

Claims

We Claim:

1. A system (100) for authorizing a user to provide access to home automation, said system (100) comprising:
 - a smart wearable device (102) configured with one or more motion and biometric sensors, wherein the smart wearable device (102) detects a first set of user actions and biometric parameters of a subject user and to generate a first data comprising the first set of user actions, biometric information, and profile information of the subject user,
 - characterized in that:
 - a communication network, wherein, the subject first data from the smart wearable device (102) is encrypted and transmitted to a security module (108) through the communication network;
 - a home automation module (106) comprising the security module (108), wherein the security module (108) is configured to decrypt and analyze the first data, extract and identify at least one of an authorization type and a usage pattern, validate the extracted data by comparing with a set of multi-modal authorization profiles stored in a database (112) corresponding to the subject user, and grant access to the subject user for a plurality of IoT (Internet of Things) devices configured in the home automation module (106), wherein the home automation module (106) is enabled by the security module (108) only upon successful authentication of the user, based on the combined evaluation of the gesture pattern and biometric information, wherein the security module (108) is configured to generate a dynamic session key based on the user's role and access level, and to manage the subject user by maintaining organized data including user profiles, user actions, user activities, and session states, thereby optimizing accessibility for the home automation module (106), and wherein the smart wearable device (102) is further configured to detect removal from the user's body and to automatically revoke the subject user's authorization in real time.
2. The system as claimed in claim 1, wherein the smart wearable device (102), configured with one or more motion and biometric sensors, is configured to detect a first set of actions comprising a single action, a sequence of actions, or a gesture, while simultaneously capturing at least one of a biometric information.

3. The system as claimed in claim 2, wherein the smart wearable device (102) captures one or more positions and movements of at least one hand of the subject user in real time, and maps the captured data to a gesture pattern which is synchronized with variations in biometric information recorded during the movement.
4. The system as claimed in claim 1, wherein the smart wearable device (102) comprises at least one of a smartwatch, analog watch, wearable band, or any IoT device, including a biometric module configured to detect at least one physiological parameter while the subject user performs a gesture.
5. The system as claimed in claim 4, wherein the authorization pattern in the analog watch is generated by the subject user through pressing one or more crowns, wherein each press is validated by generating a time-stamped hardware token, forming part of the authorization pattern.
6. The system as claimed in claim 1, wherein the smart wearable device (102) is operable in either a sequential or simultaneous manner to generate at least one composite authorization pattern comprising motion data and biometric information.
7. The system as claimed in claim 1, wherein the IoT devices in the home automation module include at least one of light, fan, AC, door, motor, TV, coffee maker, chimney, electrical circuits, and safety lockers.
8. The system as claimed in claim 1, wherein granting access comprises permitting the subject user to interact with at least one IoT device by performing at least one of the following actions of opening, closing, operating, checking status, viewing, or modifying the configuration settings of the respective IoT device.
9. The system as claimed in claim 1, wherein the authorization type includes at least one, or a combination, of PIN, password, gesture pattern, accelerometer and gyroscope values, iris data, and fingerprint data, wherein the authorization pattern comprises security related information used to determine the user's identity and access privileges.
10. A method for storing user information, the method comprising:
 - inputting and capturing, by a smart wearable device (102), a first set of actions and biometric parameters of a user, and generating a first data set by the smart wearable device (102), wherein the first data includes at least one of the first set of actions, biometric information, device type, device ID, and the name of the user;
 - encrypting and transmitting the first data, through a communication network, to a security module (108);

processing, by the security module (108), the received first data to extract at least one of an authorization type and pattern, along with the associated biometric information;

authenticating the user by verifying the extracted information with multi-modal authorization profiles; and

storing, in a database (112), the validated data as part of a user profile, including device details, configuration settings, and access rules associated with the security module (108) and the authorized IoT devices within the home automation system.

11. The method as claimed in claim 10, wherein the first set of actions comprises at least one, or a combination, of an authorization type and an authorization pattern.
12. The method as claimed in claim 11, wherein the authorization type includes at least one, or a combination, of PIN, password, gesture pattern, accelerometer and gyroscope values, iris data, and fingerprint data, wherein the authorization pattern comprises security information used to determine the user's identity and level of access.
13. A method for authorizing a user to provide access to a home automation system through a smart wearable device (102), the method comprising:
 - detecting and preparing, by one or more motion and biometric sensors, a first set of actions performed by a user along with corresponding biometric and user information, wherein the smart wearable device (102) encrypts the resulting first data;
 - transmitting the encrypted first data to a security module (108), wherein the security module (108) is configured to decrypt and analyze the received first data, and validate the user's identity through combined verification of gesture data and biometric information against reference data stored in a database (112), wherein, upon successful validation, the security module (108) generates a temporary session key and assigns a tiered access scope to selected IoT devices, and wherein the home automation module (106) is enabled only during an active session, and with the session being automatically revoked upon removal of the wearable device or upon expiration of a predefined session timer.
14. The method as claimed in claim 13, wherein the user initiates a session through the smart wearable device (102), and pauses or terminates the session using a biometric gesture.
15. The method as claimed in claim 13, wherein access to IoT devices is restricted based on the user profile, and context based access control rules.