization module 108 to minimize the loss or exposure of the confidential data by capturing the security and privacy controls provided by the buyer. Implementation of which could be active if it provides active monitoring or passive if captures the information in document or any other static service level agreement. The loss minimization module 108 evaluates the buyer's capability for providing a secure environment for data usage, it is particularly important if the data consists of PII (Personally Identifiable Information), PHI (Protected Health Information) or any other sensitive information. In case of a threat, whether inside or outside, the buyer should minimize the impact on the seller. A buyer should maintain this capability as high as they

can because this will establish their readiness for any contingency and as well as capability for handling volatile and toxic data. The loss minimization module 108 evaluates the buyer's capability for providing a secure environment for data usage. The loss minimization module 108 is used to assess the disclosed measures and controls deployed by the buyer.

[0031] According to an embodiment of the disclosure, the system 100 includes the multiparty verification and dispute resolution module 110. The multiparty verification and dispute resolution module 110 provides secure multi-party verification of disputed data by exposing the data to the larger data marketplace community, wherein independent parties may assess its quality and notify the platform provider about the result and completes the secure multi-party verification process. The independent and anonymous evaluators will get karma points for their help. The karma points could be in the form of some virtual or actual currency or data exchange or compute cycles or other fungible good or commodity. In the case of multi-party computation which is a subfield of cryptography, the plurality of parties jointly compute a function over their inputs while keeping those inputs private. Whereas in multi-party verification the plurality of parties apply their proprietary algorithm /solution / tool on a common data while keeping the algorithm/solution/tool private. This feature helps in two scenarios. 1) Dispute resolution – In case a dispute between the seller and the buyer, this allows independent parties to evaluate the quality of the data sold by the seller to the complainer and share their result with the platform provider. 2) Sandbox environment – Could be used by the prospective buyers to sample some representative data before buying it from the seller. This feature will ensure higher reputation for the seller.

[0032] In the secure multiparty verification process the disputing parties go to the platform provider with their concern/issue which then may decide to involve other parties to verify the sanity, quality, quantity and other features of the disputed dataset. In one of the instance, the platform may disclose a part or complete dataset in a time bound arena without disclosing the identity of the disputing parties. Other independent and unrelated participants may choose to assess the disputed points and may run their proprietary algorithms on the sample dataset and provide their feedback to the platform. This feedback can then be used for resolving the dispute between the parties. The participating

parties here doesn't know anything about the disputing parties or other participating verifiers and also they don't have to disclose their verification algorithm. On settlement of the dispute some karma points will be distributed to the participating parties based on the quality of the feedback. The quality will be assessed on the basis of quality matrices defined by the platform or mutually agreed upon by the disputing parties.

[0033] According to an embodiment of the disclosure, the system 100 also takes care of the impact of dynamic data on complaint filing. The system 100 also helps in reducing the number of false complaints due to the buyer's own faulty logic/algorithm/processing. When working with static data the buyer may need to do multiple iterations to ensure whether the problem is with the shared content. In a given setup where data is streamed to the buyer there might be a scenario where the buyer may face an issue with the data. Now, the buyer has to decide between report fast vs report safe i.e. report as soon as the problem is faced or do some kind of exception handling and process more data and if the problem persists then report. This is particularly useful in streaming data delivery as it might result in false complaint filing and disrupting processing of real-time/streaming content. If the problem is on the buyer's side then it will impact their reputation score. Whereas if they play safe and try to provide a cushion for exceptional scenarios then they might risk on loosing critical data points and also have to provide additional infrastructure or code or logic to handle exceptional scenarios. The buyer maintaining this kind resilience in their infrastructure will have higher reputation point. In addition to that, the data processing window is short and their might not be persisted. Therefore, if a buyer includes extra code or deploy additional storage pool to accommodate and reanalyze any issue then they should be given additional reputation as they don't put additional load on the system and over populate a platform's complaint queue.

[0034] According to an embodiment of the disclosure, the system 100 is configured to be used when there are more than two parties are involved in the single transaction and one of the party is malicious party. In this case, the system 100 assigns a group reputation score in addition to the individual reputation scores of the parties. In case of the malicious party, then the group's reputation score will go down. Apart from this, other participants will also see some reduction in their scores based on history of

previous cooperation with the malicious parties, their current peer network and their own standing in the market. This will ensure that slowly but steadily all malicious parties will be signaled and sidelined.

[0035] According to an embodiment of the disclosure the system 100 further includes an influencer detection module 112 in a multi-party transaction. The influencer detection module 112 is configured to be used when one of the party is trying to influence the data transaction. In addition to that, the influencer detection module 112 also configured to detect if one of the party is trying to ruin the reputation of the other parties or their own collaborators. To avoid such allegation and scenarios, the influencer detection module 112 uses the previous history and rating trends of entities and their nearest neighbors in the peer network. If an influencing party is found then appropriate actions are taken, for example, applying penalties on influencers or damping their given rating. The influencer detection module 112 breaks such networks so that overall neutrality of the system remains unquestionable. The system 100 also configured to detect the fake data transactions.

[0036] According to an embodiment of the disclosure, the insider trading detection module 114 is configured to detect any kind of collusion between related parties, wherein they are related and buy from and sell data to each other. This way they will keep boasting each other's reputation and other vital statistics. According to another embodiment of the disclosure, the complaint and reputation decay calculation module 118 will remove any inactive complaint from the queue. This is important because it removes dead complaints from the queue and also helps in maintaining healthy reputation management.

[0037] According to another embodiment of the disclosure, the reputation lending module 120 acts like a virtual bank for reputation wherein a participant with higher or sufficient reputation point might want to help a new entrant in exchange of some prescribed benefits. According to another embodiment of the disclosure, the active guidance module 124 keeps track of old issues and their remediation. It tags and index all historical items and may suggest as a solution to a complainer in case of similar or near matching tags or queries or keywords.

[0038] The system 100 also configured to check the activeness of the parties.

According to an embodiment of the disclosure, the inactivity monitoring module 116 is configured to identify and remove inactive participants from the marketplace if any participant or user is inactive for more than a specified inactivity time period. In a multiparty data marketplace there could be two scenarios. In the first scenario, the seller becomes inactive – In such case her reputation decays with time. This is done as the seller might not have the latest trends and data points. Although, in some exceptional cases the worth of historical data might increase. In the second scenario, the buyer becomes inactive – In such case any complaints which are pending and needs buyer's attention will decay with time. This is done to avoid any unjustified penalizing of the seller or vice versa. This feature helps in keeping inactive entities/parties outside the mainstream, and hence, crowding of the data marketplace.

[0039] According to another embodiment of the disclosure, the system 100 includes the reputation bank 126. Whenever a new party joins the marketplace, it start with a default reputation score, though, every so often, to sell a particular item the new party may require higher reputation score. Earning the minimal required amount of reputation will require some time, and hence may result in loss due to competition. The reputation bank basically operates like a normal bank but deals in reputation points. The operation of the reputation bank can be explained with the following example. The reputation bank participant with higher reputation and trust score depositing a part of their scores in the bank, provided and managed by the platform provider. The reputation bank will lend the required/requested reputation to the new entrant, though the reputation bank will require some kind of collateral. In case of successful sale the reputation bank will charge some percent of the profit and release the collateral. In addition to that, the reputation bank will keep a part of the earning and shares the remaining amount with the depositors in accordance with their % deposit. It should be appreciated that the reputation bank may also provide various other technique.

[0040] According to another embodiment of the disclosure, the system 100 also employs a trust ranking algorithm for updating of the reputation score. Reputation is not prediction of the future, but knowledge of the past. Whereas, trust is a measure of something which is associated with future. Through the present complaint and reputation management system it is possible to get trustworthiness score of a participant party. In

similar lines the trust calculation module 122 calculates the trustworthiness of a participant by considering the factors, though not limited to these, time of delivery, quality, duration, corpus, reputation, data return filing, affiliation, collaboration network etc. To accomplish this the system 100 employs multiple algorithms, for example, a simple algorithm may use history, order frequency, delivery and payment time, reputation and trust score of the nearest neighbors in the peer network. The party connected with higher ranking peer will have higher score as compared to the party which is connected with a low ranking party. In other words, the system promotes good behavior, better data quality and value added services because only then higher ranking party's entities will connect with a lower ranking party.

[0041] According to an embodiment of the disclosure, the system 100 also provides a feature of data returns. The purpose of filing of data returns is to create or update transactional records with the data marketplace platform. This record is favorably looked upon or used by the other participating entities like reputation bank, buyers or sellers, platform etc. It also suggest that the filer is a law abiding party and is active/alive in that fiscal quarter/year. In an example, the system and method we use it as one of the feature to calculate reputation of an entity. A party with good data return history might get certain privileges like higher threshold or cushioning from self-reputation deduction by filing false complaint or might get a first predetermined karma points than normal party (relatively new entrants or misbehaved parties) by participating in multi-party secure verification. To other parties it is also an indicator of one's market reach, change in corpus size, number of transaction happened (we don't disclose with whom these transaction happened), kind and number of complaints filed by/against the party and their current status/resolution. Above use cases are for just for illustrative purposes and may include many other such use-cases.

[0042] In operation, a flowchart 200 illustrating the steps involved in managing complaint and reputation of the party in a multi-party data marketplace is shown in Fig. 3A, 3B, 3C according to an embodiment of the disclosure. Initially at step 202, the data market place is accessed by the users using the user interface 128. In other words, at least one party is entered in the data market place. In an example the entering the first party is shown at step 202A, entering the second party is shown at step 202B, and entering the N^{th}

party is shown at step 202N. At step 204, it is checked by the processor 104 for each of the party that whether the party is new or not. If party is new, then at step 206, the initial reputation score of the party is calculated using the reputation calculation module 106. The reputation score can be calculated the formula mentioned above. If the party is not new, then at step 208, the old reputation score of the party is retrieved from the reputation bank 126. In the next step at 210, the reputation score of the party is updated based on the old reputation score retrieved from the reputation bank 126.

[0043] In the next step 212, it is checked that, is there any complaint filed by the party or filed against the party. If the party is involved in any complaint, then at step 214, reputation score of the party is recalculated and updated after verification as per first set of predefined conditions. The first set of predefined conditions takes care of various criteria for verifying the validity of the complaint. It should be appreciated that after the verification, the reputation score of the party my get increased or decreased. If the party is not involved in any complaint, then at step 216, data loss is minimized in the data transaction using the loss minimization module 108. In the next step 218, if there is a dispute related to quality or usability of the data then the data set in question is verified by the multiparty secure verification and dispute resolution module 110. The multiparty secure verification allows the third party verifiers to hide their intellectual property in the form code, algorithm or similar instrument. Also, the module facilitates blind verification which stops any kind of bias for or against the disputing parties.

[0044] In the next step 220, it is checked that is there any party who is influencing the data transactions for their personal benefits. If yes, then at step 222, the reputation score of all the involved parties are updated after the verification as per a second set of predefined conditions. The second set of predefined conditions includes criteria for verifying the validity of influencer and the insider trader. It is verified that whether actually a buyer or the seller is trying the influence the data transaction. If there is no influencing then, at step 222, it is checked whether there is an insider trading the data transaction. If yes then at step 224, the reputation score of all the parties are further updated, else at step 226, it is checked that whether there is any inactive party in the data marketplace. If there is any inactive party for more than the specified inactivity time period then at step 228, the reputation score is updated once again based on a third set of

predefined conditions. It should be appreciated that the predefined set of conditions are different for the seller and are different for the buyer. In the next step 230, a set of insights are gathered from the data transaction for future transactions. And finally at step 232, the reputation score of each of the involved parties is updated with the final reputation score in the reputation bank 126.

[0045] Fig. 4A, 4B, 4C shows a flowchart 300 illustrating the steps involved in managing the reputation and complaint filed by the buyer in the data market place. It should be appreciated that the flowchart 300 should be read in conjunction with explanation of various modules and steps as explained in Fig. 1 and Fig. 3A, 3B, 3C. Initially, three aspects are checked by the processor. First, whether the number of errors has crossed a predefined threshold, second these errors are not handled by the buyer and third, active guidance is helpful or not. After that the complaint is filed by the buyer, the buyer can either wait for the seller's response or the complaint goes to the seller's queue. Once the complaint is in the seller's queue, then the seller can classify the complaint. After that, three aspects are checked by the seller, first whether more data needed, second is there any issue with product or data and third, does the seller want the third party verification. If issue is with the data, then the problem is analysed and a patch is created. If 3rd party verification is required then the content is shared for verification. If there is more data needed, then additional data is requested by the seller. If additional data is not provided by the buyer in stipulated time then complaint value is decayed over the time. If complaint value is less than a threshold then the complaint is removed from the queue and the process is stopped. At the same time, as mentioned earlier, when the buyer is waiting for the response he checks whether data is requested by the seller, if yes then the seller formulate the response and send it back to the buyer. Finally the seller checks if a satisfactory solution is provided by the buyer for his complaint. If yes, then the solution is applied and the complaint is closed by the buyer.

[0046] Fig. 5A, 5B, 5C, 5D shows a flowchart 400 illustrating the steps involved in managing the reputation and complaint filed by the seller in the data market place. It should be appreciated that the flowchart 400 should be read in conjunction with explanation of various modules and steps as explained in Fig. 1 and Fig. 3A, 3B, 3C. Initially, the issue is classified by the seller. In the next step the seller reminds the buyer.

Based on the complaint the buyer provides the solution. If solution is not satisfactory, then the seller checks four aspects. First, if there is a non-payment related issue then the seller files the complaint and inform the participating parties. Second, if there is a security then the seller files the complaint and inform the participating parties. Third, if there is a usage concern issue the seller files the complaint and inform the participating parties. Fourth, is there an insider sharing or external influencer, then warn the buyer and files complaint against all the related participating parties.

[0047] Once the complaint is filed then either the seller can wait or it goes in the buyer's queue. Once the complaint is in the buyer's queue, the buyer classifies the complaint. In the next step, the buyer requests for additional data if needed. If additional data is not provided in stipulated time then complaint value is decayed over the time. If complaint value is less than a threshold then the complaint is removed from the queue. At the same time, as mentioned earlier, when the seller is waiting for the response finally the seller checks if a satisfactory solution is provided by the buyer for his complaint. If yes, then the solution is applied and the complaint is closed by the seller.

[0048] In the next step when the request is closed, the issue and resolution is logged at the platform provider's end for future reference and active guidance. The platform provider checks if this is a recurring issue, then the buyer / seller is penalized for repeating their misconduct.

[0049] Fig. 6A, 6B, 6C, 6D, 6E shows a flowchart 500 illustrating the steps involved in managing the reputation of the seller or the buyer in the data market place. It should be appreciated that the flowchart 500 should be read in conjunction with explanation of various modules and steps as explained in Fig. 1 and Fig. 3A, 3B, 3C. Initially reputation score of the user is set as zero. In the next step, the reputation score of the user is updated, if the user has karma points. In the next step when the new transaction comes up, the affiliation, replication nodes, sandboxing, corpus repository and market reach are extracted from the SLA document. In the next step, it is checked if this is known affiliation. If yes then affiliation points are added to the reputation score. In the next step, contingency planning points are added to the reputation score if replication have nodes. In the next step, points are added to the reputation score for sampling and secure verification if sandboxing is provided for verification. Finally, wholesale seller

points are added to the reputation score if the size of corpus is more than a threshold.

[0050] In the next step, it is also checked that if this is a multi-party transaction. Based on the collaboration with the trusted parties, citizen points are added to the reputation or points deducted from the reputation score. In the next step, it is checked whether there is any collaboration with the sister parties and accordingly points are deducted from the reputation score. If this is not multi-party transaction, then it is checked whether it supports dynamic content and supports error cushioning. Based on the checking either consideration points are added to the reputation score or list of pending complaints are updated.

[0051] Going back to earlier step, if that is not the new transaction, then list of pending complaints are updated. In the next step, status of the complaint is checked. If this is not filed by self then three points are checked. First, if this is not a valid complaint then a fixed percentage of points are added to the reputation score for the party. Second, if the complaint is not pending with the party then a fixed percentage of points are deducted from the reputation score for the party. Third, if the complaint is not pending for a maximum wait time then a fixed percentage of points are deducted from the reputation score for the party. In the next step, if the complaint is filed by the self then it is checked whether it is pending with self then two aspects are checked. First, If pending with self then complaint is decayed if it pending for more than a maximum wait time. Second, complaint score is less than a threshold, then the complaint is marked dead and the complaint is removed from the queue and a fixed percent of score is deducted from the party's reputation score. In the next step, if the complaint is not pending with the self then it is checked whether this is a false complaint. The false complaint counter is updated by one and complaint is marked dead once it crosses the threshold of maximum false count.

[0052] The written description describes the subject matter herein to enable any person skilled in the art to make and use the embodiments. The scope of the subject matter embodiments is defined by the claims and may include other modifications that occur to those skilled in the art. Such other modifications are intended to be within the scope of the claims if they have similar elements that do not differ from the literal language of the claims or if they include equivalent elements with insubstantial

differences from the literal language of the claims. The embodiment, thus provides the system and method for securely executing a transaction request using a communication channel.

[0053] It is, however to be understood that the scope of the protection is extended to such a program and in addition to a computer-readable means having a message therein; such computer-readable storage means contain program-code means for implementation of one or more steps of the method, when the program runs on a server or mobile device or any suitable programmable device. The hardware device can be any kind of device which can be programmed including e.g. any kind of computer like a server or a personal computer, or the like, or any combination thereof. The device may also include means which could be e.g. hardware means like e.g. an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA), or a combination of hardware and software means, e.g. an ASIC and an FPGA, or at least one microprocessor and at least one memory with software modules located therein. Thus, the means can include both hardware means and software means. The method embodiments described herein could be implemented in hardware and software. The device may also include software means. Alternatively, the embodiments may be implemented on different hardware devices, e.g. using a plurality of CPUs.

[0054] The embodiments herein can comprise hardware and software elements. The embodiments that are implemented in software include but are not limited to, firmware, resident software, microcode, etc. The functions performed by various modules described herein may be implemented in other modules or combinations of other modules. For the purposes of this description, a computer-usable or computer readable medium can be any apparatus that can comprise, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

[0055] The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current

examples of optical disks include compact disk-read only memory (CD-ROM), compact disk-read/write (CD-R/W) and DVD.

[0056] A data processing system suitable for storing and/or executing program code will include at least one processor coupled directly or indirectly to memory elements through a system bus. The memory elements can include local memory employed during actual execution of the program code, bulk storage, and cache memories which provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution.

[0057] Input/output (I/O) devices (including but not limited to keyboards, displays, pointing devices, etc.) can be coupled to the system either directly or through intervening I/O controllers. Network adapters may also be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices through intervening private or public networks. Modems, cable modem and Ethernet cards are just a few of the currently available types of network adapters.

[0058] A representative hardware environment for practicing the embodiments may include a hardware configuration of an information handling/computer system in accordance with the embodiments herein. The system herein comprises at least one processor or central processing unit (CPU). The CPUs are interconnected via system bus to various devices such as a random access memory (RAM), read-only memory (ROM), and an input/output (I/O) adapter. The I/O adapter can connect to peripheral devices, such as disk units and tape drives, or other program storage devices that are readable by the system. The system can read the inventive instructions on the program storage devices and follow these instructions to execute the methodology of the embodiments herein.

[0059] The system further includes a user interface adapter that connects a keyboard, mouse, speaker, microphone, and/or other user interface devices such as a touch screen device (not shown) to the bus to gather user input. Additionally, a communication adapter connects the bus to a data processing network, and a display adapter connects the bus to a display device which may be embodied as an output device such as a monitor, printer, or transmitter, for example. The preceding description has been presented with reference to various embodiments. Persons having ordinary skill in

the art and technology to which this application pertains will appreciate that alterations and changes in the described structures and methods of operation can be practiced without meaningfully departing from the principle, spirit and scope.

CLAIMS:

1. A method for complaint and reputation management of users in a data marketplace, the method comprising a processor implemented steps of:

accessing the data marketplace by the users for a data transaction;

calculating an initial reputation score of each of the users using a reputation calculation module if the user is a new user, else;

retrieving and updating the reputation score of the user from a reputation bank;

updating the reputation score of the user if there is a complaint against the user, wherein the reputation score is updated after verification as per a first set of predefined conditions;

checking if there is an influencer in the data transaction;

checking if there is an insider trading in the data transaction, wherein updating the reputation score of each of the users if there is at least one of influencer or insider trading in the data transaction after verification as per a second set of predefined conditions;

checking if there is the user inactive in the data marketplace, wherein decaying the reputation score of the user if the user is inactive in the data marketplace for more than a specified inactivity time period;

gathering a set of insights from the data transaction for future transactions; and

updating the final reputation score of each of the users in the reputation bank.

2. The method of claim 1 further comprising decaying the reputation of the user in case the user is unresponsive to the complaint against the user and removing the related complaint from the data marketplace.

3. The method of claim 1, wherein the user is a set of buyers or a set of sellers in the data transaction.

4. The method of claim 1, further comprising a loss minimization module for evaluating the user's capability for providing a secure environment for data usage if the user is a buyer of the data.

5. The method of claim 1, wherein the first set of predefined conditions includes criteria for verifying the validity of the complaint.

6. The method of claim 1, wherein the second set of predefined conditions includes criteria for verifying the validity of influencer and the insider trader.

7. The method of claim 1 further comprising a trust ranking algorithm for updating the reputation score of the user, wherein the trust ranking algorithm generates a trust score based on a trustworthiness of the user.

8. The method of claim 1, wherein the data used in the data transaction has a data credit score based on the demand of the data.

9. The method of claim 1 further comprises the step of dispute resolution between the set of buyers and the set of sellers through a set of independent parties in a secure way

10. The method of claim 1, wherein the data marketplace is a multiparty data marketplace.

11. The method of claim 1, wherein the reputation score is calculated based on at least one or more of history of the user, affiliation, quality, corpus size, trust, delivery time, market reach, payment time, request frequency, peer network of the user.

12. A system for complaint and reputation management of users in a data marketplace, the system comprises:

a user interface for accessing the data marketplace by the users for a data transaction;
a memory; and

a processor in communication with the memory, the processor further configured to perform the steps of:

calculating an initial reputation score of each of the users using a reputation calculation module if the user is a new user, else;

retrieving and updating the reputation score of the user from a reputation bank;

updating the reputation score of the user if there is a complaint against the user, wherein the reputation score is updated after verification as per a first set of predefined conditions;

checking if there is an influencer in the data transaction;

checking if there is an insider trading in the data transaction, wherein updating the reputation score of each of the users if there is at least one of influencer or insider trading in the data transaction after verification as per a second set of predefined conditions;

checking if there is the user inactive in the data marketplace, wherein decaying the reputation score of the user if the user is inactive in the data marketplace for more than a specified inactivity time period;

gathering a set of insights from the data transaction for future transactions; and

updating the final reputation score of each of the users in the reputation bank.

13. A non-transitory computer-readable medium having embodied thereon a computer program for complaint and reputation management of users in a data marketplace, the method comprising a processor implemented steps of:

accessing the data marketplace by the users for a data transaction;

calculating an initial reputation score of each of the users using a reputation calculation module if the user is a new user, else;

retrieving and updating the reputation score of the user from a reputation bank;

updating the reputation score of the user if there is a complaint against the user, wherein the reputation score is updated after verification as per a first set of predefined conditions;

checking if there is an influencer in the data transaction;

checking if there is an insider trading in the data transaction, wherein updating the reputation score of each of the users if there is at least one of influencer or insider trading in the data transaction after verification as per a second set of predefined conditions;

checking if there is the user inactive in the data marketplace, wherein decaying the reputation score of the user if the user is inactive in the data marketplace for more than a specified inactivity time period;

gathering a set of insights from the data transaction for future transactions; and

updating the final reputation score of each of the users in the reputation bank.