D3-Delta Document

July 12, 2020

**Resolved Defects and Inconsistency in Requirements Elicitation Document:**

1.Noise

* Removing “A stakeholder is of shorter height” from stakeholder identification.

**Resolved Defects and Inconsistency in Vision Document:**

1.Noise

* Removing statement “Keeping the environment safe and clean” from Vision Document Section 4.3 Need of Environmental considerations.

2.Terminology Clash

* Changing terminology “ecosystem” into “system platform” in Vision Document Section 3.2 User Environment

3.Terminology Clash

* Changing terminology “owner”, “homeowner”, “family”, “family and pets”, “home members” into “homeowner and their family members” throughout Vision Document.
* Changing “home users”, “people”, “you”, “the user” and “the users” into “users” throughout Vision Document.

4.Designation Clash

* Changing “Receives temporary and limited access to home features like one time access key, internal system status , maintenance status etc.” into “Receives daliy limited access to home features like one time access key, internal system status , maintenance status etc.” in Vision Document Section 3.1 Resposibilities of Temporary Users.
* Changing “Given access to some house services but not all. Receives temporary access to features on a need basis.” into “Given access to some house services but not all. Receives monthly access to features on a need basis.” in Vision Document Section 3.1 Resposibilities of Secondary Users.

July 17,2020

**Resolved Risks and Introduced New Requirements:**

1. All the sensitive information which is stored should be encrypted.
2. All the sensors should be checked every year by an expert.
3. System will send reminders to the homeowner that he/she needs to have the sensors checked otherwise there is no guarantee that security and safety features will be working properly.
4. A network firewall should be installed to prevent hackers from taking control of the devices.
5. The password of home internet should be encrypted to prevent hackers even if they bypass the firewall.
6. The system must ask the user to do a combination of different gestures in order to access the system. For example smiling and raising his/her eyebrows at the same time.
7. The system should encrypt all the data before uploading to the cloud.
8. Security features should have a backup battery and be able to work without the internet.
9. Cameras should be able to detect fire using live image recognition to identify actual fire.
10. Introduce the requirement that the system will prompt the user to remove masks, hats, gloves and glasses before using any biometric system which will help reduce the risk likelihood.
11. The system should invoke a fingerprint recognition system for identification when facial recognition is failed three times.
12. Keep backup features for time critical operations that are reliable and can be handled both manually by users and automatically by system.
13. Device firmware should be updated regularly.
14. All the devices should have a rollback update feature that undo changes if they are not compatible with the system.