

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a cloud computer system, from a mobile computing device, a request for a service from an enterprise computer system, wherein the cloud computer system is located at a first geographical location that is different from a second geographical location of the enterprise computer system, and wherein the cloud computer system and the enterprise computer system communicate over a public communication network;

obtaining, by the cloud computer system, for a user of the mobile computing device associated with the request, a security authentication to obtain at least one service through the cloud computer system;

storing, by the cloud computer system, information indicating the security authentication;

identifying, based on the security authentication of the user, by the cloud computer system, a plurality of enterprise computer systems accessible to the user through the cloud computer system;

verifying, by the cloud computer system, that the enterprise computer system is included in the plurality of enterprise computer systems accessible to the user;

determining, by the cloud computer system, a security protocol for requesting the service from the enterprise computer system;

generating, by the cloud computer system, a security token corresponding to the determined security protocol for the enterprise computer system, wherein the security token is generated based on the information indicating the security authentication of the user; and

sending, by the cloud computer system, to the enterprise computer system, a request for the requested service, wherein the request includes the generated security token.

2. The method of claim 1, wherein at least one of the plurality of enterprise computer systems communicates using a different security protocol than a different one of the plurality of enterprise computer systems.

3. The method of claim 1 or 2, wherein the request received from the mobile computing device and the request sent to the enterprise computer system conform to different representational state transfer (REST) architectural styles.

4. The method of claim 1 or 2, wherein the request received from the mobile computing device includes a first hypertext transfer protocol (HTTP) message and wherein the request sent to the enterprise computer system includes a second HTTP message.

5. The method of any of claims 1 to 4, wherein the request received from the mobile computing device includes user identity information of the user.

6. The method of any of claims 1 to 5, further comprising:
sending a request to an identity management system to determine the security authentication of the user.

7. The method of any of claims 1 to 6, wherein the security token is structured in a format using Security Assertion Markup Language (SAML).

8. The method of any of claims 1 to 7, wherein the plurality of enterprise computer systems includes an enterprise computer system having an on-premises agent system, wherein the on-premises agent system including a plurality of server computers, each server computer providing a different enterprise service, and wherein the on-premises agent system communicates with the cloud computer system over the public communication network.

9. The method of any of claims 1 to 8, wherein the cloud computer system provides an application programming interface (API), the API using a first communication protocol to receive requests for services, wherein each enterprise computer system of the plurality of enterprise computer systems uses a second communication protocol to receive requests for services, and wherein the second communication protocol is different from the first communication protocol.

10. The method of claim 9, wherein the first communication protocol and the second communication protocol conform to a hypertext transfer protocol (HTTP).

11. The method of claim 9 or 10, wherein each enterprise computer system of the plurality of enterprise computer systems supports a different second communication protocol for receiving requests for services.

12. The method of any of claims 9 to 11, wherein the API is configurable by a user of the mobile computing device.

13. The method of any of claims 9 to 12, wherein the cloud computer system includes a database that stores metadata corresponding to one or more configurations of the API.

14. The method of any of claims 9 to 13, further comprising:
converting the request from a format of the first communication protocol to a different format corresponding to the second communication protocol, wherein the converted request is sent to the enterprise computer system.

15. The method of any of claims 9 to 14, further comprising:
receiving, from the enterprise computer system, a response for the requested service, wherein the response has a format of the second communication protocol of the enterprise computer system;

converting the response from the format of the second communication protocol to a format of the first communication protocol; and
providing the converted response to the mobile computing device.

16. A computer system comprising:
one or more processors; and
one or more memory devices coupled to the one or more processors, the one or more memory devices containing instructions which when executed on the one or more processors, cause the one or more processors to:

receive, from a mobile computing device using a first communication protocol, a request for a service, wherein the service is provided by an enterprise computer system, wherein the enterprise computer system is located at a first geographical location that is different from a second geographical location of the computer system, and wherein the enterprise computer system and the computer system communicate over a public communication network;

obtain, for a user of the mobile computing device associated with the request, a security authentication to obtain at least one service via the computer system;

store information indicating the security authentication;

identify, based on the security authentication of the user, a plurality of enterprise computer systems accessible to the user through the cloud computer system;

verify that the enterprise computer system is included in the plurality of enterprise computer systems accessible to the user;

determine a security protocol for requesting the service from the enterprise computer system;

generate a security token corresponding to the determined security protocol for enterprise computer system, wherein the security token is generated based on the information indicating the security authentication of the user, and wherein the generated security token is included in the request sent to the enterprise computer system.

convert the request received from the mobile computing device, wherein the request is converted from a first format of a first communication protocol to a second format of a second communication protocol, wherein the second communication protocol is different from the first communication protocol;

send the converted request to the enterprise computer system;

receive, from the enterprise computer system via the second communication protocol, a response to the converted request for the service;

convert the response received from the enterprise computer system, wherein the response is converted from the second format of the second communication protocol to the first format of the first communication protocol; and

send the converted response to the mobile computing device.

17. The computer system of claim 16, wherein the enterprise computer system includes an on-premises agent system, wherein the on-premises agent system is associated with an on-premises local area network of an entity, wherein the on-premises agent system includes a plurality of server computers, each server computer providing a

different enterprise service, and wherein the on-premises agent system communicates with the computer system over the public communication network.

18. The computer system of claim 17, further comprising:

a firewall connected with the computer system, wherein an internal network and an external network are separated by the firewall, and wherein the firewall is configured to:

permit communication, conforming to the first communication protocol, between the mobile computing device and the computer system; and
permit communication, conforming to the second communication protocol, between the computer system and the on-premises agent system.

19. A cloud computer system to facilitate communication between a mobile computing device and an on-premises enterprise computer system, the cloud computer system comprising:

a cloud computer device configured to:

receive, through an application programming interface (API), from a mobile computing device, a message conforming to a first format of a first application protocol; and

generate and send, to the agent, a message conforming to a second format of a second application protocol;

a firewall connected with the cloud computer device, wherein an internal network and an external network are separated by the firewall, and wherein the firewall is configured to:

permit communication of messages, conforming to the first format of the first application protocol, between the mobile computing device and the cloud computing device; and

permit communication of messages, conforming to the second format of the second application protocol, between the cloud computer device and the agent;
and

a metadata repository connected with the cloud computer device, wherein the metadata repository is configured to store metadata for implementing the API, the implementing including translating between the first format and the second format, and

wherein the metadata repository is modifiable by an authenticated user via the external network.

20. The cloud computer system of claim 19, wherein the on-premises agent system includes a plurality of server computers, each server computer providing a different enterprise service, and wherein the on-premises agent system communicates with the computer system over the public communication network.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a cloud computer system, from a mobile computing device, a request for a service from an enterprise computer system, wherein the cloud computer system is located at a first geographical location that is different from a second geographical location of the enterprise computer system, and wherein the cloud computer system and the enterprise computer system communicate over a public communication network;

obtaining, by the cloud computer system, for a user of the mobile computing device associated with the request, a security authentication to obtain at least one service through the cloud computer system;

storing, by the cloud computer system, information indicating the security authentication;

identifying, based on the security authentication of the user, by the cloud computer system, a plurality of enterprise computer systems accessible to the user through the cloud computer system;

verifying, by the cloud computer system, that the enterprise computer system is included in the plurality of enterprise computer systems accessible to the user;

determining, by the cloud computer system, a security protocol for requesting the service from the enterprise computer system;

generating, by the cloud computer system, a security token corresponding to the determined security protocol for the enterprise computer system, wherein the security token is generated based on the information indicating the security authentication of the user; and

sending, by the cloud computer system, to the enterprise computer system, a request for the requested service, wherein the request includes the generated security token.

2. The method of claim 1, wherein at least one of the plurality of enterprise computer systems communicates using a different security protocol than a different one of the plurality of enterprise computer systems.

3. The method of claim 1 or 2, wherein the request received from the mobile computing device and the request sent to the enterprise computer system conform to different representational state transfer (REST) architectural styles.

4. The method of claim 1 or 2, wherein the request received from the mobile computing device includes a first hypertext transfer protocol (HTTP) message and wherein the request sent to the enterprise computer system includes a second HTTP message.

5. The method of any of claims 1 to 4, wherein the request received from the mobile computing device includes user identity information of the user.

6. The method of any of claims 1 to 5, further comprising:

sending an authentication request to an identity management system to determine the security authentication of the user.

7. The method of any of claims 1 to 6, wherein the security token is structured in a format using Security Assertion Markup Language (SAML).

8. The method of any of claims 1 to 7, wherein the plurality of enterprise computer systems includes the enterprise computer system having an on-premises agent system, wherein the on-premises agent system including a plurality of server computers, each server computer of the plurality of server computers providing a different enterprise service, and wherein the on-premises agent system communicates with the cloud computer system over the public communication network.

9. The method of any of claims 1 to 8, wherein the cloud computer system provides an application programming interface (API), the API using a first communication protocol to receive requests for services, wherein each enterprise computer system of the plurality of enterprise computer systems uses a second communication protocol to receive requests for services, and wherein the second communication protocol is different from the first communication protocol.

10. The method of claim 9, wherein the first communication protocol and the second communication protocol conform to a hypertext transfer protocol (HTTP).

11. The method of claim 9 or 10, wherein each enterprise computer system of the plurality of enterprise computer systems supports a different second communication protocol for receiving the requests for services.

12. The method of any of claims 9 to 11, wherein the API is configurable by the user of the mobile computing device.

13. The method of any of claims 9 to 12, wherein the cloud computer system includes a database that stores metadata corresponding to one or more configurations of the API.

14. The method of any of claims 9 to 13, further comprising:

converting the request from a format of the first communication protocol to a different format corresponding to the second communication protocol, wherein the converted request is sent to the enterprise computer system.

5 15. The method of any of claims 9 to 14, further comprising:

receiving, from the enterprise computer system, a response for the requested service, wherein the response has a format of the second communication protocol of the enterprise computer system;

10 converting the response from the format of the second communication protocol to a format of the first communication protocol; and

providing the converted response to the mobile computing device.

16. A computer system comprising:

one or more processors; and

15 one or more memory devices coupled to the one or more processors, the one or more memory devices containing instructions which when executed on the one or more processors, cause the one or more processors to:

20 receive, from a mobile computing device using a first communication protocol, a request for a service, wherein the service is provided by an enterprise computer system, wherein the enterprise computer system is located at a first geographical location that is different from a second geographical location of the computer system, and wherein the enterprise computer system and the computer system communicate over a public communication network;

obtain, for a user of the mobile computing device associated with the request, a security authentication to obtain at least one service via the computer system;

25 store information indicating the security authentication;

identify, based on the security authentication of the user, a plurality of enterprise computer systems accessible to the user through the cloud computer system;

verify that the enterprise computer system is included in the plurality of enterprise computer systems accessible to the user;

determine a security protocol for requesting the service from the enterprise computer system;

5 generate a security token corresponding to the determined security protocol for the enterprise computer system, wherein the security token is generated based on the information indicating the security authentication of the user, and wherein the generated security token is included in a request sent to the enterprise computer system;

10 convert the request received from the mobile computing device, wherein the request is converted from a first format of the first communication protocol to a second format of a second communication protocol, wherein the second communication protocol is different from the first communication protocol;

send the converted request to the enterprise computer system;

receive, from the enterprise computer system via the second communication protocol, a response to the converted request for the service;

15 convert the response received from the enterprise computer system, wherein the response is converted from the second format of the second communication protocol to the first format of the first communication protocol; and

send the converted response to the mobile computing device.

17. The computer system of claim 16, wherein the enterprise computer system includes an on-premises agent system, wherein the on-premises agent system is associated with an on-premises local area network of an entity, wherein the on-premises agent system includes a plurality of server computers, each server computer of the plurality of server computers providing a different enterprise service, and wherein the on-premises agent system communicates with the computer system over the public communication network.

18. The computer system of claim 17, further comprising:
25 a firewall connected with the computer system, wherein an internal network and an external network are separated by the firewall, and wherein the firewall is configured to:

permit communication, conforming to the first communication protocol, between the mobile computing device and the computer system; and

30 permit communication, conforming to the second communication protocol, between the computer system and the on-premises agent system.

19. (Currently Amended) A cloud computer system to facilitate communication between a mobile computing device and an on-premises enterprise computer system, the cloud computer system comprising:

a cloud computer device configured to:

5 receive, through an application programming interface (API), from a mobile computing device, a message conforming to a first format of a first application protocol; and

generate and send, to the an agent, a message conforming to a second format of a second application protocol;

10 a firewall connected with the cloud computer device, wherein an internal network and an external network are separated by the firewall, and wherein the firewall is configured to:

permit communication of messages, conforming to the first format of the first application protocol, between the mobile computing device and the cloud computer device; and

15 permit communication of messages, conforming to the second format of the second application protocol, between the cloud computer device and the agent; and

a metadata repository connected with the cloud computer device, wherein the metadata repository is configured to store metadata for implementing the API, the implementing including translating between the first format and the second format, and wherein the metadata repository is modifiable by an authenticated user via the external network.

20 20. (Currently Amended) The cloud computer system of claim 19, wherein the agent includes a plurality of server computers, each server computer of the plurality of server computers providing a different enterprise service, and wherein the agent communicates with the computer system over the public communication network.