

SYSTEMS AND METHODS FOR CUSTOMIZABLE AUTHENTICATION AND/OR AUTHORISATION OF ACCESS TO RESOURCES

FIELD OF THE INVENTION

5

[01] The present invention relates to universal login methods and systems, and more specifically to policy-based, dynamic-attribute methods and systems enabling a customizable authentication and/or authorisation of access to resources.

10 BACKGROUND OF THE INVENTION

[02] The background description provided herein is for the purpose of generally presenting the context of the present invention. Work of the presently named inventors, to the extent it is described in this background section, as well as aspects of the description that may not otherwise qualify as prior art at the time of filing, are neither expressly nor impliedly admitted as prior art against the present invention.

[03] For authentication and authorisation, there are currently two main standards, OpenID Connect and OAuth respectively. OpenID Connect standard involves users creating accounts by selecting an OpenID Connect identity provider which will then use those accounts to sign onto any website that accepts OpenID Connect authentication on their behalf. OAuth (Open authorisation) is a token-based open protocol for authentication on the Internet. It allows an end user's account to be used by third-party services like various mobile applications (Twitter, Facebook etc.) by acting as an intermediary on his/her behalf. This intermediary does not give up the user's password but instead provides the third-party services with an access token giving them the authorisation to specific user account information.

[04] However, these two standards do not allow varying access to many user types and do not provide enough tools for data tracking and reporting. They provide limited flexibility in access control hence security is not good enough. The problems with existing technologies (OAuth and OpenID Connect) are further summarized as follows.

[05] **Limited user types for login.** OAuth and OpenID Connect classify users in 2 categories, "allowed access to the resource" and "not allowed access to the resource". This limitation poses a problem to resources that require more than 2 types of access rights, such as providing partial access to some user types. Existing technologies offer only either full access to the resource or completely reject them. The resource administrator still has to implement access control methods for all users that services using OAuth and OpenID Connect allow through. Taking an application as an example, this means that all users that download an application can go through to the application where access control is then determined. The bulk of access control has to be done by the administrator at the end of resource and not by the authenticating and authorising service. This consumes the administrator's

time and effort to set up various control logic, databases and complex user settings and to build these controls into the resource in the form of post-login management and privacy adherence. Such access control methods may also lead to slower performance by the resource. These access control settings are also specific only to that particular resource and cannot be used by other resources.

5

[06] **Lack of customizability and flexibility.** OAuth and OpenID Connect only capture what the login provider sets. For example, any application that uses Google to authenticate their users only captures the user's email address; there is no customization to allow authentication based on attributes that the application administrator wants (e.g. location of login device, timing) even if the administrator is not interested in capturing the email address. This means that existing technology is only able to provide a fixed degree of factor-checking to all resources that they support. Regardless of the security needs of individual resource, all resources supported by OAuth and OpenID Connect services have to undergo the same degree of factor-checking dictated by the services. For example the services either allow all users to access the resources easily or make all users go through strict and tedious factor-checking.

10

[07] **Generic security settings.** Current services leveraging OAuth and OpenID Connect offer generic security settings to all resources that rely on them for authentication and authorisation. A compromise of authentication and authorisation process of one resource could mean that other resources can be exposed to the same danger through similar methods.

15

[08] **Lack of control over limiting users' actions.** Secure resources dealing with sensitive information (such as finance management applications) cannot use single sign-on services such as "Google Sign-in" as such services usually allow users themselves to control the degree of factor-checking that they wish to undergo. Users may unknowingly or deliberately reduce the degree of such checks even when they should not for security reasons. For example, a user can turn off "Two-Factor Authentication" (2FA) on his/her Google account, after which "Google Sign-in" may allow the user to access the resources that it services without 2FA validation. This reduces security in preventing fraudulent access should the account be stolen by someone else.

20

25

[09] **Lack of knowledge of users attempting to login to a resource.** OAuth and OpenID Connect only let the administrator know when a user attempts to login and if the said user logs in successfully or is rejected. No additional information is provided to the administrator that could be used to potentially alert them to nefarious user login attempts and improve their security alertness. This means that an administrator is merely aware that a particular user's login attempt is rejected but not the reason.

30

[10] Therefore, it is one purpose of the present invention to provide authentication and/or authorisation using federated identity. Such authentication and/or authorisation is customizable, for

example, by customizing one or more policies for an application, the application administrator is able to customize the process of the authentication and/or authorisation.

[11] It is another purpose of the present invention to provide authentication and/or authorisation with multiple levels of access right to resources. With multiple levels of access right available, the present invention is able to determine the most suitable level of access right according to the users' real time situation.

[12] It is another purpose of the present invention to provide device dependent systems and methods. For example, an application administrator can decide that an authentication can become less stringent if a user has been using the same device in a safe country; the administrator can even design separate policies for different locations and time. For example, one policy for Singapore during office hours, another one for Singapore after office hours, and a further one for approved countries.

[13] It is another purpose of the present invention to provide systems and methods to avoid the need for any administrator to manage the users' personal information including passwords. This also provides better security as none of the resources stores any information that can be a potential management nightmare. For example, some prior art techniques use user managing modules (e.g. identity routers) at the resource end for the administrator to manage the users; the present invention eliminates the need for any such kind of user managing modules to be connected to the protected resources, this also has the advantage of making sure no malicious code is in the user managing modules.

SUMMARY OF INVENTION

[14] According to one aspect of the present invention, it provides a system for authenticating and/or authorising a user for accessing one of a plurality of resources, comprising:

- a. a client module for processing and storing details of the plurality of resources;
- b. a policy module for processing and storing a plurality of policies, each of which defines one or more factors to be checked for the authentication and/or authorisation;
- c. a user module for processing and storing potential users' information;
- d. a controlling module for controlling and processing the authentication and/or authorisation; and
- e. an authentication token module for processing and storing authentication tokens and details of authentication;

wherein each of the plurality of resources corresponds to one or more policies;
wherein the one or more policies specify different levels of access right for accessing the corresponding resource;

wherein the controlling module determines which policy is applicable based on the user's information and the information stored in the user module; and

wherein the user is authenticated and/or authorised based on the applicable policy.

[15] According to another aspect of the present invention, it provides a method for registering a resource to a system of the present invention by a resource administrator, comprising the steps of:

- 5 a. logging into the system;
- b. registering a client ID with the system;
- c. receiving a secret from the system;
- d. providing allowed domains to the system;
- e. registering or changing one or more policies with the system;
- 10 f. providing potential users' information to the system;
- g. adding a function to redirect logins to the system; and
- h. providing the secret to a backend of the resource.

[16] According to another aspect of the present invention, it provides a method for authenticating a user to access a resource using a system of the present invention, comprising the steps of:

- 15 a. receiving a login request from the user for accessing the resource;
- b. receiving information provided by the user for accessing the resource;
- c. checking potential users' information required for accessing the resource;
- d. comparing the potential users' information required for accessing the resource with the
- 20 information provided by the user;
- e. retrieving all policies corresponding to the resource and determining an applicable policy;
- f. validating one or more factors defined in the applicable policy;
- g. generating an authentication token for the user and storing details of authentication in the
- system; and
- 25 h. authenticating the user by providing the authentication token to the user.

[17] According to another aspect of the present invention, it provides a method for authorising a user with an authentication token to access a resource using a system of the present invention, comprising the steps of:

- 30 a. providing the authentication token to the resource by the user;
- b. retrieving a secret in the resource;
- c. sending the secret, the authentication token and a client ID of the resource from the resource
- to the system;
- d. validating the client ID and secret in the system;
- 35 e. retrieving an OpenID token and details of authentication in the system;
- f. generating an access token and passing it along with the OpenID token to the resource from
- the system; and
- g. authorising the user to access the resource.

[18] According to another aspect of the present invention, it provides a computer program comprising instructions which, when the program is executed by a computer, cause the computer to carry out the above methods.

5 [19] According to another aspect of the present invention, it provides a computer-readable medium comprising instructions which, when executed by a computer, cause the computer to carry out the above methods.

10 [20] According to another aspect of the present invention, the details of the plurality of resources provide corresponding relationship between the plurality of resources and the plurality of policies.

[21] According to another aspect of the present invention, the system further comprises an information collection module for collecting any required information or data.

15 [22] According to another aspect of the present invention, the required information or data is collected manually and/or automatically.

20 [23] According to another aspect of the present invention, the potential users' information is any identity which can be used to identify the potential users, such as username, email address and/or phone number.

[24] According to another aspect of the present invention, the levels of access right include full access right and partial access right.

25 [25] According to another aspect of the present invention, one user may have the full access right and the partial access right under different conditions.

[26] According to another aspect of the present invention, at least one of the plurality of policies is dynamic.

30 [27] According to another aspect of the present invention, if a policy is dynamic, one or more factors defined in the dynamic policy can be changed.

35 [28] According to another aspect of the present invention, the at least one dynamic policy predefines one or more conditions so that when the one or more predefined conditions is/are met, another one of the plurality of policies takes precedence over the at least one dynamic policy.

[29] According to another aspect of the present invention, the system prompts the user to provide any required information which has not been provided by the user.

40

[30] According to another aspect of the present invention, if the resource has multiple differing user types or roles, the system matches the user to a valid user type or role based on the potential users' information.

5 [31] According to another aspect of the present invention, wherein if there is no match from the comparison, the authentication process is to be terminated and a "no-match" error is to be sent to a resource administrator and/or the user with details of the error.

10 [32] According to another aspect of the present invention, if the validation of the one or more factors defined in the applicable policy is not successful, the authentication process is to be terminated and a "no-match" error is to be sent to a resource administrator and/or the user with details of the error.

15 [33] According to another aspect of the present invention, the one or more factors defined in the applicable policy can be fulfilled by the information provided by the user, by information collected by the system or by information stored in the system.

20 [34] According to another aspect of the present invention, the information collected by the system is selected from the group of ID of accessing device, location of accessing device, accessing time and country in which the user is making access.

[35] According to another aspect of the present invention, the information provided by the user includes any of birthdate, pin number, location, title, username, email address and phone number.

25 **BRIEF DESCRIPTION OF THE DRAWINGS**

[36] Figure 1 depicts a process of an application administrator registering the application on a sign-on service that uses OAuth and OpenID Connect according to a prior art technique.

30 [37] Figure 2 depicts a process of a user signing into an application using OAuth and OpenID Connect according to a prior art technique.

[38] Figure 3 depicts how access control is implemented with the use of OAuth and OpenID Connect according to a prior art technique.

35

[39] Figure 4 depicts how access control is implemented according to one embodiment of the present invention.

40 [40] Figure 5 depicts a system for authentication and/or authorisation according to one embodiment of the present invention.

[41] Figure 6 depicts an example of a policy and its structure according to one embodiment of the present invention.

[42] Figure 7 depicts a flow chart showing details of a process that a resource administrator may use to register a resource onto a system in order to begin using its services according to one embodiment of the present invention.

[43] Figure 8 depicts a flow chart showing the authentication of a potential user of an application according to one embodiment of the present invention.

[44] Figure 9 depicts a flow chart showing details of a process of authentication using some of the components as depicted in Figure 5 according to one embodiment of the present invention.

[45] Figure 10 depicts a flow chart showing details of a process of authorisation after the user has been authenticated according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[46] While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed or terms used, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

[47] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, that the present invention may be practised without these specific details. Well-known methods, procedures and components have not been described in detail so as not to unnecessarily obscure aspects of the implementations.

[48] In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks, steps and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

[49] Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to affect the communication.

[50] Several features are described hereafter that can each be used independently of one another or with any combination of other features. However, any individual feature may not address any of the problems discussed above or might only address one of the problems discussed above. Some of the problems discussed above might not be fully addressed by any of the features described herein. Although section headings are provided, information related to the subject under a particular heading, but not found in the section under that heading, may also be found elsewhere in the specification.

[51] It will also be appreciated that, although the terms first, second, etc. may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another and not necessarily to suggest a fixed sequential order. For example, a first item could be termed a second item, and, similarly, a second item could be termed a first item and so on.

[52] The terms “comprise”, “contain” and “include” are generally interpreted as being non-exhaustive and open-ended, which means other alternatives might be included, no matter which form they are in. For example, “a combination comprising components A and B” could include a combination of components A, B and C.

[53] It will also be appreciated that the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will further be understood that the term “and/or” as may be used herein refers to and encompasses any and all possible combinations of one or multiple of the associated listed items.

[54] The definitions of some terms are provided below which apply throughout the present invention. Unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by those skilled in the art to which the present invention belongs.

[55] “Resource” is a resource or supply of information, documents or functionalities that potential users may wish to access, obtain, amend or use. For example, a resource can be a computer software application for realizing certain functionalities, a resource can also be a database from which

a user can access, amend, edit or delete any information therein provided that such user has the right to do so.

[56] "Federated Identity" is an account created in one system which can be used to log in to a different system. For example, for a first system with a first Identity Provider (FIdP) which provides users and a Service Provider (SP) to which users log in, and for a second system with a second Identity Provider (SIdP) which provides users and the same SP to which users log in, a common user of both FIdP and SIdP can be provided with an account by the same SP to log in to FIdP and SIdP.

[57] "Attribute" is a property of the potential users to be declared before accessing a resource. Each individual resource defines the types and number of attributes required from their users in order to gain access thereto (e.g. Phone Number, Email Address and Username). For example, upon logging in, a user must enter an email address, his/her birthdate and a phone number that matches that stored in the database in order to be granted access to the resource.

[58] "Policy" is a set of factors that need to be fulfilled by a potential user in order to be granted access to the resource during the logging-in process. Policy chosen to be used in authenticating and/or authorising the user will be determined by the conditions set by the resource administrator beforehand. For example, a resource administrator may have provided 2 policies upon registering the resource into the SP, "Policy A" and "Policy B". "Policy A" is used to authenticate and authorise users within Singapore whereas "Policy B" is used to authenticate and authorise users in countries outside Singapore. For example, when a user logs in, the user's location can be detected in order to decide which policy, "Policy A" or "Policy B" to apply to the user. A user logging in from Singapore will need to validate 1 factor in order to gain access to the resource under "Policy A" whereas a user logging in from Indonesia will need to validate 2 factors in order to gain access to the same resource under "Policy B".

[59] "Factor" is a condition that needs to be fulfilled in order for users to access a resource during the logging-in process. Factor(s) to be used are determined by the policy applicable to the users. For example, under "Policy A" mentioned above, a user located in Singapore may only access the resource upon validating the factor "must be located in Orchard Road" by providing his location via GPS. If the said user is not in Orchard Road, the authenticating and/or authorising system will deny the user's access to the resource and notify the resource administrator and/or the user depending on the policy specifications. In another example, under "Policy B" mentioned above, a user located in Indonesia must validate the following 2 factors:

- a) validating his email address by providing an 8-character alphanumeric code emailed to him after initiating the login attempt; and
- b) providing his/her birthdate upon prompting.

[60] Figure 1 depicts a process of registration of an application 104 to an SP 102 using OAuth and OpenID Connect by an application administrator 100 according to a prior art technique, comprising the following steps:

1. The application administrator 100 logs into the SP 102.
2. The application administrator 100 registers a client ID with the SP 102.
3. The SP 102 returns a secret to the application administrator 100.
4. The application administrator 100 provides allowed domains to the SP 102.
- 5a. The application administrator 100 adds a button to redirect login to the SP 102.
- 5b. The application administrator 100 provides the secret to the backend of the application 104.

[61] Figure 2 depicts a process of a user signing into an application 204 through an SP 202 using OAuth and OpenID Connect according to a prior art technique, the process comprises:

1. After the user 200 clicks the button of the application 204, he/her is redirected to the SP 202.
2. The SP 202 initiates the process and prompts the user 200 to proceed further.
3. The SP 202 matches the user's sign-in information.
4. If the user 200 signs in successfully, the SP 202 provides an OAuth Token to the user 200.
5. The user 200 then can provide the OAuth Token to the backend of the application 204.
6. The backend of the application 204 sends the OAuth Token and secret to the SP 202 for verification.
7. Once verified, the SP 202 provides access token and ID token to the backend of the application 204.
8. The backend of the application 204 grants the user 200 access to the application 204.

[62] Figure 3 depicts how access control is implemented for applications with the use of OAuth and OpenID Connect according to a prior art technique. As depicted in Figure 3, the access control is rendered individually at the application side. The user 300 logs in different applications through the same system 302. The access control 304, 306 and 308 are managed separately at the backend of each of the applications 310, 312 and 314. It is appreciated that, in such kind of systems, an application administrator needs to control each user's access right at the backend of the application, which costs a lot of time and effort for setting up the configuration and for subsequent maintenance of such configuration. Further, if there are different levels of access right for different conditions for the same user, more time and effort will be required for the configuration and maintenance.

[63] Figure 4 depicts how access control is implemented for applications using a system 404 according to one embodiment of the present invention. As depicted in Figure 4, the access control 402 is managed at the system 404 side. It is able to decide the levels of access right the users 400 are permitted before they enter the applications 406, 408 and 410 through the use of policies, thus providing a complete authentication and/or authorisation service necessary for the application administrator(s) or developer(s) in contrast to existing technologies which provide a partial service.

[64] Figure 5 shows a system 500 built upon the currently known standards of OAuth and OpenID Connect standard according to one embodiment of the present invention. In this embodiment of the present invention, the system comprises a Policy Module 502, a User Module 504, a Controlling Module 506, an Authentication Token Module 508, a Client Module 510 and an Information Collection Module 512. The details of each module are further described as below:

- **Policy Module 502**

It is in this Policy Module 502 that one or more policies determining the types of users allowed to access one or more resources and the corresponding levels of access right are also stored. Policies also specify any factors to check in order to grant users such access right.

- **User Module 504**

It is in this User Module 504 that users and their attributes (e.g. username, email address, phone number, etc.) to be matched are stored. A potential user has to match their respective attributes to that stored in this module in order to gain access to a resource.

- **Controlling Module 506**

Controlling Module 506 connects resources and different modules and dictates the logical flow of the process of the authentication and/or authorisation. The roles or types of users are specified in the controlling Module 506. Such roles or types would determine the users' levels of access right to the resources as dictated by their corresponding policies. Overall, the Controlling Module 506 controls and processes the authentication and authorisation.

- **Authentication Token Module 508**

It is in this Authentication Token Module 508 that Authentication Tokens and details of authentication are stored. An Authentication Token is provided to an authenticated user who will present it to the resource to gain access.

- **Client Module 510**

The Client Module 510 stores details of resources using service of the system 500. Such details may include which policies in the Policy Module 502 correspond to each of the resources.

- **Information Collection Module 512**

Optionally, an Information Collection Module 512 is included for collecting any information or data that is required to be collected according to the applicable policies. Such information or data may be provided by the user or auto-collected by the Information Collection Module 512. The information or data to be collected may include country in which the user is requesting for access, specific location of access, information of the device used to access (e.g. ID of the accessing device, types of device, etc.) and time of access, etc. Such information may also

include the history login data for the assessment of subsequent authentication and/or authorisation.

[65] Every time a user requests to login to a resource, the Controlling Module 506 will look up the attributes required by the resource that are registered. The user will then need to provide the attributes (e.g. email, username) he/she knows to initiate the authentication process.

[66] The User Module 504 may then match the user to a type or role declared by the resource beforehand. The user will gain the level of access right allowed to that specific type or role of users as matched. Optionally, if the resource treats all its users the same in terms of access provided, this matching process may be skipped.

[67] It is appreciated that each user may have one or more roles or types, subject to the definition and configuration of policies. For example, a policy may define that a user has the right to read and edit during office hours but only has the right to read after office hours. As another example, a user may be downgraded to a normal user from an administrator role when he/she is overseas.

[68] The Client Module 510 will then decide which policy is suitable to be applied to the user and then proceed to get the relevant policy factors (e.g. login device ID, time of day, location, etc.) that it is concerned with from the Policy Module 502. The Controlling Module 506 will check database for a matching policy to be applied to the user.

[69] Policy factors can be inputted manually (e.g. phone number, staff ID, email address) or collected or generated automatically (e.g. location, number of days since last logged in, login device ID). Policy factors can also be automatically captured and stored in the system based on past login inputs and used again automatically if the same user and policy is used. For example, should "User Y" login to the application under "Policy Z" for the second time and "User Y" previously, on his first login, provided his birth date also under prompting by "Policy Z", User Y may not need to input his birth date again as the entered birth date is stored in the invention. The Controlling Module will provide the stored birth date to fulfill "Policy Z" resulting in more convenience for "User Y".

[70] The provided/captured factors are checked as to whether they fulfill the required factors of the policy. If all the factors of the policy are fulfilled, the Authentication Token Module 508 will proceed to provide the user with an Authentication Token.

[71] If the login attempt is considered to be legitimate, the subsequent approval process for allowing the user to use the resource is similar to those commonly known frameworks. To proceed with authorisation of the user, the resource provides an authentication token back to the system, the details of the method will be further described below.

[72] If the login attempt is considered to be illegitimate, the user's login attempt will be rejected and made known to the resource administrator. For example, if a Policy defines that a user can only use an application if he/she is physically in Singapore, the system may detect the user's physical location when he/she requests to use the application and reject the access request if he/she is outside of Singapore; and the administrator/user can be informed that the rejection was due to the non-compliance of the user's physical location when request. As another example, if a policy defines that a user can only access the first part of a database after office hours, and the same user can access the first and second parts of the database during office hours, the system may reject the user's request to access the second part of the database after office hours and inform the administrator/user that the rejection was due to the non-compliance of the user's accessing time. It is appreciated that, with such a system, the resource administrator will be able to configure different levels of access right and the associated conditions. Therefore, the present invention makes it possible for the administrators to understand the detailed information of why a user was rejected, rather than merely know the occurrence of a rejection as with existing technologies.

[73] The resource administrator is able to design different policies as desired. As an example according to one embodiment of the present invention, the policy depicted in Figure 6 contains multiple factors, "Description", "Day", "Location", "Device Security", "Time", "Duration since first login" etc. The policy may also contain a list of factors and provide a function of adding factors for the convenience of the resource administrator. When designing a policy, the resource administrator may include any factors shown by default, or choose any factors in the List of Factors. In case that one or more desired factors are not found in the provided list of factors, the resource administrator is able to add such factor(s).

[74] According to one embodiment of the present invention, as depicted in Figure 7, the resource administrator 700 may register a resource to the system 702 with the following steps:

1. The resource administrator 700 logs into the system 702.
2. The resource administrator 700 registers a Client ID with the system 702.
3. The system 702 returns a Secret to the resource administrator 700.
4. The resource administrator 700 provides allowed domains to the system 702.
5. The resource administrator 700 registers or changes the policy attributes with the system 702.
6. The resource administrator 700 populates matches to the system 702 by providing the potential users' information to the system 702.
- 7a. The resource administrator 700 adds a button to redirect login to the system 702.
- 7b. The resource administrator 700 provides the Secret to the backend of the resource 704.

[75] Figure 8 depicts the flow of authenticating a potential user of a resource according to one embodiment of the present invention. As a first step 800, the user needs to provide attributes to the system. Optionally, as a second step 802, the system may match the attributes provided by the user. In step 804, the system decides which policy to apply according to the attributes matched. In step

806, after the applicable policy is decided, the system checks the compliance of the user with the factors of the applicable policy. In step 808, if it is confirmed that the user is complying with the applicable policy, Authenticating Token will be provided to the user.

- 5 [76] Figure 9 depicts a flow chart showing details of process of authentication using the components of the system 500 according to the embodiment as depicted in Figure 5:
1. User 900 attempts to login to a resource using the system 500, for which the user 900 needs to hand over Client ID and other attributes to prove his/her identity.
 2. Controlling Module 506 checks the Client Module 510 to learn what type of attributes to check
10 for users of that specific resource.
 - 2a. If there are missing attributes required by the resource, the Controlling Module 506 prompts the user 900 to provide the missing attributes.
 3. The attributes stored in the User Module 504 are retrieved and compared with that provided by the user 900. If the attributes match, the authentication procedure continues, otherwise the
15 authentication process will terminate with a “no-match” error raised to the resource administrator and/or the user 900.
 4. (Optional) If the resource has multiple differing user types or roles, the Controlling Module 506 matches the user to a valid user type or role.
 - 4a. If a match is found, the Controlling Module 506 will deem the user logging in as the matched
20 type or role, otherwise the authentication process will terminate with a “no-match” error raised to the resource administrator and/or the user 900.
 5. The Controlling Module 506 will retrieve all policies from the Policy Module 502 that was provided by the resource to which the user 900 wishes to login.
 - 5a. The Controlling Module 506 will return and apply the first policy that matches the conditions of
25 the specific login attempt as a suitable policy.
 6. Actions in the suitable policy are then performed to validate the factors declared in the suitable policy.
 - 6a. (Optional) If factors that require user to input (e.g. birthdate, pin number, location) exist, the Controlling Module 506 will fulfill these factors by prompting the user for additional inputs,
30 demand the Information Collection Module 512 to automatically collect factor information (e.g. Device ID, Device location via GPS) or use past factor values to fulfill the factors of the suitable policy.
 - 6b. The factors of the suitable policy are then validated.
 7. If the factors of the suitable policy are fulfilled, the Controlling Module 506 will then proceed to
35 generate an Authentication Token for the user and stores the details of the authentication into the Authentication Token Module 508.
 8. The Authentication Token is provided to the user for the user to subsequently proceed on with the authorisation process.

[77] Figure 10 depicts a flow chart showing some details of the process of authorisation after the user has been authenticated using the components of the system 500 according to the embodiment as depicted in Figure 5, which comprises the following steps:

- 1) User 1000 provides the Authentication Token to the backend of the resource 1002.
- 2) The resource 1002 retrieves the Secret from its own database 1004.
- 3) The resource 1002 sends the Secret, Authentication Token and Client ID to the Controlling Module 506.
- 4) The Controlling Module 506 validates the Client ID and Secret provided.
- 5) The Controlling Module 506 retrieves an OpenID Token and details of authentication from the Authentication Token Module 508 using the Authentication Token.
- 6) The system 500 generates an Access Token and passes it along with the OpenID Token to the resource 1002.
- 7) The resource 1002 authorises the user 1000 to proceed to use the resource 1002.

[78] It is appreciated that the systems and methods of the present invention provide a policy-based authentication and/or authorisation which can be customized by the resource administrator. The resource administrator is able to provide the policies that he/she wants the potential user to adhere to in order to access the resource. Policies are used to determine the users' levels of access right to the resource.

[79] Therefore, the systems and methods of the present invention enable authenticating users according to any number and types of attributes indicated in the policies designed by the resource administrator. For example, for a resource which allows only users geographically present in Singapore to access, the geographical coordinates of the device could be used in the authentication and/or authorisation process. The resource administrator can add, delete or change the policies whenever desired.

[80] Policies can also allow differences in degree of factor-checking required between various login methods in contrast to fixed factor checks. For example, a user using a smart phone to log in may be required to follow up with an input of a 6-digit code sent to him/her via SMS to be allowed access into the resource whereas a user logging in via a registered corporate laptop (identified by Device ID) does not need to.

[81] In the present invention, the attribute-checking process in authentication and/or authorisation is dynamic through the use of policies. This means that the number and types of attributes used in authenticating and/or authorising a user may change in accordance to the policy used to authenticate and/or authorise the said user. This provides convenience to frequent compliant users while maintaining security barriers against nefarious users and preventing fraudulent access. In other words, a first policy may base on certain conditions as desired/predefined refer to a second policy so that such second policy may take precedence; further, such second policy may return the precedence

to such first policy or refer the precedence to a third policy if certain other conditions as desired/predefined are met.

[82] For example, a user logging into a resource for the first time may be required to provide 4 attributes (e.g. username, email, location and phone number) under "Policy C". After one month of usage, the user's authentication and/or authorisation method may switch to "Policy D" for subsequent logins where only username and location may be required. The user's authentication and/or authorisation method may switch back to "Policy C" again where 4 attributes are required if the system detects that the user is attempting to log in from overseas. As a further example, if a user keeps accessing the resource under "Policy D" with a particular device, the user's authentication and/or authorisation method may switch to "Policy E" for subsequent logins where only username may be required.

[83] The resource administrator's time and effort are saved by the avoidance of the need to implement user access controls in the form of post-login management and privacy adherence (as seen in Figure 3) as these functionalities are done by the system (as seen in Figure 4). Access controls refer to a system in place to determine the levels of access right to the resource that an authenticated and authorised user may have (e.g. User of role "Supervisor" may have access to more functionalities of the application than that of role "Employee").

[84] The present invention offers enhanced security as multiple factors can be used in authorisation and authentication. For example, even with a password stolen, the thief may not be able to log into the stolen account with a similar device as the policy can dictate that the exact same last login device must be used in order to be granted access.

[85] The present invention allows resource administrators to create different user account types with differing levels of access right to different portion of the resource. This is done through the use of policies, such as one policy for each type of users. Hence, the present invention helps support resources that need multiple user types.

[86] The invention allows each individual resource to decide the level of security it requires in its authentication and/or authorisation process. Each resource decides the number of attributes required alongside the number and degree of factors to check. Hence, each resource can control for itself its level of security it wishes to impose on potential users.

[87] The invention allows resource administrators to decide the degree of factor-checking that is required to access the resource instead of letting the user decide. This upholds the complex factor-checking standard required by secure resources holding sensitive information in order to maintain high level of security.

Application of the present Invention

[88] Generally, the present invention can be used by any existing resource with an authentication and/or authorisation process. Resources using external existing technology for authentication and/or authorisation (Google etc.) can switch to a system according to the present invention easily by simply providing policies.

[89] Resources that are already using third-party authentication and/or authorisation services like "Google Sign-in" can switch to a system according to the present invention if their administrators want more customization and flexibility. This can be easily done by assigning and providing policies to a system according to the present invention. Policies can be added, deleted or modified at any time. Policies can contain any number and types of factors as dictated by the resource administrator, such as location, type of device used for login and number of days since last logged-in.

[90] Resources in a system according to the present invention will provide policies to the Controlling Module 506 to dictate the user types or roles that the resources will allow access as well as the associated levels of access right. For example, a resource administrator can provide the invention with 2 policies. 1 for current employees which gives the user full access to the resource and 1 for ex-employees which gives the user partial access to the resource. If the user does not match either of these policies, user would be rejected access to the resource. Hence, access control to the resource does not have to be done internally which would require a lot more time and efforts in terms of server and database maintenance by the resource administrator. The complexity of the policy is up to each resource administrator to set. Hence, the present invention is able to cater authentication and/or authorisation process for any resources.

[91] While the disclosure contained herein has set forth some of the preferred embodiments and application of the present invention, it is not intended to limit that the present invention can only be implemented/applied/used as in these embodiments/examples. It will be appreciated by those skilled in the art that variations to the combination of elements and steps disclosed may be made without departing from the scope and spirit of the invention. Such variations may include, but are not limited to, selection of alternate platforms and operating systems, and implementation of the process as a servlet or other program embodiment.

CLAIMS

1. A system for authenticating and/or authorising a user for accessing one of a plurality of resources, comprising:

- a. a client module for processing and storing details of the plurality of resources;
 - b. a policy module for processing and storing a plurality of policies, each of which defines one or more factors to be checked for the authentication and/or authorisation;
 - c. a user module for processing and storing potential users' information;
 - d. a controlling module for controlling and processing the authentication and/or authorisation;
 - and
 - e. an authentication token module for processing and storing authentication tokens and details of authentication;
- wherein each of the plurality of resources corresponds to one or more policies;
- wherein the one or more policies specify different levels of access right for accessing the

corresponding resource;

wherein the controlling module determines which policy is applicable based on the user's information and the information stored in the user module; and

wherein the user is authenticated and/or authorised based on the applicable policy.

2. The system of claim 1, wherein the details of the plurality of resources provide corresponding relationship between the plurality of resources and the plurality of policies.

3. The system of claim 1 or 2, wherein the system further comprises an information collection module for collecting any required information or data.

4. The system of claim 3, wherein the required information or data is collected manually and/or automatically.

5. The system of any one of the preceding claims, wherein the potential users' information is any identity which can be used to identify the potential users.

6. The system of claim 5, wherein the potential users' information includes any of username, email address and phone number.

7. The system of any one of the preceding claims, wherein the levels of access right include full access right and partial access right.

8. The system of claim 7, wherein one user may have the full access right and the partial access right at different conditions.

9. The system of any one of the preceding claims, wherein at least one of the plurality of policies is dynamic.

10. The system of claim 9, wherein if a policy is dynamic, one or more factors defined in the dynamic policy can be changed.

11. The system of claim 9, wherein the at least one dynamic policy predefines one or more conditions so that when the one or more predefined conditions are met, another one of the plurality of policies takes precedence over the at least one dynamic policy.

12. A method for registering a resource to a system according to any one of claims 1-11 by a resource administrator, comprising the steps of:

- a. logging into the system;
- b. registering a client ID with the system;
- c. receiving a secret from the system;
- d. providing allowed domains to the system;
- e. registering or changing one or more policies with the system;
- f. providing potential users' information to the system;
- g. adding a function to redirect logins to the system; and
- h. providing the secret to a backend of the resource.

13. A method for authenticating a user to access a resource using a system according to any one of claims 1-11, comprising the steps of:

- a. receiving a login request from the user for accessing the resource;
- b. receiving information provided by the user for accessing the resource;
- c. checking potential users' information required for accessing the resource;
- d. comparing the potential users' information required for accessing the resource with the information provided by the user;
- e. retrieving all policies corresponding to the resource and determining an applicable policy;
- f. validating one or more factors defined in the applicable policy;
- g. generating an authentication token for the user and storing details of authentication in the system; and
- h. authenticating the user by providing the authentication token to the user.

14. The method of claim 13, wherein the system prompts the user to provide any required information which has not been provided by the user.

15. The method of claim 13 or 14, wherein if the resource has multiple differing user types or roles, the system matches the user to a valid user type or role based on the potential users' information.

16. The method of any one of claims 13 to 15, wherein if there is no match from the comparison, the authentication process is to be terminated and a “no-match” error is to be sent to a resource administrator and/or the user with details of the error.

5

17. The method of any one of claims 13 to 15, wherein if the validation of the one or more factors defined in the applicable policy is not successful, the authentication process is to be terminated and a “no-match” error is to be sent to a resource administrator and/or the user with details of the error.

10

18. The method of any one of claims 13 to 17, wherein the one or more factors defined in the applicable policy can be fulfilled by the information provided by the user, by information collected by the system or by information stored in the system.

15

19. The method of claim 18, wherein the information collected by the system is selected from the group of ID of accessing device, location of accessing device, accessing time and country in which the user is making access.

20

20. The method of any one of claims 15 to 19, wherein the information provided by the user includes any of birthdate, pin number, location, title, username, email address and phone number.

20

21. A method for authorising a user with an authentication token according to any of claims 13 to 20 to access a resource using a system according to any of claims 1 to 11, comprising the steps of:

25

- a. providing the authentication token to the resource by the user;
- b. retrieving a secret in the resource;
- c. sending the secret, the authentication token and a client ID of the resource from the resource to the system;
- d. validating the client ID and secret in the system;
- e. retrieving an OpenID token and details of authentication in the system;
- f. generating an access token and passing it along with the OpenID token to the resource from the system; and
- g. authorising the user to access the resource.

30

22. A computer program comprising instructions which, when the program is executed by a computer, cause the computer to carry out the method according to any one of claims 12 to 21.

35

23. A computer-readable medium comprising instructions which, when executed by a computer, cause the computer to carry out the method according to any one of claims 12 to 21.

40