CLAIMS

What is claimed, is:

1. A system for checking online user data for correctness and for using score models based on non-personal data of users to assess risks, the system comprising:

1) a data collecting means for collecting data from a user's client device and for sending the collected data to an indexing means, wherein the data to be collected include at least:

- the data of a user's online session at an online resource of a server;
- the data of the user's client device participating in data exchange with the server; and
- the data of user's activity on the client device;

2) an indexing means for calculating indexes based on the collected data and using pre-set indexation rules, and for sending the calculated indexes to a risk assessment means;

3) a risk assessment means for calculating the risks of a user accessing server resources, based on the calculated indexes, comprising:

- a system for searching for and evaluating stable markers of rare events, including an anti-fraud scoring system;
- a system for seamless identification and indexation linked to the details of user’s client device and user’s online behaviour; and
- a system for detecting and identifying stable identification markers or devices and user online behaviour, online makeup of markers, monitoring of marker stability, and online indexation of devices and users taking into account type 1 and type 2 errors; and

4) a right generating means for generating access rights for a user to access server resources, based on the calculated risks;

wherein the indexing means is further capable of assessing the completeness of the collected data, and, in case the collected data are not complete enough, generating a request for collecting additional data and sending it to the data collecting means, so that a minimum required amount of data is collected.

2. The system of claim 1, which has a client/server architecture, wherein the data collecting means operates on the client side, while the indexing means, the risk assessment means, and the right generating means operate on the side of at least one server.

3. The system of claim 1, wherein, in order to collect the user's data, the data collecting means is installed on the user's client device first, at the user's request.

4. The system of claim 1, wherein the risks of a user accessing server resources is a numerical value within a pre-defined range, where the lowest number reflects the maximum security of server resources when the given user interacts with them, and the highest number reflects the minimum security of server resources.

5. The system of claim 4, wherein the security of server resources means that there is a possibility that, at least:

- the credit money will not be returned within the first 90 days after the estimated maturity date;
- the loan payment will not be effected within the first 90 days after the first such payment has been scheduled;
- said resources will be compromised;
- said resources will be modified; or
- said resources will be accessed in an unauthorized fashion.

6. The system of claim 1, wherein the access rights for the user to access the server resources are represented by the user's registration on said server.

7. The system of claim 1, further comprising a log-in means for:

1) calculating indexes based on the collected data;

2) at the user's first request to the server for accessing its resources, calculating their indexes and bringing the results in line with the generated access rights for the user to access the server resources; and

3) at each of the user's subsequent request to the server for accessing its resources, using the previously generated access rights for the user to access the server resources, that correspond to the calculated indexes.

8. The system of any preceding claim, wherein the indexing means is configured to keep requesting new data from the data collecting means, at least until:

- the data completeness check returns a positive result,
- the amount of data stays within a pre-set range, or
- the number of requests to the data collecting means exceeds a pre-set number.

9. A method for checking online user data for correctness and for using score models based on non-personal data of users to assess risks, the method comprising the following steps performed by the means provided in the system of claim 1:

1) collecting data from a user’s client device, wherein the data to be collected include at least:

- the data of a user’s online session at an online resource of a server;

- the data of the user's client device participating in data exchange with the server; and
- the data of user's activity on the client device;

2) calculating indexes based on the collected data and using pre-set indexation rules;

3) based on the calculated indexes, calculating the risks of a user accessing server resources, comprising using:

- a system for searching for and evaluating stable markers of rare events, including an anti-fraud scoring system;
- a system for seamless identification and indexation linked to the details of user's client device and user's online behaviour; and
- a system for detecting and identifying stable identification markers or devices and user online behaviour, online makeup of markers, monitoring of marker stability, and online indexation of devices and users taking into account type 1 and type 2 errors; and

4) based on the calculated risks, generating access rights for a user to access server resources

wherein, after the index calculation step, the completeness of the collected data is further assessed, and, in case the collected data are not complete enough, a request for for collecting additional data is generated and and sent to the data collecting means, so that a minimum required amount of data is collected.

10. The method of claim 9, wherein, in order to collect the user's data, the data collecting means is installed on the user's client device first, at the user's request.

11. The method of claim 9, wherein the risks of a user accessing server resources is a numerical value within a pre-defined range, where the lowest number reflects the maximum security of server resources when the given user interacts with them, and the highest number reflects the minimum security of server resources.

12. The method of claim 9, wherein the security of server resources means that there is a possibility that, at least:

- the credit money will not be returned within the first 90 days after the estimated maturity date;
- the loan payment will not be effected within the first 90 days after the first such payment has been scheduled;
- said resources will be compromised;
- said resources will be modified; or
- said resources will be accessed in an unauthorized fashion.

13. The method of claim 9, wherein the access rights for the user to access the server resources are represented by the user’s registration on said server.

14. The method of claim 9, further comprising the following steps:

1) calculating indexes based on the collected online session data;
2) at the user's first request to the server for accessing its resources, calculating their indexes and bringing the results in line with the generated access rights for the user to access the server resources; and
3) at each of the user's subsequent request to the server for accessing its resources, using the previously generated access rights for the user to access the server resources, that correspond to the calculated indexes.