

CLAIMS

What is claimed is:

1. A system for utilizing behavioral features to authenticate a user entering login credentials, the system comprising
an electronic processor, the electronic processor configured to
receive a request to access a user account, the request including behavioral features;
compare the behavioral features included in the request to behavioral features included in a user behavior profile associated with the user account, the behavioral features included in the user behavior profile include behavioral features associated with one or more previous requests to access the user account;
based on the comparison, generate one or more scores including at least one selected from the group comprising a recency score, a frequency score, a novelty score, and a temporality score;
for each of the one or more scores,
compare the score to a predetermined threshold; and
based on the comparison of the score to the predetermined threshold, adjust a match value; and
compare the match value to one or more predetermined thresholds to determine whether the behavioral features included in the request to access the user account authenticates the user, does not authenticate the user, or is inconclusive.
2. The system according to claim 1, wherein the behavioral features include at least one selected from the group comprising a geolocation, an IP address, a UDID, a DID, a device fingerprint, a web browser, a user agent, an email domain, an ISP, an operating system version, and a time stamp.
3. The system according to claim 1, wherein the request includes biometric data in addition to the behavioral features and the electronic processor is configured to utilize the behavioral features to authenticate the user when the biometric data is insufficient to authenticate the user.
4. The system according to claim 3, wherein the electronic processor is configured to determine a reason that there is insufficient biometric data to authenticate the user; and

depending on the reason for the insufficient amount of biometric data, determine which behavioral features to analyze to determine the one or more scores and determine one or more predetermined thresholds to compare the one or more scores, match value, or both to.

5. The system according to claim 1, wherein the electronic processor is configured to generate the frequency score based on whether one or more of the behavioral features included in the request are, based on behavioral features included in the user behavior profile, frequently associated with requests to access the user account.

6. The system according to claim 1, wherein the electronic processor is configured to generate the novelty score based on whether one or more of the behavioral features included in the request do not match a behavioral feature included in the user behavior profile.

7. The system according to claim 1, wherein the electronic processor is configured to generate the recency score based on whether one or more of the behavioral features included in the request match a behavioral feature included in the user behavior profile and associated with one or more most previous requests to access the user account.

8. The system according to claim 1, wherein the electronic processor is configured to generate a first temporality score based on whether a time and a date associated with the request is similar to a date and a time that one or more most previous requests are associated with.

9. The system according to claim 1, wherein the electronic processor is configured to generate a second temporality score based on whether time elapsed between a time associated with the request and a most previous request to access the user account is within one standard deviation of an average time elapsed between previously received consecutive requests to access the user account.

10. The system according to claim 1, wherein the electronic processor is configured to generate a velocity score based on whether at least a predetermined number of requests to access the user account associated with the same behavioral feature are received during a predetermined time period.

11. A method for utilizing behavioral features to authenticate a user entering login credentials, the method comprising

receiving a request to access a user account, the request including behavioral features;

comparing the behavioral features included in the request to behavioral features included in a user behavior profile associated with the user account, the behavioral features included in the user behavior profile include behavioral features associated with one or more previous requests to access the user account;

based on the comparison, generating one or more scores including at least one selected from the group comprising a recency score, a frequency score, a novelty score, and a temporality score;

for each of the one or more scores,

comparing the score to a predetermined threshold; and

based on the comparison of the score to the predetermined threshold, adjusting a match value; and

comparing the match value to one or more predetermined thresholds to determine whether the behavioral features included in the request to access the user account authenticates the user, does not authenticate the user, or is inconclusive.

12. The method according to claim 11, wherein the behavioral features include at least one selected from the group comprising a geolocation, an IP address, a UDID, a DID, a device fingerprint, a web browser, a user agent, an email domain, an ISP, an operating system version, and a time stamp.

13. The method according to claim 11, wherein the request includes biometric data in addition to the behavioral features and the method further comprising utilizing the behavioral features to authenticate the user when the biometric data is insufficient to authenticate the user.

14. The method according to claim 11, the method further comprising generating the frequency score based on whether one or more of the behavioral features included in the request are, based on behavioral features included in the user behavior profile, frequently associated with requests to access the user account.

15. The method according to claim 11, the method further comprising generating the novelty score based on whether one or more of the behavioral features included in the request do not match a behavioral feature included in the user behavior profile.

16. The method according to claim 11, the method further comprising generating the recency score based on whether one or more of the behavioral features included in the request

match a behavioral feature included in the user behavior profile and associated with one or more most previous requests to access the user account.

17. The method according to claim 11, the method further comprising generating a first temporality score based on whether a time and a date associated with the request is similar to a date and a time that one or more most previous requests are associated with.

18. The method according to claim 11, the method further comprising generating a second temporality score based on whether time elapsed between a time associated with the request and a most previous request to access the user account is within one standard deviation of an average time elapsed between previously received consecutive requests to access the user account.

19. A non-transitory computer-readable medium with computer-executable instructions stored thereon that are executed by an electronic processor to perform a method of utilizing behavioral features to authenticate a user entering login credentials, comprising: receiving a request to access a user account, the request including behavioral features;

comparing the behavioral features included in the request to behavioral features included in a user behavior profile associated with the user account, the behavioral features included in a user behavior profile include behavioral features associated with one or more previous requests to access the user account;

based on the comparison, generating one or more scores including at least one selected from the group comprising a recency score, a frequency score, a novelty score, and a temporality score;

for each of the one or more scores,

comparing the score to a predetermined threshold; and

based on the comparison of the score to the predetermined threshold, adjusting a match value; and

comparing the match value to one or more predetermined thresholds to determine whether the behavioral features included in the request to access the user account authenticates the user, does not authenticate the user, or is inconclusive.

20. The non-transitory computer-readable medium according to claim 19, wherein the behavioral features include at least one selected from the group comprising a geolocation, an

IP address, a UDID, a DID, a device fingerprint, a web browser, a user agent, an email domain, an ISP, an operating system version, and a time stamp.