CLAIMS

What is claimed is:

1. A method, comprising:

receiving, by a server system associated with a payment network, a payment transaction request for a payment transaction by a payment card of a user, the payment transaction request comprising information of the payment card;

upon receiving the payment transaction request, facilitating, by the server system, a selection of an authentication option from a plurality of authentication options presented to the user on an interface related to enabling payment and authorization using the payment card, the plurality of authentication options presented for authenticating the payment transaction associated with the payment transaction request;

upon receiving the selection of the authentication option, dynamically adapting, by the server system, a timeout period of an authentication session for authenticating the payment transaction based on the selection of the authentication option; and

terminating, by the server system, the authentication session upon expiry of the timeout period,

wherein the timeout period is dynamically adapted based on a plurality of timers, each timer of the plurality of timers being associated with one or more authentication options of the plurality of authentication options, and

wherein the dynamically adapting the timeout period comprises:

accessing, by the server system, a first timer among the plurality of timers associated with the authentication option and a second timer among the plurality of timers associated with an alternate authentication option;

accessing, by the server system, a predefined rule among a set of predefined rules corresponding to overriding the authentication option; and

adapting, by the server system, the timeout period based on at least one from among the first timer, the second timer and the predefined rule for overriding.

2. The method as claimed in claim 1, further comprising:

receiving, by the server system, a user preference input for configuring the plurality of timers; and

storing, by the server system, the user preference input.

3. The method as claimed in claim 1, wherein the dynamically adapting the timeout period comprises:

determining, by the server system, the timeout period based at least on the set of predefined rules, the set of predefined rules defined based on one or more timers of the plurality of timers; and

facilitating, by the server system, display of the timeout period on the interface.

4. The method as claimed in claim 3, further comprising:

determining, by the server system, the timeout period for the payment transaction based at least one on a plurality of usage analytics data, the plurality of usage analytics data including one or more of a type of a user device and web browser information.

5. The method as claimed in claim 3, further comprising:

accessing, by the server system, a user profile information of the user, the user profile information comprising a historical authentication time for authenticating a set of historical payment transactions based on the authentication option; and

determining, by the server system, the timeout period for the payment transaction based at least on the authentication option, the set of predefined rules and the user profile information.

6. The method as claimed in claim 3, further comprising:

receiving, by the server system, the alternate authentication option from the user for authenticating the payment transaction by overriding the authentication option selected prior by the user, the alternate authentication option selected from a remainder of the plurality of authentication options.

7. The method as claimed in claim 1, further comprising:

receiving, by the server system, a plurality of usage analytics data associated with the user from a merchant interface, the plurality of usage analytics data comprising one or more of:

a type of a user device, and

a web browser information.

8. The method as claimed in claim 1, wherein the plurality of authentication options is at least one of:

a One-Time Password (OTP) option;
a Quick Response (QR) code option;
a static password option; and
a biometric-based password option.

9. A server system, comprising:
a memory comprising executable instructions; and
a processor communicably configured to execute the instructions to cause the server system to at least perform
receiving a payment transaction request from a merchant interface for a payment transaction by a payment card of a user, the payment transaction request comprising information of the payment card,
upon receiving the payment transaction request, facilitating a selection of an authentication option from a plurality of authentication options presented to the user on an interface related to enabling payment and authorization using the payment card, the plurality of authentication options presented for authenticating the payment transaction associated with the payment transaction request;
upon receiving the authentication option, dynamically adapting a timeout period of an authentication session for authenticating the payment transaction based on the authentication option; and
terminating the authentication session upon expiry of the timeout period,
wherein the timeout period is dynamically adapted based on a plurality of timers, each timer of the plurality of timers being associated with one or more authentication options of the plurality of authentication options, and
wherein the dynamically adapting the timeout period comprises:
accessing a first timer among the plurality of timers associated with the authentication option and a second timer among the plurality of timers associated with an alternate authentication option;
accessing a predefined rule among a set of predefined rules corresponding to overriding

the authentication option; and

adapting the timeout period based on the first timer, the second timer and the predefined rule for overriding.

10. The server system as claimed in claim 9, wherein the server system is further configured to perform:

accessing a user profile information of the user, the user profile information comprising a historical authentication time for authenticating a set of historical payment transactions based on the authentication option; and

determining the timeout period for authenticating the payment transaction based at least on the authentication option, a timer associated with the authentication option and the historical authentication time.

11. The server system as claimed in claim 9, wherein the plurality of authentication options is at least one of:

a One-Time Password (OTP) option;

a Quick Response (QR) code option;

a static password option; and

a biometric-based password option.

12. A method for dynamically adapting a timeout period of a payment transaction, the method comprising:

receiving, by a server system associated with a payment network, a payment transaction request initiated from a merchant interface for the payment transaction by a payment card of a user, the payment transaction request comprising a payment card information of the payment card of the user;

upon receiving the payment transaction request, provisioning, by the server system, a plurality of authentication options for the user to authenticate the payment transaction on an interface related to enabling payment and authorization using the payment card, the plurality of authentication options comprising a one-time password (OTP) option and a static password option;

receiving, by the server system, a selection of an authentication option among the plurality of options from the user;

adapting, by the server system, the timeout period of an authentication session for authenticating the payment transaction based on the selection of the authentication option and one or more of a set of predefined rules, a plurality of usage analytics data, and a user profile information, the plurality of usage analytics data including one or more of a type of a user device and web browser information; and

terminating, by the server system, the authentication session upon expiry of the timeout period.

13. The method as claimed in claim 12, wherein the plurality of authentication options further comprises:

a Quick Response (QR) code option; and

a biometric-based password option.

14. The method as claimed in claim 12, wherein the user profile information comprises a historical authentication time for authenticating historical payment transactions based on the authentication option.