WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

receiving, by a server computer, an authentication request comprising an application identifier associated with an application or a user device identifier associated with a user device, the authentication request originating from the user device;

receiving, by the server computer, a set of behavioral data associated with the application or the user device;

responsive to receiving the application identifier or device identifier, obtaining, by the server computer, a fuzzy vault associated with the application identifier or the user device identifier; and

determining, by the server computer, a reconstructed key value using the fuzzy vault and the set of behavioral data,

wherein the application or the user device is authenticated using the reconstructed key value, wherein the set of behavioral data is a first set of behavioral data, and wherein the method further comprises an enrollment process, the enrollment process including:

receiving, by the server computer, an enrollment request comprising the application identifier or the user device identifier and an enrollment key value;

receiving, by the server computer, a second set of behavioral data associated with the user device or the application;

forming, by the server computer, a polynomial using the enrollment key value, wherein one or more portions of the enrollment key value form coefficients of the polynomial;

determining, by the server computer, a set of genuine points by inputting the second set of behavioral data into the polynomial; and

forming the fuzzy vault using the set of genuine points and random chaff points, wherein the fuzzy vault comprises the set of genuine points and the random chaff points on a graph.

2. The method of claim 1, wherein the server computer is a fuzzy extractor server computer and wherein the fuzzy vault is stored in an authentication server computer, and the method further comprises:

generating, by the fuzzy extractor server computer, a hash of the reconstructed key value; and

transmitting, by the fuzzy extractor server computer, the hash of the reconstructed key value and the application identifier or the user device identifier to the authentication server computer, wherein the authentication server computer verifies the hash of the reconstructed key value with a hash of an enrollment key value, and wherein the authentication server computer notifies the user device that the user device or the application is authenticated.

3. The method of claim 1, wherein the set of behavioral data is obtained from a plurality of sensors in communication with or within the user device.

4. The method of claim 1, wherein the set of behavioral data includes one or more of: CPU consumption by the application or the user device, memory consumption by the application or the user device, a number of successful communications with the application or the user device, a number of files accessed by the application or the user device, a number of system calls performed by the application or the user device, an average response time of the application or the user device, a number of packets sent by the application or the user device, or a number of packets received by the application or the user device.

5. The method of claim 1, wherein the server computer is a fuzzy extractor server computer and wherein the fuzzy vault is stored in an authentication server computer, and the fuzzy extractor server computer receives the authentication request from the user device via the authentication server computer.

6. The method of claim 1, wherein determining, by the server computer, the reconstructed key value using the fuzzy vault and the set of behavioral data comprises:

using the behavioral data to identify a candidate set of points in the fuzzy vault;

forming a polynomial with the candidate set of points; and

determining the reconstructed key value using coefficients of the polynomial.

7. The method of claim 6, wherein the behavioral data includes a plurality of feature values, and using the behavioral data to identify the candidate set of points in the fuzzy vault comprises:

for each feature value of the plurality of feature values, comparing the feature value to a fuzzy vault value corresponding to a point in the fuzzy vault; and

selecting, as one of the candidate set of points, the point in the fuzzy vault if the fuzzy vault value is within a predetermined threshold of the one of the feature value.

8. The method of claim 1, further comprising:

transmitting the fuzzy vault to the user device, wherein the user device stores the fuzzy vault.

9. The method of claim 1, further comprising:

deleting, by the server computer, the enrollment key value after forming the fuzzy vault.

10. The method of claim 1, wherein the application or the user device is granted access to a computing service based on the authentication.

11. The method of claim 1, wherein the set of behavioral data comprises time series data, the method further comprising:

computing a statistical value based on the time series data for at least a subset of the behavioral data, wherein the statistical value is used to determine the reconstructed key value.

12. The method of claim 1, wherein the set of behavioral data comprises a plurality of feature values, the method further comprising:

computing a normalized value for each of the feature values; and

generating a binary feature vector based on the normalized values, wherein the binary feature vector is used to determine the reconstructed key value.

13. A server computer comprising:

a processor; and

a non-transitory computer-readable medium comprising code, executable by the processor, for implementing operations comprising:

receiving an authentication request comprising an application identifier associated with an application or a user device identifier associated with a user device, the authentication request originating from the user device;

receiving a set of behavioral data associated with the application or the user device;

responsive to receiving the application identifier or device identifier, obtaining a fuzzy vault associated with the application identifier or the user device identifier; and

determining a reconstructed key value using the fuzzy vault and the set of behavioral data,

wherein the application or the user device is authenticated using the reconstructed key value, wherein the set of behavioral data is a first set of behavioral data, and wherein the operations further comprise an enrollment process, the enrollment process including:

receiving, by the server computer, an enrollment request comprising the application identifier or the user device identifier and an enrollment key value;

receiving, by the server computer, a second set of behavioral data associated with the user device or the application;

forming, by the server computer, a polynomial using the enrollment key value, wherein one or more portions of the enrollment key value form coefficients of the polynomial;

determining, by the server computer, a set of genuine points by inputting the second set of behavioral data into the polynomial; and

forming the fuzzy vault using the set of genuine points and random chaff points, wherein the fuzzy vault comprises the set of genuine points and the random chaff points on a graph.

14. The server computer of claim 13, wherein:

the set of behavioral data is obtained from a plurality of sensors in communication with or within the user device; and

the set of behavioral data includes one or more of: CPU consumption by the application or the user device, memory consumption by the application or the user device, a number of successful communications with the application or the user device, a number of files accessed by the application or the user device, a number of system calls performed by the application or the user device, an average response time of the application or the user device, a number of packets sent by the application or the user device, or a number of packets received by the application or the user device.

15. The server computer of claim 13, wherein determining the reconstructed key value using the fuzzy vault and the set of behavioral data comprises:

using the behavioral data to identify a candidate set of points in the fuzzy vault;

forming a polynomial with the candidate set of points; and

determining the reconstructed key value using coefficients of the polynomial.

16. A computer-implemented method comprising:

transmitting, by an authentication server computer to a fuzzy extractor server computer, an authentication request for an application or a user device comprising an application identifier or a user device identifier, the authentication request originating from the user device,

thereby causing computation of a reconstructed key value by the fuzzy extractor server computer using a fuzzy vault associated with the application identifier or the user device identifier and a set of behavioral data associated with the application or the user device;

receiving the reconstructed key value or a hash of the reconstructed key value; and

authenticating, by the authentication server computer, the application or the user device with the reconstructed key value or the hash of the reconstructed key value,

wherein the set of behavioral data is a first set of behavioral data, and wherein an enrollment process is performed by the fuzzy extractor server computer, the enrollment process comprising:

receiving an enrollment request comprising the application identifier or the user device identifier and an enrollment key value,

receiving a second set of behavioral data associated with the user device or the application,

forming a polynomial using the enrollment key value, wherein one or more portions of the enrollment key value form coefficients of the polynomial,

determining a set of genuine points by inputting the second set of behavioral data into the polynomial, and

forming the fuzzy vault using the set of genuine points and random chaff points, wherein the fuzzy vault comprises the set of genuine points and the random chaff points on a graph.

17. The method of claim 16, wherein authenticating the application or the user device comprises:

comparing, by the authentication server computer, the hash of the reconstructed key value to a stored hashed key; and

determining, by the authentication server computer, that the hash of the reconstructed key value matches the stored hashed key.

18. The method of claim 16, wherein:

the set of behavioral data is obtained from a plurality of sensors in communication with or within the user device; and

the set of behavioral data includes one or more of: CPU consumption by the application or the user device, memory consumption by the application or the user device, a number of successful communications with the application or the user device, a number of files accessed by the application or the user device, a number of

system calls performed by the application or the user device, an average response time of the application or the user device, a number of packets sent by the application or the user device, or a number of packets received by the application or the user device.