Claims

1. A computerized method for secure access control of an online form page, the method comprising:

receiving, from a user device, an access request to access the online form page, the access request sent by a browser application executed on the user device;

receiving, from the user device, browser data associated with the browser application;

verifying the browser data;

authorizing or denying the access request based on verification of the browser data; and

sending the online form page to the user device upon authorization of the access request;

wherein the browser data comprises a browser kernel of the browser application, and wherein the access request is authorized or denied based on verification of the browser kernel; and

wherein verification of the browser kernel comprises:

sending a browser type detection instruction to the user device, the browser type detection instruction predetermined based on the browser kernel; and

receiving, from the user device, a browser type detection result from execution of the browser type detection instruction by the browser application,

wherein the access request is authorized if the browser type detection result matches the browser kernel.

2. The method of claim 1, wherein the browser type detection instruction is configured to cause an exception in the browser kernel when the browser application executes the browser type detection instruction.

3. The method of claim 2, wherein the exception comprises a program execution statement error or a memory exception error.

4. The method of any one of claims 1 to 3, wherein the browser data comprises browser attributes of the browser application, and wherein the access request is authorized or denied based on verification of the browser attributes.

5. The method of claim 4, wherein the browser attributes comprise a user agent header of the browser application, and wherein the access request is denied if the user agent header comprises a keyword associated with headless browsers.

6. The method of claim 4 or 5, wherein the browser attributes comprise graphics data associated with rendering of graphics on the browser application, and wherein the access request is denied if the graphics data is empty.

7. The method of claim 6, wherein the graphics data comprises a web graphics library and/or graphics card details of a graphic card of the user device.

8. The method of any one of claims 4 to 7, wherein the browser attributes comprise a navigator interface property of the browser application, and wherein the access request is denied if the navigator interface property comprises a true value.

9. The method of any one of claims 4 to 8, wherein the browser attributes comprise a window size of the browser application, and wherein the access request is denied if the window size is zero.

10. The method of any one of claims 1 to 9, further comprising receiving, from the user device, a device display resolution of the user device and an available display resolution for loading the online form page on the browser application, wherein the access request is authorized or denied based additionally on the device display resolution and available display resolution.

11. The method of claim 10, wherein the access request is authorized if the device display resolution and available display resolution are different.

12. A computer system for secure access control of an online form page, the system comprising:

a communication module configured for:

receiving, from a user device, an access request to access the online form page, the access request sent by a browser application executed on the user device;

receiving, from the user device, browser data associated with the browser application, wherein the browser data comprises a browser kernel of the browser application;

sending the online form page to the user device upon authorization of the access request; and

a verification module configured for:

verifying the browser data; and

authorizing or denying the access request based on verification of the browser data, wherein the access request is authorized or denied based on verification of the browser kernel;

wherein verification of the browser kernel comprises:

sending a browser type detection instruction to the user device, the browser type detection instruction predetermined based on the browser kernel; and

receiving, from the user device, a browser type detection result from execution of the browser type detection instruction by the browser application,

wherein the access request is authorized if the browser type detection result matches the browser kernel.

13. A computerized method for secure access control of an online form page, the method comprising:

receiving, from a user device, an access request to access the online form page, the access request sent by a browser application executed on the user device;

receiving, from the user device, browser data associated with the browser application;

verifying the browser data;

authorizing or denying the access request based on verification of the browser data;

sending, upon authorization of the access request, the online form page to the user device for filling a form in the online form page;

wherein the browser data comprises a browser kernel of the browser application, and wherein the access request is authorized or denied based on verification of the browser kernel; and

wherein verification of the browser kernel comprises:

sending a browser type detection instruction to the user device, the browser type detection instruction predetermined based on the browser kernel; and

receiving, from the user device, a browser type detection result from execution of the browser type detection instruction by the browser application,

wherein the access request is authorized if the browser type detection result matches the browser kernel;

receiving, from the user device, a submission request to submit the filled form;

receiving, from the user device, temporal data associated with filling of the form;

verifying the temporal data;

authorizing or denying the submission request based on verification of the temporal data; and

submitting the filled form for further processing upon authorization of the submission request.

14. A computer system for secure access control of an online form page, the system comprising:

a communication module configured for:

receiving, from a user device, an access request to access the online form page, the request sent by a browser application executed on the user device; and

receiving, from the user device, browser data associated with the browser application, wherein the browser data comprises a browser kernel of the browser application;

sending, upon authorization of the access request, the online form page to the user device for filling a form in the online form page;

receiving, from the user device, a submission request to submit the filled form;

receiving, from the user device, temporal data associated with filling of the form; and

submitting the filled form for further processing upon authorization of the submission request; and

a verification module configured for:

verifying the browser data;

authorizing or denying the access request based on verification of the browser data, wherein the access request is authorized or denied based on verification of the browser kernel;

verifying the temporal data; and

authorizing or denying the submission request based on verification of the temporal data;

wherein verification of the browser kernel comprises:

sending a browser type detection instruction to the user device, the browser type detection instruction predetermined based on the browser kernel; and

receiving, from the user device, a browser type detection result from execution of the browser type detection instruction by the browser application,

wherein the access request is authorized if the browser type detection result matches the browser kernel.