

CLAIMS

1. A method of using access tokens for identification of breach attempts in a client-server communication, the method comprising:

receiving, by a token server system from a client device, a token generation request, the token generation request comprising at least two token configuration parameters defined by a user of the client device;

storing, by the token server system, the at least two token configuration parameters;

generating, by the token server system, a valid token in response to the token generation request;

transmitting, by the token server system to the client device, the valid token;

receiving, by the token server system, a token validation request for validation of a token from an Application Programming Interface (API) server, the token validation request comprising the token received by the API server from the client device in one or more API calls of an API session, the token comprising token parameters;

accessing, by the token server system, the at least two token configuration parameters associated with a valid token for the client, the at least two token configuration parameters comprising:

a number of allowable access attempts using the valid token in the API session, and
a range of frequency of allowable access attempts using the valid token in the API session;

comparing, by the token server system, the token parameters to the at least two token configuration parameters associated with the valid token;

determining, by the token server system, one of that a number of times the token validation request is received from the API server during the API session exceeds the number of allowable access attempts and that a frequency at which the token validation request is received from the API server during the API session exceeds the range of frequency of allowable access attempts; and

transmitting, by the token server system to the API server, validation information comprising a validation failure message indicating a breach attempt.

2. The method as claimed in claim 1, wherein the at least two token configuration parameters further comprise an allowed access pattern associated with the valid token.

3. The method as claimed in claim 2, wherein the allowed access pattern is determined based on historical access patterns of the valid token in a pre-defined time period.

4. A server system for using access tokens for identification of breach attempts in a client-server communication, the server system comprising:

a memory comprising stored instructions; and

a processor operably connected to the memory and configured to execute stored instructions which when executed cause the server system to perform:

receive from a client device, a token generation request, the token generation

request comprising at least two token configuration parameters defined by a user of the client device;

store the at least two token configuration parameters;

generate a valid token in response to the token generation request;

transmit the valid token to the client device;

receive a token validation request for validation of a token from an Application

Programming Interface (API) server, the token validation request comprising

the token received by the API server from the client device in one or more API calls of an API session, the token comprising token parameters;

access the at least two token configuration parameters associated with a valid token

for the client, the at least two token configuration parameters comprising:

a number of allowable access attempts using the token in the API session, and

a range of frequency of allowable access attempts using the token in the API session;

compare the token parameters to the at least two token configuration parameters associated with the valid token; and

determine one of that a number of times the token validation request is received from the API server during the API session exceeds the number of allowable access attempts and that a frequency at which the token validation request is received from the API server during the API session exceeds the range of frequency of allowable access attempts; and

transmit validation information to the API server, the validation information comprising a validation failure message indicating a breach attempt.

5. The server system as claimed in claim 4, wherein the token validation request comprises at least an information of:

a number of access attempts using the valid token during the API session; and
a frequency of access attempts using the valid token during the API session.

6. The server system as claimed in claim 4, wherein the at least two token configuration parameters further comprise an allowed access pattern associated with the valid token.

7. The server system as claimed in claim 6, wherein the allowed access pattern for the API session is determined based on historical access patterns of the valid token in a pre-defined time period.

8. A method of using access tokens for identification of breach attempts in a client-server communication, the method comprising:

receiving, by an Application Programming Interface (API) server, an API request for client-server communication, the API request comprising a token, the token received by the API server from a client device in one or more API calls of an API session;

sending, by the API server, a token validation request for validation of the token to a token server system; and

receiving verification information corresponding to whether the token conforms to at least two token configuration parameters from the token server system, wherein the at least two token configuration parameters are associated with a valid token generated by the token server upon receiving a token generation request from the client device and are defined by a user of the client device, wherein the at least two token configuration parameters comprise:

a number of allowable access attempts using the valid token in the API session,
a range of frequency of allowable access attempts using the valid token in the API

session, and
an allowed access pattern associated with the token, wherein the allowed access pattern is determined based on historical access patterns of the valid token in previous API sessions taken over a predefined time period.

9. The method of claim 2, further comprising, after comparing the token parameters to the at least two token configuration parameters associated with the valid token:

determining, by the token server system, that an access pattern does not comply with the allowed access pattern associated with the valid token; and
transmitting, by the token server system to the API server, validation information comprising a validation failure message indicating a breach attempt.

10. The server system as claimed in claim 6, wherein the memory stores further instructions causing the processor which when executed cause the server system to perform, after comparing the token parameters to the at least two token configuration parameters associated with the valid token:

determine that an access pattern does not comply with the allowed access pattern associated with the valid token; and
transmit validation information to the API server, wherein the validation information comprises a validation failure message indicating a breach attempt.