WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a server computer from a first client device, a service request comprising one or more first data elements, wherein the one or more first data elements include a first user identifier;

hashing, by the server computer, the one or more first data elements to form a first hash using a hash function;

generating, by the server computer, a first one-time password;

storing, by the server computer, the first one-time password in association with the first hash;

transmitting, by the server computer, the first one-time password to the first client device or a second client device;

receiving, by the server computer from the first client device or the second client device, a second one-time password and one or more second data elements, wherein the one or more second data elements include a second user identifier;

hashing, by the server computer, the one or more second data elements to form a second hash using the hash function;

determining, by the server computer, the first one-time password using the second hash;

comparing, by the server computer, the first one-time password to the second one-time password; and

based on comparing the first one-time password to the second one-time password, providing, by the server computer, a service associated with the service request to the first client device.

2. The method of claim 1, wherein the one or more first data elements includes one or more first dynamic data elements including a first counter, and wherein the one or more second data elements includes one or more second dynamic data elements including a second counter.

3. The method of claim 1, wherein the hash function comprises an MD hash function, an SHA hash function, a BLAKE hash function, an MAC based hash function, or a CRC based hash function.

4. The method of claim 1, wherein the first one-time password comprises an alphanumeric string, and wherein generating the first one-time password comprises randomly generating, by the server computer, the alphanumeric string.

5. The method of claim 1, wherein:

prior to hashing the one or more first data elements, the method further comprises combining, by the server computer, the one or more first data elements, thereby generating a first combination, wherein hashing the one or more first data elements comprises hashing the first combination; and

prior to hashing the one or more second data elements, the method further comprises combining, by the server computer, the one or more second data elements, thereby generating a second combination, wherein hashing the one or more second data elements comprises hashing the second combination.

6. The method of claim 5, wherein:

combining the one or more first data elements comprises concatenating, by the server computer, the one or more first data elements; and

combining the one or more second data elements comprises concatenating, by the server computer, the one or more second data elements.

7. The method of claim 1, wherein storing the first one-time password in association with the first hash comprises storing, by the server computer, a one-time password record in a key-value table, wherein the first one-time password comprises a value associated with the one-time password record and the first hash comprises a key associated with the one-time password record.

8. The method of claim 7, wherein determining the first one-time password using the second hash comprises:

identifying, by the server computer, the one-time password record using the second hash as a key; and

determining, by the server computer, the first one-time password using the one-time password record.

9. The method of claim 1, wherein the one or more first data elements include a first intent identifier associated with the service request and wherein the one or more second data elements include a second intent identifier associated with the service request.

10. The method of claim 9, wherein the method further comprises determining, by the server computer, an intent based on the first intent identifier, and wherein the server computer generates the first one-time password based on the first intent identifier.

11. The method of claim 9, wherein the one or more first data elements and the one or more second data elements are the same.

12. The method of claim 9, wherein the first user identifier and/or the second user identifier comprises one or more of the following:

a username;

an account identifier;

a user email address;

a user phone number;

a cookie; or

a biometric.

13. The method of claim 9, wherein the first intent identifier and/or the second intent identifier comprises one or more of the following:

a user registration intent identifier;

a password recovery intent identifier;

a contact update intent identifier;

a login intent identifier; or

a privileged service intent identifier.

14. A server computer comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, the non-transitory computer readable medium comprising code or instructions, executable by the processor for performing a method according to any of the preceding claims.

15. A method comprising:

transmitting, by a client device to a server computer, a service request comprising one or more data elements, wherein the one or more data elements include a user identifier, wherein the server computer forms a first hash using a hash function and the one or more data elements, wherein the server computer generates a one-time password, and wherein the server computer stores the one-time password in association with the first hash;

receiving, by the client device from the server computer, the one-time password;

transmitting, by the client device to the server computer, the one-time password and the one or more data elements, wherein the server computer forms a second hash using the hash function and the one or more data elements, wherein the server computer determines a stored one-time password using the second hash, and wherein the server computer compares the stored one-time password to the one-time password; and

receiving, by the client device, a service provided by the server computer and corresponding to the service request, wherein the server computer provides the service to the client device based on comparing the stored one-time password to the one-time password.