CLAIMS

We Claim:

1. A computer-implemented method for authentication of an Internet-of-Things (IoT) device, comprising:

receiving, by a proxy application executing on a mobile device during a registration process, a device identifier associated with the IoT device, the device identifier entered into the proxy application by a user of the mobile device;

transmitting, by the proxy application, the device identifier to a router of a wireless network as part of the registration process, wherein the registration process establishes an association between the device identifier and the proxy application for enabling proxy authentication of the IoT device;

subsequent to the registration process, receiving by the proxy application, the device identifier from the router in response to the router receiving an authorization request comprising the device identifier with no network password from the IoT device for access to the wireless network, and the router forwarding the device identifier to the proxy application based on the established association after determining that the router has proxy authentication enabled;

prompting the user of the mobile device to enter the network password, and transmitting the entered network password in a message to the router, such that in response to the router validating the network password and granting the IoT device access to the wireless network, the IoT device transmits the device identifier to the router for subsequent network connection without a need for the mobile device or the proxy application.

2. The method of claim 1, wherein the registration phase further comprises: associating, by the proxy application, the device identifier with an application identifier used to identify the proxy application.

3. The computer-implemented method of claim 2, wherein the registration phase further comprises: registering, by the proxy application, a mapping of the device identifier to the application identifier as an identifier pair with the router.

4. The computer-implemented method of claim 3, wherein the registration phase further comprises: sending, by the proxy application, the identifier pair to the router such that the router stores the identifier pair in a credential management system or forwards the identifier pair to an authentication mapper server.

5. The computer-implemented method of claim 2, further comprising: separating functionality of the proxy application into a first proxy application and a second proxy application, wherein during the registration phase, the first proxy application and the second proxy application register as an application pair with an authentication mapper server.

6. The computer-implemented method of claim 5, further comprising: configuring the authentication mapper server to communicate request and responses for the first proxy application and the second proxy application.

7. The computer-implemented method of claim 6, further comprising: configuring the first proxy application to receive from the router the device identifier of the IoT device and determine if the IoT device has been enabled for proxy authentication by forwarding the device identifier to the authentication mapper server to validate the device identifier.

8. The computer-implemented method of claim 6, further comprising: configuring the second proxy application to prompt the user of the mobile device to enter the network password in response to receiving a validation message from the authentication mapper server, and transmit the entered network password in the message to the router through the authentication mapper server and the first proxy application.

9. The computer-implemented method of claim 1, further comprising: implementing the proxy application as a first proxy application associated with a first application identifier and a second proxy application associated with a second application identifier, wherein the first application identifier and the second application identifier include a mobile phone number of the mobile device.

10. The computer-implemented method of claim 9, further comprising:

registering a mapping between the first application identifier and the network password with a router mapper system; and

registering the second application identifier with an authentication mapper server.

11. The computer-implemented method of claim 1, wherein receiving, by the proxy application, the device identifier associated with the IoT device further comprises: automatically determining, by the IoT device, which one of a plurality of detected wireless networks to request access to by selecting the wireless network having a highest signal strength.

12. A computer-implemented method for authentication of an IoT device, comprising:

receiving, by a router, a registration request from a proxy application executing on a mobile device, the registration request including a device identifier associated with the IoT device, the device identifier entered into the proxy application by a user of the mobile device, the router further storing the device identifier and enabling a proxy authentication setting, wherein the registration request establishes an association between the device identifier and the proxy application for enabling proxy authentication of the IoT device;

receiving, by the router, an authorization request from the IoT device for access to a wireless network, the authorization request comprising at least the device identifier without a network password;

determining, by the router, if a proxy authentication setting is enabled, and if so forwarding the device identifier to the proxy application based on the established association between the device identifier and the proxy application;

receiving, by the router, a message from the proxy application, a message including a network password entered into the proxy application by the user; and

responsive to the router validating the network password, granting the IoT device access to the wireless network, the IoT device to transmit the device identifier to the router for subsequent connection without a need for the mobile device or the proxy application.

13. The computer-implemented method of claim 12, further comprising: storing, by the router, the device identifier in a credential management system.

14. The computer-implemented method of claim 13, wherein receiving the message from the proxy application with a network password entered by the user further comprises: sending, by the router, a validation request to the credential

management system, which validates the network password if a match for the network password is found.

15. The computer-implemented method of claim 12, further comprising: in response to determining that proxy authentication setting is not enabled, sending, by the router, a denial message to the IoT device.

16. The computer-implemented method of claim 12, further comprising: responsive to the IoT device being disconnected from the wireless network, receiving, by the router, the device ID from the IoT device; looking up the device ID and if found, reestablishing network connection with the IoT device without any input from the user or the mobile device.

17. The computer-implemented method of claim 12, wherein receiving, by the router, the authorization request from the IoT device further comprises: automatically determining, by the IoT device, which one of a plurality of detected wireless networks to request access to by selecting the wireless network having a highest signal strength.

18. The computer-implemented method of claim 13, further comprising: in response to the IoT device failing to receive a reply to the authorization request within a predetermined time threshold, sending, by the IoT device, an authentication request to a router of another wireless network having a next highest signal strength until the IoT device finds the router with proxy authentication enabled.

19. A system, comprising:

a router that provides a wireless network and communicates over the wireless network and an Internet;

an Internet-of-Things (IoT) device requiring first time access to the wireless network, the IoT device associated with a device identifier; and

a proxy application executing on a mobile device of a user, the proxy application to act a proxy for the IoT device during a first network authentication attempt with the router, the proxy application configured to:

receive during a registration process, the device identifier associated with the IoT device, the device identifier entered into the proxy application by the user of the mobile device;

transmit the device identifier to the router as part of the registration process, wherein the registration process establishes an association between the device identifier and the proxy application for enabling proxy authentication of the IoT device;

subsequent to the registration process, receive by the proxy application, the device identifier from the router in response to the router receiving an authorization request comprising the device identifier with no network password from the IoT device for access to the wireless network, and the router forwarding the device identifier to the proxy application based on the established association after determining that the router has proxy authentication enabled; and

prompt the user of the mobile device to enter the network password, and transmit the entered network password in a message to the router, such that in response to the router validating the network password and granting the IoT device access to the wireless network, the IoT device transmits the device identifier to the router for subsequent network connection without a need for the mobile device or the proxy application.

20. The system of claim 19, further comprising an authentication mapper server in communication with the router, and wherein functionality of the proxy application is separated into a first proxy application and a second proxy application, wherein the authentication mapper server stores a mapping between a first application identifier associated with the first proxy application, a second application identifier associated with the second proxy application, and the device ID.