CLAIMS

1. A computer-implemented method for identifying a user of a mobile device, the method being executable by one or more server communicatively coupled with the mobile device, the method comprising:

receiving (i) user identification data of the user including: a user login and a user password associated with the user; and (ii) a device identifier of the mobile device;

transmitting executable instructions to the mobile device, thereby causing the mobile device to execute:

retrieving a list of sensors available on the mobile device;

selecting, from the list of sensors, at least one available sensor;

iteratively polling the at least one available sensor for generating sensed data for a given occurrence of a synchronization event, the sensed data being indicative of user interactions of the user with the mobile device,

the generating the sensed data for the given occurrence of the synchronization event comprising:

prior to the given occurrence of the synchronization event, recording, in a first stack within a memory of the mobile device, current readings from the at least one sensor;

in response to the given occurrence of the synchronization event:

ceasing to record the current readings from the at least one sensor in the first stack, thereby generating a first plurality of readings; and

continuing to record, in a second stack within the memory of the mobile device, further current readings from the at least one sensor; and

in response to receiving an indication the synchronization event having ended;

ceasing to record the further current readings in the second stack, thereby generating a second plurality of readings; and

continuing to record, in a third stack within the memory of the mobile device, yet further current readings from the at least one sensor, thereby generating a third plurality of readings;

combining the first, second, and third plurality of readings of the sensed data to generate a vector of behavioral parameters; and

transmitting the vector of behavioral parameters to the one or more server;

receiving the vector of behavioral parameters;

aggregating respective vectors of behavioral parameters associated with the user and generated by the at least one available sensor over other occurrences of the synchronization event into behavioral data;

clustering a given behavioral parameter within the behavioral data into a respective cluster of a plurality of clusters based on a respective interaction mode of a predetermined plurality of interaction modes of the user with the mobile device at a respective occurrence of the synchronization event, responsive to which the given behavioral parameter was generated;

training, based on behavioral parameters of the respective cluster, a given classifier to determine whether in-use user interactions with the mobile device are performed by the user or not; and

storing, in a database, the given classifier in association with the user identification data of the user, the device identifier of the mobile device, and the respective interaction mode associated with the given classifier for further use in detecting a suspicious activity on the mobile device.

2. The method of claim 1, wherein the at least one available sensor of the mobile device is one of:

an accelerometer;

a gyroscope; and

a gravity sensor.

3. The method of claim 1, wherein the synchronization event comprises the user tapping on a touchscreen of the mobile device.

4. The method of claim 1, wherein the synchronization event comprises one of opening a new window in an application interface, in which the user has input the user login and the user password.

5. The method of claim 1, the synchronization event comprises both of the user tapping on a touchscreen of the mobile device and opening a new window in an application interface, in which the user has input the user login and the user password.

6. The method of claim 1, wherein the generating the sensed data comprises:
retrieving first data sensed by the at least available sensor prior to a given occurrence of the synchronization event;

retrieving second data sensed by the at least available sensor prior during the given occurrence of the synchronization event; and

retrieving third data sensed by the at least available sensor after the given occurrence of the synchronization event.

7. The method of claim 1, wherein the vector of behavioral parameters includes one or more of:

a minimum value (min) of sensor readings of the at least one available sensor in an entirety of the sensed data;

a minimum value among amplitudes (amp.min) of the sensor readings in the entirety the sensed data;

a minimum value (minS) of the sensor readings of the at least one available sensor in the sensed data sensed prior to the given occurrence of the synchronization event;

a minimum value (minF) of the sensor readings of the at least one available sensor in the sensed data sensed after the given occurrence of the synchronization event;

a maximum value (maxS) of the sensor readings of the at least one available sensor in the sensed data sensed prior to the given occurrence of the synchronization event;

a maximum value among the amplitudes (amp.maxS) of the sensor readings of the at least one available sensor in the sensed data sensed prior to the given occurrence of the synchronization event;

a maximum value (maxA) of the sensor readings of the at least one available sensor in the sensed data sensed during the given occurrence of the synchronization event;

a maximum value among the amplitudes (amp.maxA) of the sensor readings of the at least one available sensor in the sensed data sensed during the given occurrence of the synchronization event;

a maximum value (maxF) of the sensor readings of the at least one available sensor in the sensed data sensed after the given occurrence of the synchronization event;

a maximum value among the amplitudes (amp.maxF) of the sensor readings of the at least one available sensor in the sensed data sensed after the given occurrence of the synchronization event;

a variance (var) of the sensor readings of the at least one available sensor in the entirety of the sensed data;

a variance of the amplitudes (amp.var) of the sensor readings the at least one available sensor in the entirety of the sensed data;

a standard deviation (std) of the sensor readings of the at least one available sensor in the entirety of the sensed data;

a standard deviation of the amplitudes (amp.std) of the at least one available sensor in the entirety of the sensed data;

an arithmetic mean (mean) of the sensor readings of the at least one available sensor in the entirety of the sensed data;

an arithmetic mean of the amplitudes (amp.mean) of the sensor readings the at least one available sensor in the entirety of the sensed data;

a median (median) of the sensor readings of the at least one available sensor in the entirety of the sensed data;

a median of the amplitudes (amp.median) of the sensor readings the at least one available sensor in the entirety of the sensed data;

a ratio between the maximum values of maxS and maxA;

a ratio between the maximum values of amp.maxS and amp.maxA;

a ratio between the maximum values of maxF and maxA;

a ratio between the maximum values of amp.maxF and amp.maxA;

a value of an oscillation parameter of the mobile device prior to the given occurrence of the synchronization event (diffS);

a value of the oscillation parameter of the mobile device after termination of the given occurrence of the synchronization event (diffF); and

a difference of the values of the oscillation parameter of the mobile device prior to and after the termination of the given occurrence of the synchronization event (ratioSF).

8. The method of claim 1, wherein the clustering the given behavioral parameter is further based on values of an arithmetic mean value (mean) of sensor readings of the at least one available sensor.

9. The method of claim 9, wherein the at least one available sensor is a gravity sensor of the mobile device.

10. The method of claim 10, wherein, prior to the clustering, the method further comprises determining an orientation of a screen of the mobile device as being one of portrait and landscape.

11. The method of claim 1, wherein the clustering the given behavioral parameter is further based on the values of a median (median) of the sensor readings of the at least one available sensor.

12. The method of claim 12, wherein the at least one available sensor is a gravity sensor of the mobile device.

13. The method of claim 13, wherein, prior to the clustering, the method further comprises determining an orientation of a screen of the mobile device as being one of portrait and landscape.

14. The method of claim 1, wherein the predetermined plurality of interaction modes of the user with the mobile device comprises: (i) a first interaction mode while the user is in a standing position, (ii) a second interaction mode while the user is in a lying position; and (iii) a third interaction mode while the suer is in a sitting position.

15. The method of claim 1, further comprising using the given classifier for identifying the user of the mobile device by analyzing a current activity thereon, the using comprising:

causing the mobile device to execute:

iteratively polling the at least one available sensor for generating in-use sensed data for a given in-use occurrence of the synchronization event, the in-use sensed data being indicative of current user interactions with the mobile device;

analyzing the in-use sensed data to generate an in-use vector of behavioral parameters; and

transmitting the in-use vector of behavioral parameters to the one or more server;

based on the in-use vector of behavioral parameters, determining, a current interaction mode of the predetermined plurality of interaction modes with the mobile device;

searching the database to identify a respective classifier corresponding to the current interaction mode with the mobile device;

in response to failing to identify the respective classifier corresponding to the current interaction mode:

determining the current activity on the mobile device as being suspicious; and

causing execution of remedial actions against the suspicious activity;

in response to identifying the respective classifier corresponding to the current interaction mode:

applying the respective classifier to the in-use vector of behavioral parameters to generate a likelihood value representative of a likelihood of the current activity being suspicious;

in response to the likelihood value being greater than a predetermined likelihood threshold:

determining the current activity on the mobile device as being suspicious; and

causing execution of the remedial actions against the suspicious activity.

16. A system for identifying a user of a mobile device, the system comprising a server communicatively coupled with the mobile device, the server comprising at least one processor and at least one non-transitory computer-readable memory storing executable instructions, which, when executed by the at least one processor, cause the system to:

receive (i) user identification data of the user including: a user login and a user password associated with the user; and (ii) a device identifier of the mobile device;

transmit executable instructions to the mobile device, thereby causing the mobile device to execute:

retrieving a list of sensors available on the mobile device;

selecting, from the list of sensors, at least one available sensor;

iteratively polling the at least one available sensor for generating sensed data for a given occurrence of a synchronization event, the sensed data being indicative of user interactions of the user with the mobile device,

the generating the sensed data for the given occurrence of the synchronization event comprising:

prior to the given occurrence of the synchronization event, recording, in a first stack within a memory of the mobile device, current reading from the at least one sensor;

in response to the given occurrence of the synchronization event:

ceasing to record the current readings from the at least one sensor in the first stack, thereby generating a first plurality of readings; and

continuing to record, in a second stack within the memory of the mobile device, further current readings from the at least one sensor; and

in response to receiving an indication the synchronization event having ended:

ceasing to record the further current readings in the second stack, thereby generating a second plurality of readings; and

continuing to record, in a third stack within the memory of the mobile device, yet further current readings from the at least one sensor, thereby generating a third plurality of readings;

combining the first, second, and third plurality of readings of the sensed data to generate a vector of behavioral parameters; and

transmitting the vector of behavioral parameters to the one or more server;

receive the vector of behavioral parameters;

aggregate respective vectors of behavioral parameters associated with the user and generated by the at least one available sensor over other occurrences of the synchronization event into behavioral data;

cluster a given behavioral parameter within the behavioral data into a respective cluster of a plurality of clusters based on a respective interaction mode of a predetermined plurality of interaction modes of the user with the mobile device at a respective occurrence of the synchronization event, responsive to which the given behavioral parameter was generated;

train, based on behavioral parameters of the respective cluster, a given classifier to determine whether in-use user interactions with the mobile device are performed by the user or not; and

store, in a database, the given classifier in association with the user identification data of the user, the device identifier of the mobile device, and the respective interaction mode associated with the given classifier for further use in detecting a suspicious activity on the mobile device.