CLAIMS

1. A method for user identification of a user device of a user based on a current user environment, the method being executable by a server including a processor communicatively couplable, via a communication network, with the user device of the user, the method comprising:

in response to receiving, from an application content server, an indication of launching a web application on the user device of the user, causing, by the processor, the user device to receive an analytical module for installation thereof in the web application of the user device, the analytical module being configured to execute:

causing installation of an iframe container in a given page of the web application;

retrieving, from the user device, user data indicative of the current user environment of the user device, the user data unambiguously identifying the user device;

generating, based on the user data, at least one cookie file;

transmitting, via the iframe container, the at least one cookie file to at least one identification server for modification thereof to generate an in-use cookie file; and

receiving, by the processor, the in-use cookie file;

analyzing, by the processor, the in-use cookie file for determining, based on the user data, a unique user device profile of the user device,

the determining including at least one of a global identification of the user device on a third-level domain and a local identification of the user device within a region on a fourth-level domain;

in response to determining that the unique user device profile is indicative of the user device being compromised, transmitting, by the processor, a predetermined notification to the application content server for taking respective measures in respect of further user interactions from the user device with the web application.

2. The method of claim 1, wherein the modification of the at least cookie file comprises adding a time stamp to the at least one cookie and further re-encryption thereof.

3. The method of claim 1, wherein the iframe container is installed in the given page outside of an authorized zone of the web application.

4. The method of claim 1, wherein the iframe container is configured for cross-domain exchange of cookie files.

5. The method of claim 1, wherein the at least one cookie file is further analyzed on a global data analysis server for generating a global identification profile of the current user environment of the user device.

6. The method of claim 1, wherein the global identification profile includes data indicative of at least one of: data of digital fingerprints of the web application, network features of the communication network, and user behavioral habits of the user.

7. The method of claim 6, wherein the data of the digital fingerprints of the web application includes information of at least one of: a User-Agent application on the user device, time of a system clock of an operating system installed on the user device, a CPU and a GPU of the user device, a monitor resolution and window size associated the web application, a list of fonts installed in the operating system, a list of all plugins installed in the operating system, and web application extensions in the web application.

8. The method of claim 6, wherein the data of the network features of the communication network includes at least one of: information of a local network architecture and information of settings of network protocols.

9. The method of claim 6, wherein the data of the user behavioral habits of the user include at least one of: a preferred interface language of the operating system, an operating system encoding and a time zone, data in a cache of the web application on the user device and log history thereof, mouse gestures, frequency and duration of keystrokes, data from an accelerometer of the user device, changes to standard fonts and sizes thereof of the web application, changes to a standard scale of the web application and/or elements thereof, use of special features including at least one of: text colors, size, data of settings of the web application including data of at least one of: blocking of third-party cookies, DNS prefetching, pop-up blocking, and Flash security settings.

10. The method of claim 1, wherein the analytical module is a Java Script module.

11. The method of claim 1, wherein the application content server is further configured to restrict the further user interactions from the user device with the web application.

12. A system for user identification of a user device of a user based on a current user environment, the system including a server further including:

a processor communicatively couplable, via a communication network, with a user device of the user;

a non-transitory computer-readable medium storing instructions; and

the processor, upon executing the instruction being configured to:

in response to receiving, from an application content server, an indication of launching a web application on the user device of the user, cause the user device to receive an analytical module for installation thereof in a web application of the user device, the analytical module being configured to execute:

causing installation of an iframe container in a given page of the web application;

retrieving, from the user device, user data indicative of the current user environment of the user device the user data unambiguously identifying the user device;

generating, based on the user data, at least one cookie file;

transmitting, via the iframe container, the at least one cookie file to at least one identification server for modification thereof to generate an in-use cookie file; and

receive the in-use cookie file;

analyze the in-use cookie file for determining, based on the user data, a unique user device profile of the user device,

the determining including at least one of a global identification of the user device on a third-level domain and a local identification of the user device within a region on a fourth-level domain;

in response to determining that the unique user device profile is indicative of the user device being compromised, transmit a predetermined notification to the application content server

for taking respective measures in respect of further user interactions from the user device with the web application.