

Claims

We Claim,

1. A system for authorizing a user to provide access for home automation comprising:
 - a smart wearable device configured with one or more sensors, wherein the smart wearable device is capable of detecting a first set of actions performed by a user, and preparing a first data having the first set of actions and profile information of subject user;
 - a communication network, wherein, the first data from the smart wearable device is transmitted to a security module through the communication network;
 - a security module is capable of, analyzing the first data, identifying and extracting at least one of authorization type and pattern from the first data, validating the at least one of authorization type and pattern by comparing them with the information stored in a database in reference to the subject user, and providing and granting an access to the subject user, for a set of IoT devices configured in a home automation system; and
 - a database is capable of storing all profile information of one or more users including one or more device details, authorization types and patterns, configuration settings for security module and list of components in home automation system, wherein, the security module retrieves and compares the profile information, authorization type and pattern of the subject user, when subject user requests an access for the home automation system.
2. The system of claim 1, wherein, the smart wearable device which is configured with one or more sensors, finds and records one or more first set of actions includes a single action, series of actions or patterns or gestures performed by any body part of the subject user.
3. The system of claim 2, wherein, the smart wearable device captures at least one or more positions and movements of at least one hand of subject user, in real time.
4. The system of claim 1, wherein, the smart wearable device includes at least one of smart watch, analog watch, wearable band or any IoT device which detects and records the first set of actions of subject user.
5. The system of claim 4, wherein, the authorization pattern in the analog watch is generated by a subject user by pressing one or more crowns, at least for once, twice, thrice or

sequentially to complete the whole authorization pattern, wherein, subject authorization pattern is a hardware level data.

6. The system of claim 4, wherein, one or more smart wearable devices are sequentially or simultaneously used and operated to generate at least one authorization pattern from the user.
7. The system of claim 1, wherein, the IoT devices in home automation include at least one of light, fan, AC, door, motor, TV, coffee maker, chimney, electrical circuits, safety lockers.
8. The system of claim 1, wherein, granting the access is a permission to use at least one of IoT device by the subject user, at least by the way of opening, closing, operating, checking a status, viewing and modifying the configuration settings of subject IoT device.
9. The system of claim 1, wherein, the authorization type includes at least one of or combination of, pin, password, gesture pattern, accelerometer & gyro values, iris data and fingerprint, wherein, the authorization pattern is a security information to determine the user's identity and accessibility.
10. A method for storing a user information comprising:
 - inputting and capturing a first set of actions through a smart wearable device of a user, and preparing a first data by the smart wearable device, wherein the first data includes at least one of first set of actions, device type, device Id, and name of the user;
 - transmitting the first data to a security module through a communication network;
 - processing the first data by security module, wherein, the security module identifies and extracts at least one of authorization type and pattern from the first data for the subject user; and
 - storing the authorization type and pattern of the subject user as a user information at the database, wherein, the database contains all profile information of subject user including one or more device details, configuration settings for security module and list of accessible IoT devices in home automation system.
11. The method of claim 10, wherein, the first set of actions comprises at least one of or combination of authorization type and pattern.
12. The method of claim 11, wherein, the authorization type includes at least one of or combination of, pin, password, gesture pattern, accelerometer & gyro values, iris data and

fingerprint, wherein, the authorization pattern is a security information to determine the user's identity and accessibility.

13. The method of claim 11, wherein, the authorization type and pattern are set of one or more sequential data inputted through the one or more smart wearable devices of the subject user, at a given interval of time.

14. A method for authorizing a user to provide access for home automation system through a smart wearable device comprising:

detecting a first set of actions performed by a user through one or more sensors configured in the smart wearable device and preparing a first data having the first set of actions and user information, wherein, the smart wearable device encrypts the first data;

transmitting the first data over a communication network to a security module, wherein, the security module is capable of decrypting the first data;

analyzing the first data, identifying and extracting at least one of or combination of authorization type and pattern from the first data, validating the subject authorization type and pattern by comparing them with the information stored in the database in reference to the subject user, by the security module; and

providing and granting an access to the subject user for a set of IoT devices configured in a home automation system, by the security module, wherein, the set of IoT devices are permitted devices which are already configured by subject user.

15. The method of claim 14, wherein, the subject user makes a request in at least one of smart wearable device to provide access for home automation system.

16. The method of claim 14, wherein, granting the access is a permission to use at least one of IoT device by the subject user, at least by way of opening, closing, operating, checking a status, viewing and modifying the configuration settings of subject IoT device.

Claims

We Claim,

1. A system (100) for authorizing a user to provide access for home automation, said system (100) comprising:

a smart wearable device (102) configured with one or more sensors, wherein the smart wearable device (102) is capable of detecting a first set of actions performed by a subject user and preparing a first data having the first set of actions and profile information of the subject user characterized in that:

a communication network, wherein, the first data from the smart wearable device (102) is transmitted to a security module (108) through the communication network;

a home automation module (106) including the security module (108) for analyzing the first data, identifying and extracting at least one of authorization type and pattern from the first data, validating the at least one of authorization type and pattern by comparing them with the information stored in a database (112) in reference to the subject user, and providing and granting an access to the subject user, for a set 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) when the user is identified and authorized by the security module (108), wherein the security module (108) is configured to authenticate the subject user of the smart wearable device (102) or a mobile device (104) for the home automation module (106) through one or more pattern of actions performed by the first user through the subject smart wearable device (102), wherein the security module (108) manages the subject user, and organizes user profiles, user actions, user activities to streamline the accessibility for the home automation module (106), and

the database (112) configured for storing all profile information of one or more users including one or more device details, authorization types and patterns, configuration settings for security module (108) and list of components in home automation system, wherein the security module (108) retrieves and compares the profile information, authorization type and pattern of the subject user, when subject user requests an access for the home automation system.

2. The system as claimed in claim 1, wherein the smart wearable device (102) which is configured with one or more sensors, finds and records one or more first set of actions

includes a single action, series of actions or patterns or gestures performed by any body part of the subject user.

3. The system as claimed in claim 2, wherein the smart wearable device (102) captures at least one or more positions and movements of at least one hand of subject user, in real time.
4. The system as claimed in claim 1, wherein the smart wearable device (102) includes at least one of smart watch, analog watch, wearable band or any IoT device which detects and records the first set of actions of subject user.
5. The system as claimed in claim 4, wherein the authorization pattern in the analog watch is generated by a subject user by pressing one or more crowns, at least for once, twice, thrice or sequentially to complete the whole authorization pattern, wherein, subject authorization pattern is a hardware level data.
6. The system as claimed in claim 1, wherein the smart wearable device (102) is sequentially or simultaneously used and operated to generate at least one authorization pattern from the user.
7. The system as claimed in claim 1, wherein the IoT devices in home automation include at least one of light, fan, AC, door, motor, TV, coffee maker, chimney, electrical circuits, safety lockers.
8. The system as claimed in claim 1, wherein granting the access is a permission to use at least one of IoT device by the subject user, at least by the way of opening, closing, operating, checking a status, viewing and modifying the configuration settings of subject IoT device.
9. The system as claimed in claim 1, wherein the authorization type includes at least one of or combination of, pin, password, gesture pattern, accelerometer & gyro values, iris data and fingerprint, wherein, the authorization pattern is a security information to determine the user's identity and accessibility.
10. A method for storing a user information, said method comprising:
 - inputting and capturing, by a smart wearable device (102), a first set of actions of a user, and preparing a first data by the smart wearable device (102), wherein the first data includes at least one of first set of actions, device type, device Id, and name of the user;
 - transmitting, by a communication network, the first data to a security module (108);

processing, by security module (108), the first data, wherein, the security module (108) identifies and extracts at least one of authorization type and pattern from the first data for the subject user; and

storing, on a database (112), the authorization type and pattern of the subject user as a user information, wherein the database (112) contains all profile information of subject user including one or more device details, configuration settings for the security module (108) and list of accessible IoT devices in home automation system, wherein the authorization type and pattern are set of one or more sequential data inputted through the one or more smart wearable devices of the subject user, at a given interval of time.

11. The method as claimed in claim 10, wherein the first set of actions comprises at least one of or combination of authorization type and pattern.
12. The method as claimed in claim 11, wherein the authorization type includes at least one of or combination of, pin, password, gesture pattern, accelerometer & gyro values, iris data and fingerprint, wherein, the authorization pattern is a security information to determine the user's identity and accessibility.
13. A method for authorizing a user to provide access for home automation system through a smart wearable device (102), said method comprising:

detecting and preparing, by one or more sensors, a first set of actions performed by a user and user information, wherein the one or more sensors are configured in the smart wearable device (102), the smart wearable device (102) is configured to encrypt the first data;

transmitting, by a communication network, the first data over a communication network to a security module (108), wherein the security module (108) is configured for decrypting the first data, wherein the security module (108) is included in a home automation module (106) for analyzing the first data, identifying and extracting at least one of authorization type and pattern from the first data, wherein the home automation module (106) is enabled by the security module (108) when the user is identified and authorized by the security module (108), wherein the security module (108) is configured to authenticate the subject user of the smart wearable device (102) or a mobile device (104) for the home automation module (106) through one or more pattern of actions performed by the first user through the smart wearable device (102), wherein the security module (108) manages the subject user, and organizes user profiles, user

actions, user activities to streamline the accessibility for the home automation module (106).

analyzing, by the security module (108), the first data, identifying and extracting at least one of or combination of authorization type and pattern from the first data, validating the subject authorization type and pattern by comparing them with the information stored in the database (112) in reference to the subject user, by the security module (108); and

providing and granting an access, by the security module (108), to the subject user for a set of IoT (Internet of Things) devices configured in a home automation module (106), wherein the set of IoT devices are permitted devices which are already configured by subject user.

14. The method as claimed in claim 13, wherein the subject user makes a request in at least one of smart wearable device (102) to provide access for home automation module (106).
15. The method as claimed in claim 13, wherein granting the access is a permission to use at least one of IoT device by the subject user, at least by way of opening, closing, operating, checking a status, viewing and modifying the configuration settings of subject IoT device.