

(51) International Patent Classification:
H04L 9/32 (2006.01)(21) International Application Number:
PCT/MY2015/050098(22) International Filing Date:
4 September 2015 (04.09.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI2014702836 26 September 2014 (26.09.2014) MY(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology
Park Malaysia, Kuala Lumpur, 57000 (MY).(72) Inventors: **ABU BAKAR, Khairul Azmi**; C/o Mimos
Berhad, Technology Park Malaysia, Kuala Lumpur, 57000
(MY). **NG, Kang Siong**; C/o Mimos Berhad, Technology
Park Malaysia, Kuala Lumpur, 57000 (MY). **ALWYN,
Goh**; C/o Mimos Berhad, Technology Park Malaysia, Ku-
ala Lumpur, 57000 (MY). **BONG, Chin Wei**; C/o Mimos
Berhad, Technology Park Malaysia, Kuala Lumpur, 57000
(MY). **DEREK WILLIAM, Holtby**; C/o Mimos Berhad,
Technology Park, Kuala Lumpur, 57000 (MY).(74) Agent: **H A RASHID, Ahmad Fadzlee**; Ipvolusi Sdn Bhd,
A-3-3A, Centrio Pantai Hillpark, No. 1, Jalan Pantai
Murni, Kuala Lumpur, 59200 (MY).(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

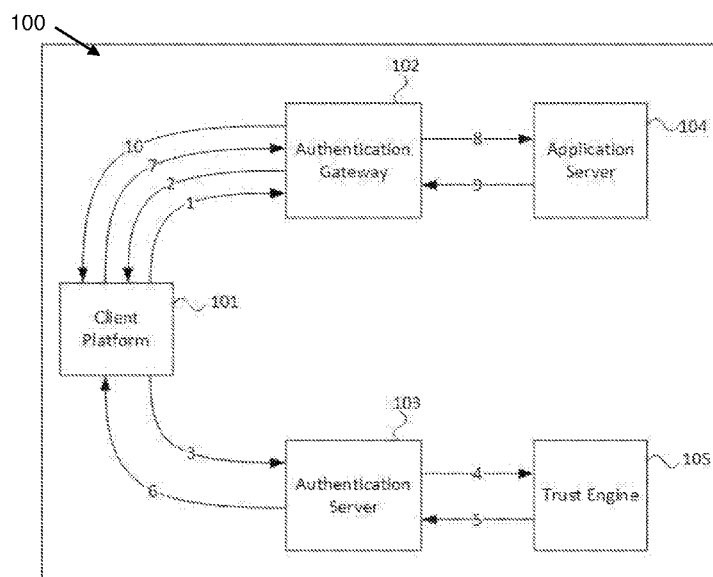
(54) Title: A SYSTEM AND METHOD FOR AUTHENTICATING A USER BASED ON USER BEHAVIOUR AND ENVIRON-
MENTAL FACTORS

FIG. 1

(57) Abstract: The present invention relates to a system and method for authenticating a user based on user behaviour and environmental factors. The system (100) allows the user to access to an application server by evaluating the trust value of environmental and user behaviour factors. The system (100) comprises a Client Platform (101), an Authentication Gateway (102), an Authentication Server (103), an Application Server (104), and a Trust Engine (105).

**Declarations under Rule 4.17:**

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *of inventorship (Rule 4.17(iv))*

Published:

- *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

**A SYSTEM AND METHOD FOR AUTHENTICATING A USER BASED ON USER
BEHAVIOUR AND ENVIRONMENTAL FACTORS**

FIELD OF INVENTION

5 The present invention relates to a system and method for authenticating a user based on user behaviour and environmental factors.

BACKGROUND OF THE INVENTION

10 System security is essential in preventing untrusted user to access the information or data. The information needs to be protected from unauthorized or unintended access. Logging in using specific username and password or token is among the techniques used to grant access to a user. However, these techniques have their own weaknesses that make the information vulnerable to being accessed by unauthorized users. Thus, this may lead to fraud and information
15 leakage to unintended persons.

 In regards to this, European Patent Publication No. EP 1205058 A2, discloses a security architecture in which a single sign-on (SSO) is provided. Session credentials are used to maintain continuity of a persistent session across
20 multiple accesses to one or more information resources, and in some embodiments, across credential level changes. Session credentials are secured, e.g., as a cryptographically secured session token, such that they may be inspected by a wide variety of entities or applications to verify an authenticated trust level, yet may not be prepared or altered except by a trusted authentication
25 service. The system of the prior art associates trust level requirements with information resources. Authentication schemes (e.g., those based on passwords, certificates, biometric techniques, smart cards, etc.) are associated with trust levels, and in some embodiments, with environmental parameters. For example, in one configuration, a login service obtains login credentials for an entity
30 commensurate with the trust level requirement(s) of an information resource or information resources to be accessed and with environment parameters that affect the sufficiency of a given credential type. Once login credentials have been obtained for an entity and have been authenticated to a given trust level, session credentials are issued and access is granted to information resources for which the
35 trust level is sufficient. By using the session credentials, access is granted without

the need for further login credentials and authentication. In some configurations, session credentials evidencing an insufficient trust level may be remedied by a session continuity preserving upgrade of login credential.

5 However, the prior art authenticates the user based on the user behaviour only. It is risky and unsafe if the credentials fall to the wrong hands. Moreover, the
aforesaid prior art enables SSO for access to multiple applications subject to prior
specification of trust parameters, and authentication and environmental information
10 obtained within session of interest. The prior art does not address authentication
and environmental information prior to session of interest. The prior art is also
embodied in system incorporating tight-coupling of authentication and authorization
sub-systems, latter of which is necessarily application-specific, and therefore
restrictive. Hence, the prior art may not be suitable in system incorporating loose-
coupling of authentication and authorization systems, as would be the case for
15 contemporary Web-based client-server application systems.

SUMMARY OF INVENTION

In one aspect of the present invention, a system for authenticating a user
based on user behaviour and environmental factors is provided. The system (100)
20 allows the user to access to an application server by evaluating the trust value of
environmental and user behaviour factors. The system (100) comprises a Client
Platform (101), at least one Authentication Gateway (102) having at least one
Application Server (104) accessible by the Client Platform (101) based on a trust
value, Authentication Server (103), and a Trust Engine (105). The Trust Engine (105)
25 is characterised in that the Trust Engine (105) is configured to compute
trustworthiness of the user based on user behaviour and environmental factors in
relation to a selected trust model. Moreover, the Trust Engine (105) includes an
Adaptive Behavioural Analytics Module (106) to analyse user behaviour factors and
environmental factors of the user, a User Behaviour and Environmental Factors
30 Update Module (107) to track user behaviour factors and the environmental factors, a
Trust Policy Module (110) to provide policies and rules associated with a trust model,
and a Trust Model Module (111) to provide selection of multiple trust models, wherein
each of the trust model stores the rules and policy for user behaviour and
environmental factors to compute the overall trust value.

Preferably, at least one Authentication Gateway (102) is configured to undertake specification of trust threshold, wherein the specification is dependent on each group of Application Server (104).

5 Preferably, the User Behaviour and Environmental Factors Update Module (107) includes a Positive Factor Repository (108) for storing history of positive group factor for user behaviour and environmental factors; and a Negative Factor Repository (109) for storing history of negative group factor for user behaviour and environmental factors.

10

In another aspect of the present invention, a method for authenticating a user based on user behaviour and environmental factors is provided. The method is characterised by the steps of submitting user credential from a Client Platform (101) to an Authentication Server (103); checking and verifying the user credentials by the Authentication Server (103); evaluating a trust value by performing an adaptive analysis based on present and past user behaviour and environmental factors by the Trust Engine (105); allowing access to an Application Servers (104) if the trust value is above a trust threshold; and denying access to the Application Servers (104) and submitting additional user credential by the Client Platform (101) if the trust value is below a trust threshold.

20

Preferably, the step of evaluating a trust value by performing an adaptive analysis based on present and past user behaviour and environmental factors includes selecting a trust model from a set of trust models in the Trust Model Module (111); evaluating current and history of positive behaviour and environmental factors to compute the trust value; evaluating current and history of negative behaviour and environmental factors to compute a penalty; penalizing negative user and environment factors by increasing or decreasing the computed trust value; transforming the trust value into a trust surface; estimating the trust threshold from the trust surface, wherein the trust threshold is within a range of a maximum and minimum values of the trust surface; comparing the computed trust value to the trust threshold; authenticating access for user if the trust value above the trust threshold; determining if user has reached the termination condition; depending on the policy on the termination condition in the selected trust model, activating FAIL_SAFE to grant authentication or activating FAIL_SECURE to deny authentication.

35

Preferably, the steps of evaluating positive user behaviour and environmental factors includes tracking the positive user behaviour and environmental factors; extracting the current positive user behaviour and environment atomic factor; retrieving positive history user behaviour and environmental factor from Positive Factor Repository **(108)**; obtaining rules and policies from the Trust Policy Module **(110)**; and computing the trust value based on the rules and policies.

Preferably, the step of evaluating negative user behaviour and environmental factors includes tracking the negative user behaviour and environmental factors; extracting the current negative user behaviour and environment atomic factor, identifying number of attempts to access the application; retrieving negative history user behaviour and environment factor from the Negative Factor Repository **(109)**; obtaining rules and policies from the Trust Policy Module **(110)**; and computing trust value based on the rules and policies

Preferably, the step of penalizing user and environment factors includes tracking and recording the negative user behaviour and environment factors; calculating the number of unsuccessful defining the rejection factors in order to generate penalty list; identifying suspicious user behaviour and environment factors with the computed penalty; incurring the penalty to the trust level to reduce trustworthiness; and alerting the administrator of the system about the incident.

Preferably, the step of transforming the trust value into a trust surface includes extracting each user behaviour factor and environmental factor; assigning a relative weightage based on authentication outcome for each user behaviour and environmental factor; aggregating the weighted user behaviour factors; aggregating the weighted environmental factors; and transforming weighted aggregated user behaviour and environmental factors into the trust surface encompassing anticipated range of user behaviour and environment, wherein a maximum value of the trust surface is an asymptotic maximum that corresponds to high preponderance of positive user behaviour and environmental factors, and a maximum value of the trust surface is an asymptotic minimum of the trust surface that corresponds to high preponderance of negative user behaviour and environmental factors.

Preferably, the step of aggregating the weighted user behaviour factors includes correlating of current positive authentication outcome with previous positive authentication outcomes as positive contribution to present trust contribution; correlating of current negative authentication outcome with previous negative authentication outcomes as negative contribution to present trust contribution; converging the positive and negative contributions; correlating of multiple authentication credentials, as accumulation over multiple interactions within application of interest, resulting in positive or negative contribution to trust computation; and converging the contributions from the correlations of multiple authentication credentials.

Preferably, the step of aggregating the weighted environmental factors includes correlating of current positive environmental factor with previous positive environmental factors as positive contribution to present trust contribution; correlating of current negative environmental factor with previous negative environmental factors as negative contribution to present trust contribution; converging the positive and negative contributions; correlation of multiple environment factors as positive or negative contribution to trust computation; and converging the contributions from correlations of multiple environment factors.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention.

FIG. 1 illustrates a block diagram of a system for authenticating user based on user behaviour and environmental factors (**100**) according to an embodiment of the present invention.

FIG. 2 illustrates a block diagram of a Trust Engine (**105**) of the system (**100**) of **FIG.1**.

FIG. 3 illustrates a flowchart of a method for authenticating user based on user behaviour and environmental factors (**100**) according to an embodiment of the present invention.

FIG. 4 illustrates a flowchart of a sub-method for evaluating a trust value by performing adaptive analysis of the method of **FIG. 3**.

5 **FIGS. 5(a-b)** illustrate flowcharts of sub steps for executing user behaviour and environmental factors update of the sub-method in **FIG. 4**.

FIG. 6 illustrates a flowchart of sub steps for penalizing negative user and environmental factors of the sub-method of **FIG. 4**.

10

FIG. 7 illustrates a flow diagram for transforming the trust value into a trust surface of the sub-method of **FIG.4**.

15 **FIG. 8** illustrates an exemplary of a trust surface of environmental factors and user behaviour factors using hyperbolic tangent.

DESCRIPTION OF THE PREFFERED EMBODIMENT

A preferred embodiment of the present invention will be described herein below with reference to the accompanying drawings. In the following description, well known functions or constructions are not described in detail since they would obscure the description with unnecessary detail.

25 **FIG. 1** illustrates a block diagram of a system for authenticating user based on user behaviour and environmental factors (**100**) according to an embodiment of the present invention. The system (**100**) allows the user to access to an application server by evaluating the trust value of environmental and user behaviour factors. The environmental factors include time of logging in, user's geographical location and type of browser used while the user behaviour factors are the user credentials used by the user which include username and password, OTP (one-time password) token, SMS and certificates. The system (**100**) comprises a Client Platform (**101**), an Authentication Gateway (**102**), an Authentication Server (**103**), an Application Server (**104**), and a Trust Engine (**105**).

35 The Client Platform (**101**) is connected to the Authentication Gateway (**102**) and the Authentication Server (**103**) via network. The Client Platform (**101**) is a user

interface or a browser operated by the user to attempt access to the Application Server (104). The Client Platform (101) provides the user behavioural factor to be verified by the Authentication Server (103). The Client Platform (101) also provides the environmental factors to be evaluated by the Trust Engine (105) via the
5 Authentication Server (103).

The Authentication Gateway (102) is connected to the Client Platform (101) and the Application Server (104) via network. The Authentication Gateway (102) redirects the request attempted by the user to the Authentication Server (103) via the
10 Client Platform (101). The Authentication Gateway (102) is configured with the specification of trust threshold of the Application Server (104), and allows the user to access the Application Server (104) if the trust value required is met.

The Authentication Server (103) is connected to the Client Platform (101) and
15 the Trust Engine (105) via network. The Authentication Server (103) collects and verifies the user credentials specific to application access of interest.

The Application Server (104) is connected to the Authentication Gateway (102) via network. The Application Server (104) includes an application that the user wants to
20 access and it is accessible after the trust value required by the system (100) is met. At least one Authentication Gateway (102) is configured to undertake specification of trust threshold, wherein the specification is dependent on the corresponding Application Server (104).

25 The Trust Engine (105) is connected to the Authentication Server (103) via network. The Trust Engine (105) computes the trustworthiness of the user from the user behaviour and environmental factors according to the selected trust model. It evaluates whether the trustworthiness meets or exceeds the trust value required to access the Application Server (104).

30

Referring to FIG. 2, the Trust Engine (105) comprises of an Adaptive Behavioural Analytics Module (106), a User Behaviour and Environmental Factors Update Module (107), a Trust Policy Module (110), and a Trust Model Module (111).

The Adaptive Behavioural Analytics Module **(106)** analyses the present and past user behaviour factors and also environmental factors related to the authentication of the user. The User Behaviour and Environmental Factors Update Module **(107)** tracks the user behaviour factors and the environmental factors.

5

The User Behaviour and Environmental Factors Update Module **(107)** comprises of a Positive Factor Repository **(108)** and a Negative Factor Repository **(109)**. The Positive Factor Repository **(108)** stores the history of positive group factor or successful authentication for user behaviour and environmental factors while the
10 Negative Factor Repository **(109)** stores the history of negative group factor or unsuccessful authentication for user behaviour and environmental factors.

The Trust Policy Module **(110)** provides the policies and rules that are associated with the trust models. The Trust Model Module **(111)** provides selection of
15 multiple trust models. Each of the model stores the rules and policies for user behaviour and environmental factors in order to compute the overall trust value. These policies and rules define the importance and significance level of the user behaviour and environmental factor. The authentication decision for termination condition is also defined in those policies and rules.

20

FIG. 3 illustrates a flowchart of a method for authenticating user based on user behaviour and environmental factors according to an embodiment of the present invention. The method undertakes single sign-on (SSO) by assessment of user authentication behaviour and environmental information against prior specification, at
25 Application Server **(104)**, of trust requirements. Moreover, the method undertakes assessment of trust based in both present and previous user behaviour, and additionally on both generic and user-specific environmental conditions.

Initially, a user interacts with the system **(100)** by using the Client Platform
30 **(101)**. The user enters his credentials through the Client Platform **(101)** by using a login mechanism as in step **401**. The environmental factors are also provided by the Client Platform **(101)**. The Authentication Server **(103)** then collects and verifies the credentials of the user as in step **402**.

Next, the adaptive analysis is performed by the Adaptive Behavioural Analytics Module (106) in the Trust Engine (105) as in step 403. The adaptive analysis is performed to evaluate a trust value of the user in order to grant or deny access to the Application Server (104). The Adaptive Behavioural Analytics Module (106) retrieves rules and policies from the Trust Policy Module (110) associated with the selected trust model from the Trust Model Module (111) in the Trust Engine (105) to establish a trust value for the user. Each user behaviour and environmental factor is assigned with a weightage trust value based on the retrieved rule and policy. The overall trust value is then obtained by aggregating and evaluating the present and past user behaviour and environmental factors from the Positive Factor Repository (108) and Negative Factor Repository (109) that resides in the User Behaviour and Environmental Factors Update Module (107).

The Adaptive Behavioural Analytics Module (106) then determines whether trust value computed is not less than the trust threshold as in step 404. If not, the method returns to step 401 where the Authentication Server (103) prompts the user to select another user credential, the previous user credential that had been successfully used being disabled. If the trust value computed is not less than the trust threshold, the user is allowed to access the Application Server (104). Otherwise, the user is denied to access the Application Server (104) as in step 405 and the user has to submit another different credential through the Client Platform (101). This entails capture and update of multiple user and client attributes, subsequently categorized as user or environment factors, and additionally categorized as positive or negative factors. This is undertaken by means of iterating multiple authentication strategies; for assigning each authentication factor with values or importance level that contribute to the trust required for a service provided; and further allowing the user to choose one or many authentication strategies from the list provided.

FIG. 4 illustrates a flowchart of a sub-method for evaluating the trust value by performing the adaptive analysis of the method of FIG. 3. The Trust Engine (105) selects a trust model from multiple trust models provided in the Trust Model Module (111) and the trust policy that is associated with the selected trust model from the Trust Policy Module (110) as in step 501. The trust model provides the trust value computation method, and allows selection of one or more trust computation methods, and correspondingly trust requirements for each application of interest, the net effect

of which is to estimate the impact of positive or negative elements, as might arise from user and environment factors. Trust computation is also inclusive of aggregation of current and previous history of positive and negative user and environment behaviour based on the trust model selected; penalizing negative user and environment behaviour to be used for assessment of penalty to the trust level; then transforming aggregation of positive and negative, current and previous history of the user and environment factors into a trust surface for estimation as to whether valuation on trust surface exceeds trust threshold specified by application.

Next, the aggregation and evaluation of current and history of positive user behaviour and environmental factors are done to determine the trust value as in step **502**. Assessment based on the user behaviour is done by the User Behaviour and Environmental Factors Update Module (**107**). The history of positive user behaviour is retrieved from the Positive Factor Repository (**108**). This assessment undertakes computation of positive factors inclusive of successful authentication history used to establish user behaviour or environmental profile, and correspondingly negative factors inclusive of failed authentication history or behaviour not corresponding to user behaviour or environmental profile.

Thereon, the Adaptive Behavioural Analytics Module (**106**) aggregates and evaluates the current and history records of negative user behaviour and environmental factors to determine the penalty to the computed trust as in step **503**. The history of negative user behaviour is retrieved from the Negative Factor Repository (**109**).

Next, the Adaptive Behavioural Analytics Module (**106**) penalizes negative user and environmental factors by decreasing the computed trust value as in step **504**. The trust value computed is transformed into the trust surface and the trust threshold is estimated from the trust surface as in step **505**. The trust threshold to be established on behalf of application is in need of establishment in any authentication request, as collected and computed from user behaviour and environmental data, as obtained from user and client attributes. This methodology establishes contributions of significance for all parameters for estimating the positive or negative impact of user and environment factors, both specific to particular user of interest or of generic interest encompassing all access requests independent of particular user; and

furthermore specifies the transformation method used to construct the appropriated trust surface.

5 The Adaptive Behavioural Analytics Module **(106)** determines whether the trust value is above the trust required as in decision **506**. If the trust value computed is above the trust required, the user authentication is successful. If the trust value computed is below the trust required, the user authentication fails. Adaptive analysis occurs over several iterations allowing user to choose one of more authentication methods from the list provided, wherein each authentication method or combination
10 thereof is assigned with values corresponding to importance of contribution to the trust required for application of interest.

Next, the Adaptive Behavioural Analytics Module **(106)** determines whether the user has reached the termination condition as in decision **507**. The termination
15 condition happens when all possible user behaviour and environmental factors have been successfully used but the computed trust value still does not meet the required trust value. Depending on the policy in the selected trust model, the system **(100)** could either activate either FAIL_SECURE or FAIL_SAFE. In FAIL_SECURE, user is not authenticated by the system **(100)** and access to the Application Server **(104)** is
20 denied. On the other hand, in FAIL_SAFE, user is considered authenticated even though the user of interest unable to attain the required trust threshold.

FIGS. 5(a-b) illustrate flowcharts of sub steps for executing user behaviour and environmental factors update of the sub-method in **FIG. 4**. The capture and
25 update of these multiple user and client attributes, as specified user and environmental factors, is inclusive of but not limited to time, location, particular client platform of interest, and application of interest. Based on **FIG. 5a**, the positive user behaviour factor and the positive environmental factor are tracked and recorded as in step **701** and step **702**.

30

Atomic factor extraction is executed as in step **703**. The information such as time login, browser type, geolocation and so on are extracted from the contextual data and transformed into a necessary format when a user logs in. The login attribute based on the positive factors is computed and updated in the Positive Factor
35 Repository **(108)** as in step **704**. Each of the information is stored in a repository

database in different formats. For example, the login time is stored as timestamp format, geolocation is stored as string of city region and country, and so on.

Based on **FIG. 5b**, the negative user behaviour factor and the negative environmental factor are tracked and recorded as in step **705** and step **706**.

Atomic factor extraction is executed as in step **707**, identical to step **703** for positive factor. The number of failed login attempt is calculated in step **708**. The penalty attribute is then computed based on the negative attempts by the user. The computed attribute penalty is updated in the Negative Factor Repository (**109**).

The negative factors identified are used to define rejection factors as in step **709**. The user behaviour and environmental factors from records of failed login attempt are considered in the rejection factors. The rejection factors are generated under the following two circumstances. The particular user identification is defined as a rejection factor if the user keeps presenting wrong credentials using the same user identification when trying to access application from different environmental factors. The environment factor is considered as a rejection factor if there are numbers of failed attempts for different user identities but under the same environment factor. The generated rejection factors are updated in the Negative Factor Repository (**109**).

FIG. 6 illustrates a flowchart of sub steps for penalizing the negative user and environmental factors of the sub-method of **FIG. 4**. The suspicious user and environment factor are identified as in step **801**, by conducting specific assessment to evaluate user behaviour originating from particular client, inclusive but not limited to singular client from which originates multiple application access attempts using different user identities. The number of failed attempts is identified as in step **802**, by prior stipulation of such client and user behaviour originating thereof as being suspicious. The penalty is computed for the user as in step **803**, resulting from suspicious clients and user behaviour originating thereof, such penalties inclusive of, but not limited to, preventing user access for specified periods of time. The computation of the penalty is based on number of failed attempt for a predefined period of time, such that each failed attempt contributes to the value of the penalty. The higher the number of failed attempt, the longer the period of penalty given to the

suspicious user. For example, if there are more than 10 failed attempts from the same environmental factor, any further log in attempt from that environmental factor will have its trust value reduced, such that any subsequent authentication attempt from that particular environment factor results in penalty assessed on the user. The user is identified and marked with the computed penalty as in step 804. Next, the computed penalty is incurred to the trust value to resulting in reduction of trust level of particular access attempt regarded suspicious as in step 805. In step 806, the administrator of the system (100) is alerted that the user has been given the penalty.

FIG. 7 illustrates a flow diagram for transforming the trust value into a trust surface of the sub-method of FIG.4. A plurality factors are divided into environmental factors and user behaviour. For example, location, time, browser type, target applications and so on is aggregated into an environmental factor which is then transformed into a dimension ranging from definitely low to definitely high impact towards the trust value. This aggregation of environment factors is partially obtained from client platform of interest. Similarly, each factor based on one or many selections of login mechanism is aggregated into user behaviour which is also transformed into a dimension ranging from definitely low to definitely high impact towards the trust value. This aggregation of user behaviour factors, as undertaken by user of interest, is pertinent to application access request of interest. Thus, the trust surface encompasses anticipated range of user behaviour and environment, wherein a maximum value of the trust surface is an asymptotic maximum that corresponds to high preponderance of positive user behaviour and environmental factors, and a minimum value of the trust surface is an asymptotic minimum of the trust surface that corresponds to a high preponderance of negative user behaviour and environmental factors, with trust threshold as specified by application of interest lies in range specified by aforesaid maximum and minimum valuations. The sub-method for transforming the trust value into a trust surface includes extracting each user behaviour factor and environmental factor; assigning a relative weightage based on authentication outcome for each user behaviour and environmental factor; aggregating the weighted user behaviour factors; aggregating the weighted environmental factors; and transforming weighted aggregated user behaviour and environmental factors into the trust surface. In aggregating the weighted user behaviour factors, the steps include demonstrating single authentication credential, resulting in positive or negative contribution to trust computation in event of correct or

incorrect authentication outcome; correlating of current authentication outcome, if adjudged positive, with previous positive authentication outcomes, resulting in positive contribution to present trust contribution, and likewise to profile of authentic user behaviour; correlating of current authentication outcome, if adjudged negative, with previous negative authentication outcomes, resulting in negative contribution to present trust contribution, and likewise to profile of authentic user behaviour; converging contributions from correlations of authentication outcomes at present time to outcomes progressively further back in time; correlating of multiple authentication credentials, as accumulation over multiple interactions within application of interest, resulting in positive or negative contribution to trust computation; and converging contributions from the correlations of progressively larger accumulations of authentication credentials. In aggregating the weighted environmental factors, the steps include capturing of single environment factor, resulting in positive or negative contribution to trust computation in event of correlation against environment factors deemed to be trustworthy or untrustworthy for all users of interest; correlating of current environmental factor, if adjudged positive, with previous positive environmental factors, resulting in positive contribution to present trust contribution, and likewise to profile of authentic environmental conditions specific to user; correlating of current environmental factor, if adjudged positive, with previous negative environmental factors, resulting in negative contribution to present trust contribution, , and likewise to profile of inauthentic environmental conditions specific to user; converging contributions from correlations of environment factors at present time to outcomes progressively further back in time; correlating of multiple environment factors, as positive or negative contribution to trust computation, against combinations of environment factors deemed to be trustworthy or untrustworthy for all users; and converging contributions from correlations of progressively more complex combinations of environment factors.

FIG. 8 illustrates an exemplary of a trust surface of environmental factors and user behaviour factors using hyperbolic tangent. The negative and positive of both user behaviour and environmental factors are aggregated to get the trust value. The range of the trust value is from -1 to 1. This range can be derived from the aggregation of user behaviour and environmental factors using the hyperbolic tangent function. If the aggregated user behaviour and environmental factors that have the trust value of 1, it means that the user is very trustworthy while if the

aggregated user behaviour and environmental factors that have the trust value of -1, it means that the user is very untrustworthy.

- 5 While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. Rather, the words used in the specifications are words of description rather than limitation and various changes may be made without departing from the scope of the invention.

CLAIMS

1. A system for authenticating a user based on user behaviour and environmental factors **(100)** comprises of:

- 5 a) a Client Platform **(101)**, on which the user engages in authentication behaviour, and which also provides data from which to collect or compute environmental data,
- 10 b) at least one Authentication Gateway **(102)** accessible by the Client Platform **(101)**, each instance thereof corresponding to, and protective of, at least one Application Server **(104)**, access to which is allowed upon successful attainment of trust required in accordance with prior specification thereof, and which otherwise redirects access request by user of interest to Authentication Server **(103)**,
- 15 c) an Authentication Server **(103)**, undertaking said redirections via intermediation of client platform **(101)**, for collection of user authentication credentials comprising authentication behaviour specific to application access of interest, and subsequently forwarding assessment of credentials to a Trust Engine **(105)**,
- 20 d) at least one Application Server **(104)** having at least one application accessible by the Client Platform **(101)** based on a trust value, with prior specification of trust to be established by user authentication behaviour or environmental conditions, and
- e) the Trust Engine **(105)**;

wherein the Trust Engine **(105)** is characterised in that:

- 25 a) the Trust Engine **(105)** is configured to assess trustworthiness of the user based on user authentication behaviour factors and environmental factors in relation to a selected trust model, such that trust valuation pertaining to access request of interest is assessed as to whether it meets or exceeds threshold specification for access request of interest; and
- 30 b) the Trust Engine **(105)** is inclusive of:
- i. an Adaptive Behavioural Analytics Module **(106)** to analyse user behaviour factors and environmental factors of the user,
- 35 ii. a User Behaviour and Environmental Factors Update Module **(107)** to track user behaviour factors and the environmental factors,

- iii. a Trust Policy Module **(110)** to provide policies and rules associated with a trust model, and
 - iv. a Trust Model Module **(111)** to provide selection of multiple trust models, wherein each of the trust model includes the trust value for user behaviour and environmental factors to compute the overall trust value.
- 5
2. The system **(100)**, as claimed in claim 1, wherein the at least one Authentication Gateway **(102)** is configured to undertake specification of trust threshold, wherein the specification is dependent on the corresponding Application Server **(104)**.
- 10
3. The system **(100)** as claimed in claim 1, wherein the User Behaviour and Environmental Factors Update Module **(107)** includes:
- 15
- a) a Positive Factor Repository **(108)** for storing current and history of positive group factor for user behaviour and environmental factors; and
 - b) a Negative Factor Repository **(109)** for storing current and history of negative group factor for user behaviour and environmental factors.
- 20
4. A method for authenticating a user access to applications adaptively based on user behaviour and environmental factors is characterised by the steps of:
- a) submitting user credentials from a Client Platform **(101)** to an Authentication Server **(103)**;
 - 25 b) checking and verifying the user credentials by the Authentication Server **(103)**;
 - c) evaluating a trust value by performing an adaptive analysis based on present and past user behaviour and environmental factors by a Trust Engine **(105)**;
 - 30 d) allowing access to an Application Server **(104)** if the trust value is above a trust threshold; and
 - e) denying access to the Application Servers **(104)** and submitting user credentials by the Client Platform **(101)** if the trust value is below the trust threshold.
- 35

5. The method as claimed in claim 4, wherein the method further comprises the steps of:

- 5 a) trust threshold to be established on behalf of application in need of such establishment, as collected and computed from user behaviour and environmental data, as obtained from user and client attributes;
- b) capture and update of multiple user and client attributes, subsequently categorized as user or environment factors, and additionally categorized as positive or negative factors;
- 10 c) computation of positive factors inclusive of successful authentication history used to establish user behaviour or environmental profile, and correspondingly negative factors inclusive of failed authentication history or behaviour not corresponding to user behaviour or environmental profile;
- 15 d) analysis inclusive of aggregation of current and previous history of positive and negative user and environment behaviour based on the trust model selected; penalizing negative user and environment behaviour to be used for assessment of penalty to the trust level; then transforming aggregation of positive and negative, current and previous history of the user and environment factors into a trust surface for estimation as to whether valuation on trust surface exceeds trust threshold specified by application; and
- 20 e) iteration allowing user to choose one of more authentication methods from the list provided wherein each authentication method or combination thereof is assigned with values corresponding to importance of contribution to the trust required for application of interest, further characterized by:
 - 25 i. trust model allowing selection of one or more trust computation methods, trust requirements for each application of interest, the net effect of which is to estimate the impact of positive or negative elements, as might arise from user and environment factors, and
 - 30 ii. operational framework encompassing trust model in which FAIL_SAFE or FAIL_SECURE access to applications are allowed, as particular case might be, in absence of

authentication behaviour or even additional authentication behaviour cannot be obtained.

6. The method as claimed in claim 4, wherein the step of evaluating a trust value
5 by performing an adaptive analysis based on present and past user behaviour and environmental factors includes:

- a) selecting a trust model from multiple trust models associated with the trust policy from the Trust Policy Module (110) and Trust Model Module (111);
- 10 b) establishing risk profile for each application with policy reference based on rules or constraints;
- c) establishing contributions of significance for all parameters for estimating the positive or negative impact of user and environment factors, both specific to particular user of interest or of generic interest
15 encompassing all access requests independent of particular user;
- d) specifying the transformation method used to construct the appropriated trust surface;
- e) iterating multiple authentication strategies for assigning each authentication factor with values or importance level that contribute to
20 the trust required for a service provided;
- f) allowing user to choose one or many authentication strategies from the list provided;
- g) activating one of the FAIL_SAFE or FAIL_SECURE options to apply when process reaches a termination condition;
- 25 h) aggregating and evaluating current and historical valuations of positive user behaviour and environmental factors pertinent to the trust model selected;
- i) computing a trust value based on the aggregated current and historical valuations of positive user behaviour and environmental
30 factors;
- j) aggregating and evaluating current and historical valuations of negative user behaviour and environmental factors pertinent to the trust model selected, and then penalizing negative user behaviour and environmental factors;
- 35 k) transforming the computed trust value into a trust surface;

- l) estimating the trust valuation from the trust surface, wherein the trust valuation is within a range of a maximum and minimum values of the trust surface;
- m) comparing the trust value to the trust threshold; and applicable termination condition;
- n) determining whether the user has reached a termination condition; and
- o) authenticating access for user if the trust value is not less than the trust threshold.

7. The method as claimed in claim 6, wherein the step of aggregating and evaluating current and historical valuations of positive user behaviour and environmental factors inclusive of:

- a) capture and update of multiple user and client attributes, as specified user factors;
- b) capture and update of multiple user and client attributes, as specified environment factors, inclusive of, but not limited to time, location, particular client platform of interest, and application of interest;
- c) tracking and recording of the positive factors based on previously successful authentication interactions, and also previously specified behaviour deemed as common to genuine authentication;
- d) extracting atomic factor from the user behaviour and environmental factors; and
- e) computing and updating login attribute based on the positive factors.

8. The method as claimed in claim 6, wherein the step of aggregating and evaluating current and historical valuations of negative user behaviour and environmental factors inclusive of:

- a) tracking and recording of the negative factors based on previously unsuccessful authentication interactions, and also previously specified behaviour deemed as anomalous and suggestive as fraudulent authentication;
- b) extracting atomic factor from the user behaviour and environmental factors;

- c) computing penalty attribute based on the negative attempts by the user;
 - d) defining rejection factors based on the negative user behaviour and environmental factors; and
 - 5 e) updating the rejection factors in a Negative Factor Repository (109).
9. The method as claimed in claim 6, wherein the step of penalizing negative user behaviour and environmental factors, by means of associating particular user and environment factors as adversely affecting establishment of trust, inclusive of but not limited to:
- 10
- a) identifying suspicious user and environmental factors, by conducting specific assessment to evaluate user behaviour originating from particular client, inclusive but not limited to singular client from which originates multiple application access attempts using different user identities;
 - 15 b) identifying number of failed attempts, by prior stipulation of such client and user behaviour originating thereof as being suspicious;
 - c) computing a penalty based on number of failed attempt for a predefined period of time, resulting from suspicious clients and user behaviour originating thereof, such penalties inclusive of, but not limited to, preventing user access for specified periods of time;
 - 20 d) identifying and marking the user with the computed penalty; and
 - e) incurring the computed penalty to the trust value, resulting in reduction of trust level of particular access attempt regarded suspicious.
- 25
10. The method as claimed in claim 6, wherein the step of transforming the trust value into a particular location on the trust surface inclusive of:
- a) aggregation of user behaviour factors, as undertaken by user of interest pertinent to application access request of interest;
 - 30 b) aggregation of environment factors, partially obtained from client platform of interest; and then
 - c) mapping onto trust surface encompassing anticipated range of user behaviour and environment; in which

- 5
- i. asymptotic maximum of trust valuation corresponds to high preponderance of positive user behaviour and environmental factors,
 - ii. asymptotic minimum of trust valuation corresponds to high preponderance of negative user behaviour and environmental factors, and
- trust threshold as specified by application of interest lies in range specified by aforesaid maximum and minimum valuations.

10

11. The method as claimed in claim 10, wherein the step of weighted aggregation of user behaviour factors is inclusive of:

15

- a) demonstrating of single authentication credential, resulting in positive or negative contribution to trust computation in event of correct or incorrect authentication outcome;

20

- b) correlating of current authentication outcome, if adjudged positive, with previous positive authentication outcomes, resulting in positive contribution to present trust contribution, and likewise to profile of authentic user behaviour;

25

- c) correlating of current authentication outcome, if adjudged negative, with previous negative authentication outcomes, resulting in negative contribution to present trust contribution, and likewise to profile of authentic user behaviour;

- d) converging contributions from correlations of authentication outcomes at present time to outcomes progressively further back in time;

- e) correlating of multiple authentication credentials, as accumulation over multiple interactions within application of interest, resulting in positive or negative contribution to trust computation; and

30

- f) converging contributions from the correlations of progressively larger accumulations of authentication credentials.

12. The method as claimed in claim 10, wherein weighted aggregation of environmental factors is inclusive of:

35

- a) capturing of single environment factor, resulting in positive or negative contribution to trust computation in event of correlation against

environment factors deemed to be trustworthy or untrustworthy for all users of interest;

- 5 b) correlating of current environmental factor, if adjudged positive, with previous positive environmental factors, resulting in positive contribution to present trust contribution, and likewise to profile of authentic environmental conditions specific to user;
- c) correlating of current environmental factor, if adjudged positive, with previous negative environmental factors, resulting in negative contribution to present trust contribution, , and likewise to profile of
10 inauthentic environmental conditions specific to user;
- d) converging contributions from correlations of environment factors at present time to outcomes progressively further back in time;
- e) correlating of multiple environment factors, as positive or negative contribution to trust computation, against combinations of environment
15 factors deemed to be trustworthy or untrustworthy for all users; and
- f) converging contributions from correlations of progressively more complex combinations of environment factors.

1/8

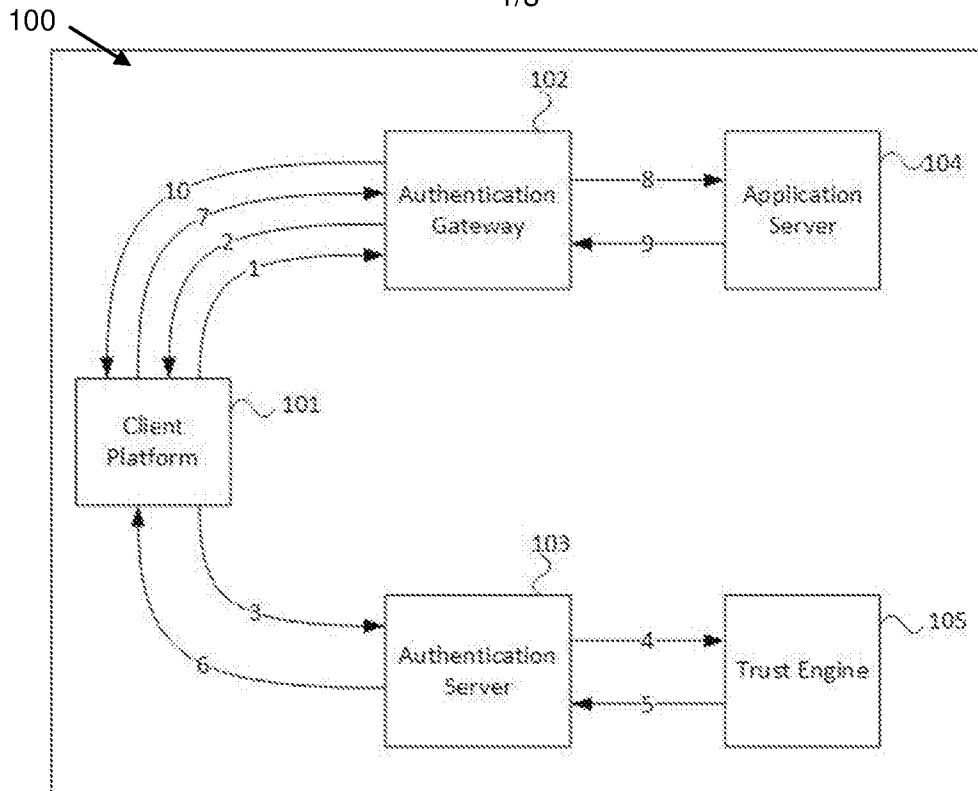


FIG. 1

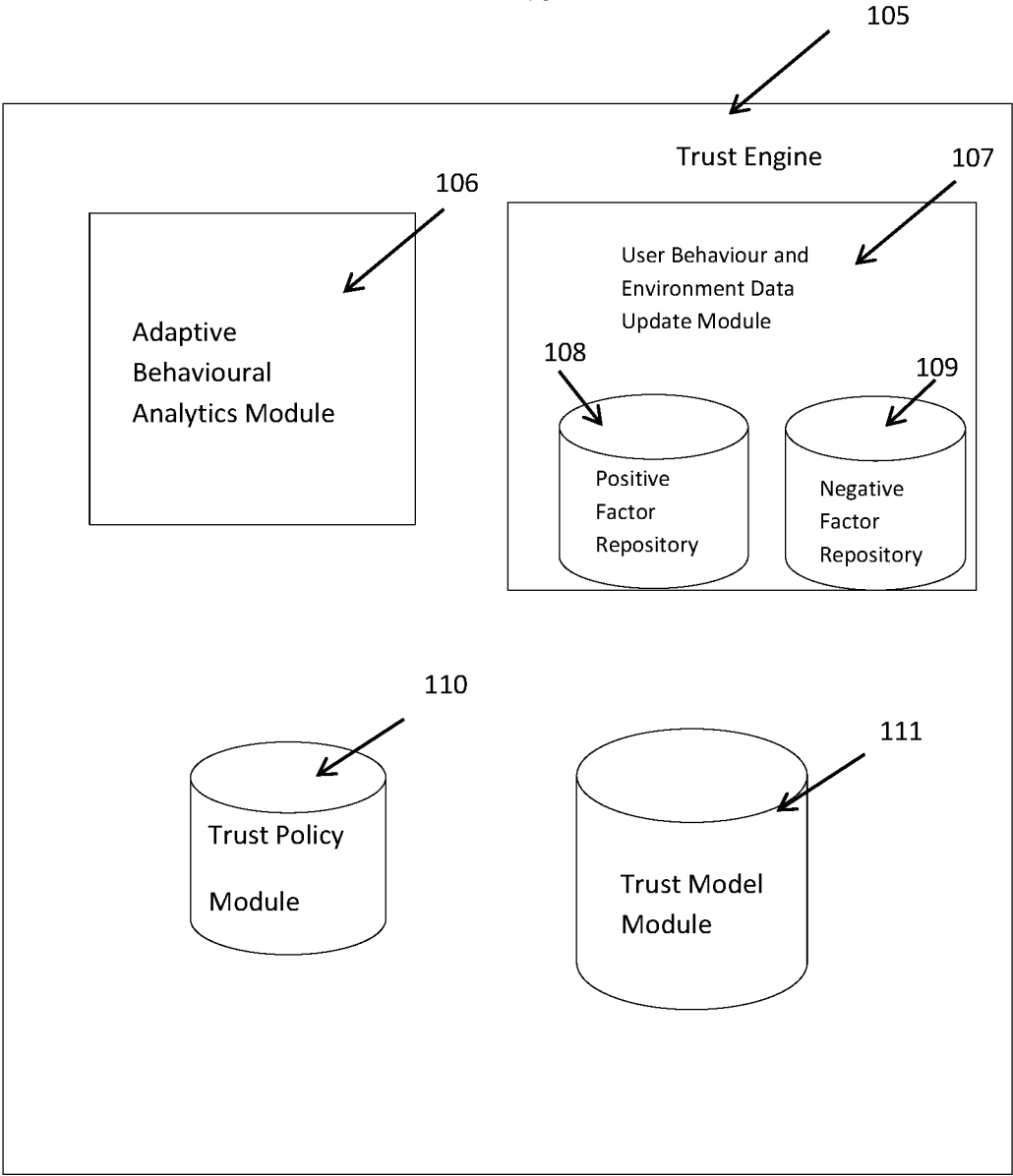


FIG. 2

3/8

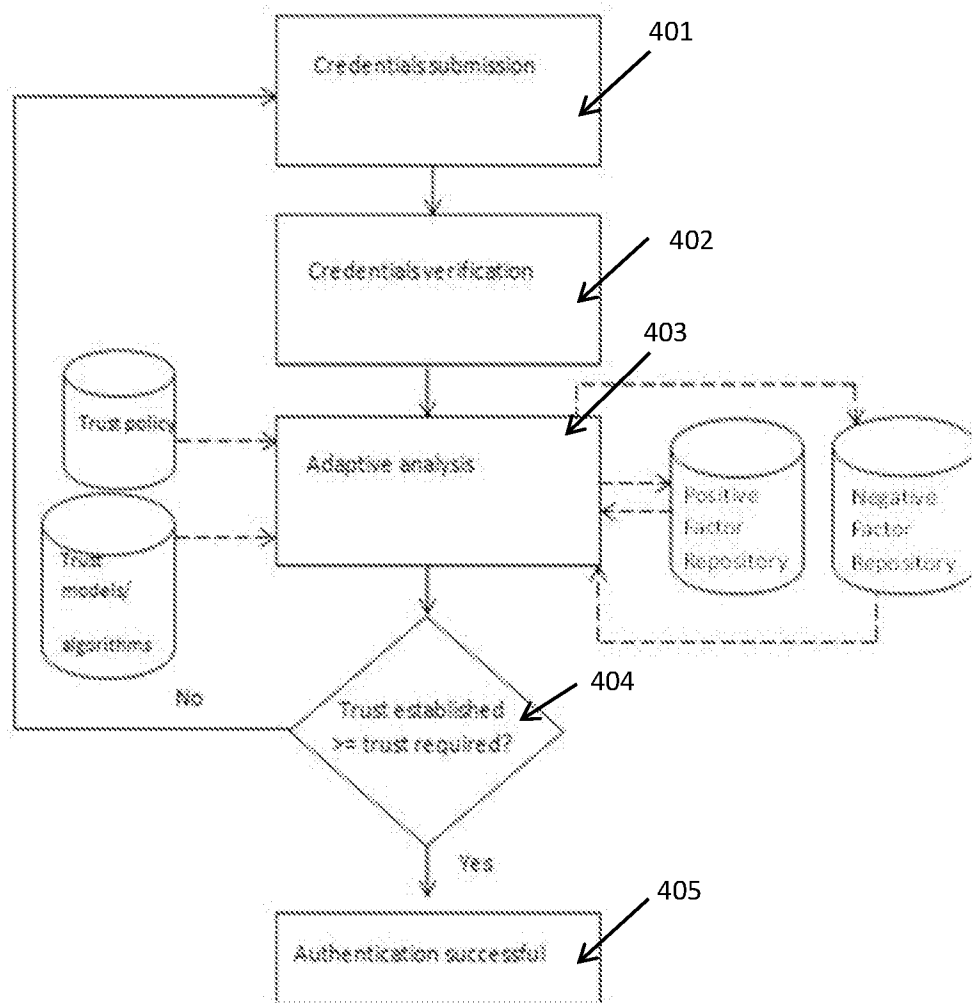


FIG. 3

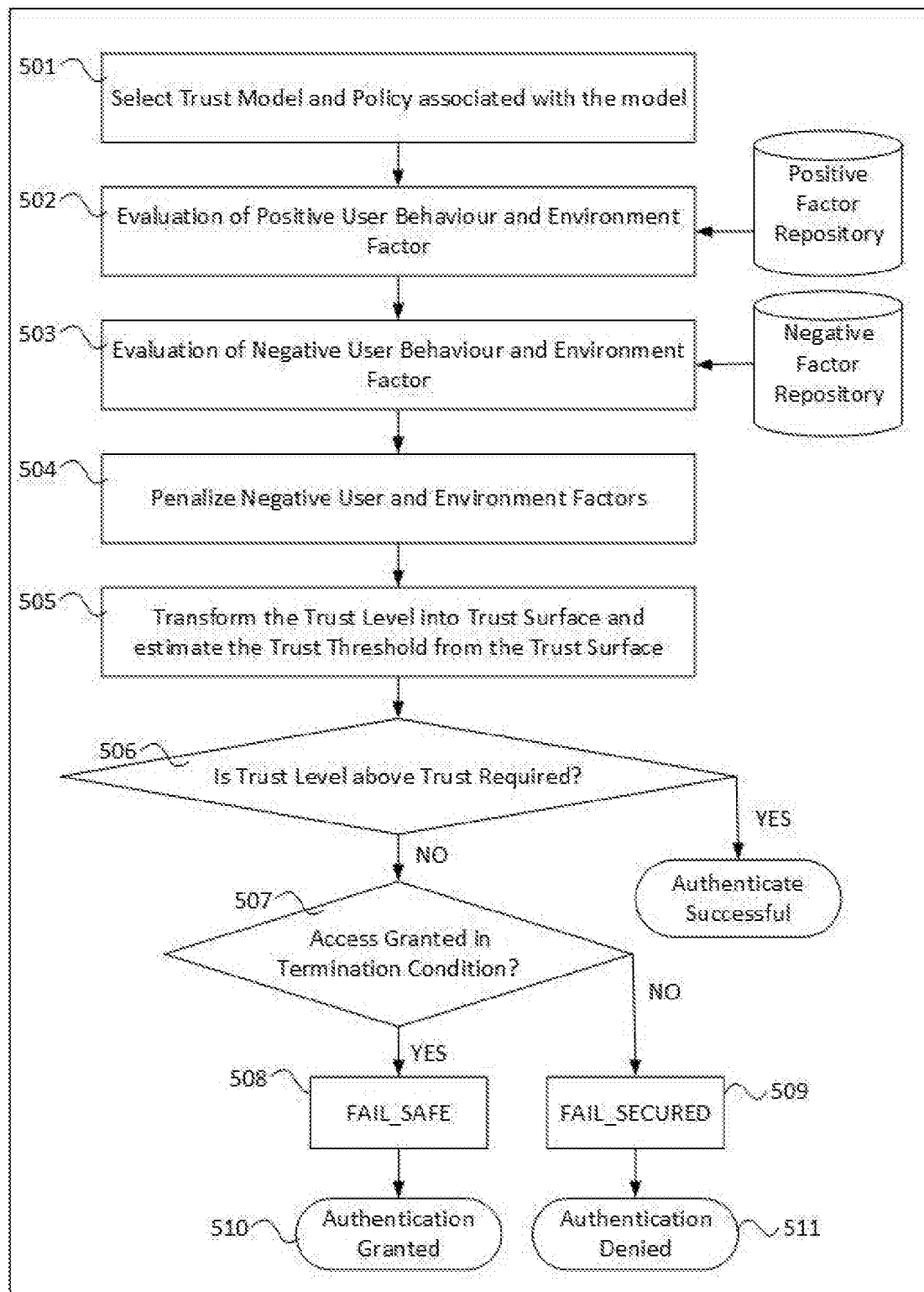


FIG. 4

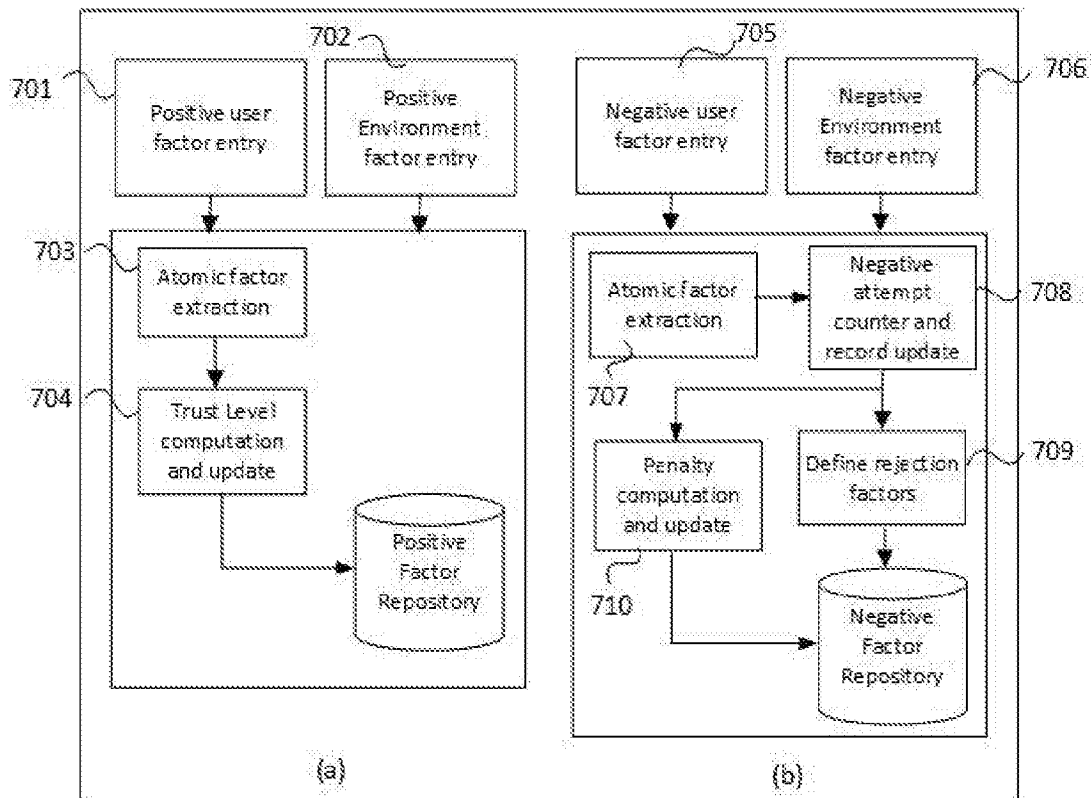


FIG. 5

6/8

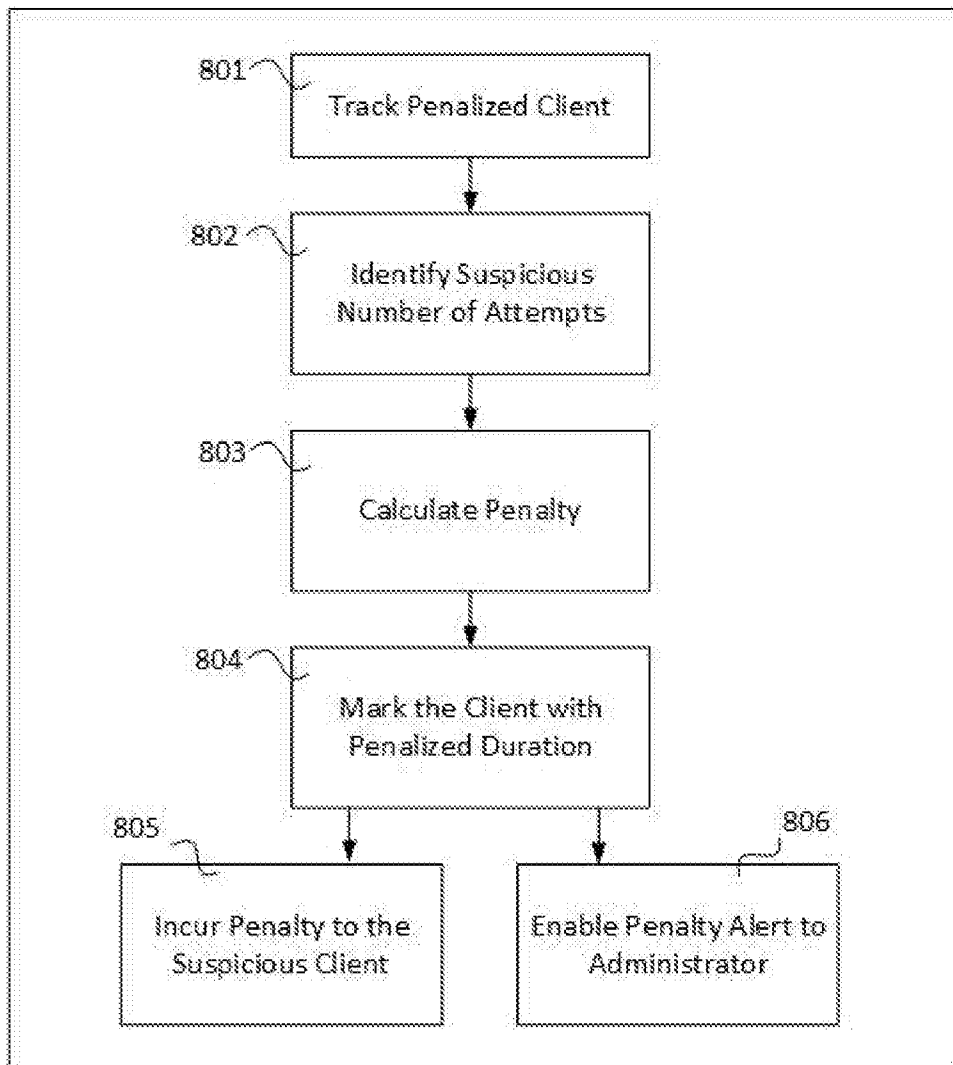


FIG. 6

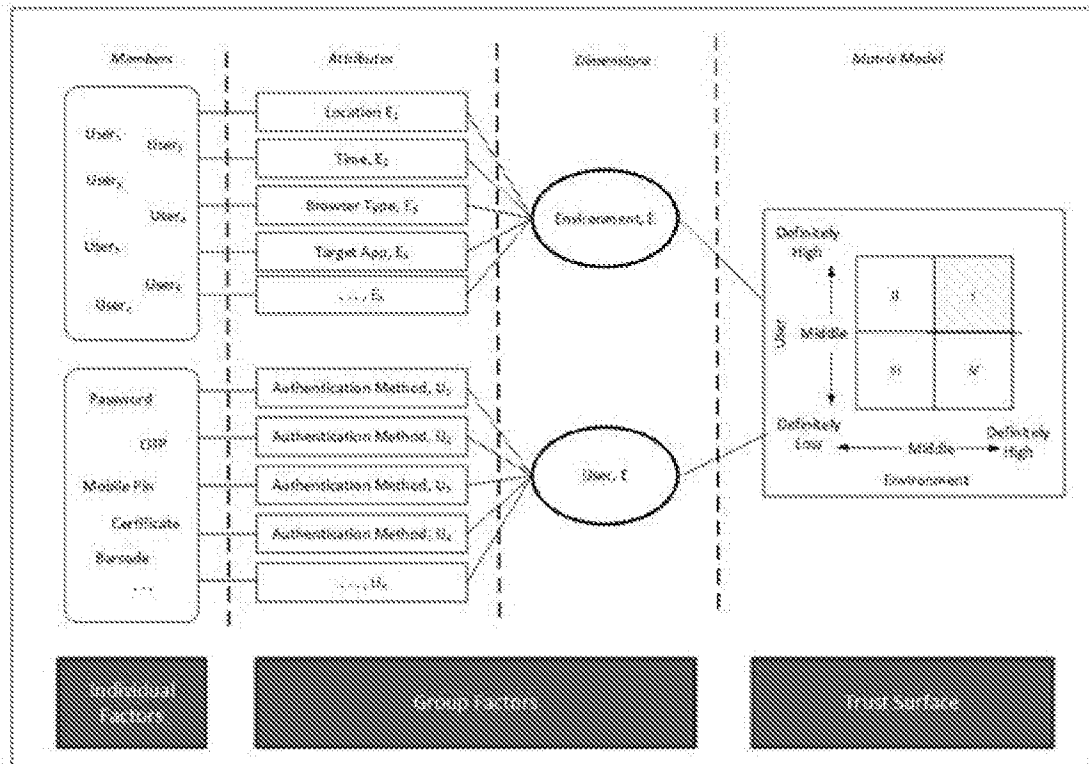


FIG. 7

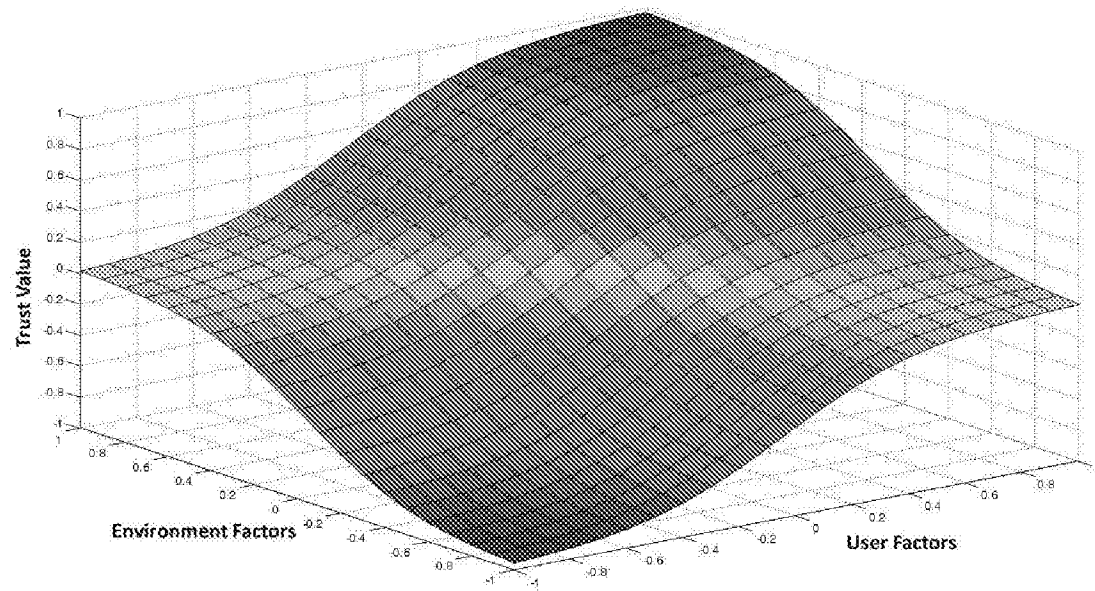


FIG. 8