CLAIMS

1. A method for managing Internet of Things (IoT) devices in an IoT system, the IoT system comprising:

a plurality of IoT devices operable by a user;

a hub for electronically coupling the plurality of IoT devices to the user;

an IOT server for electronically coupling the plurality of IoT devices with a plurality of IoT vendors;

a plurality of application programming interfaces, APIs, for enabling data sharing between the plurality of IoT vendors and the plurality of IoT devices;

a plurality of dashboard graphical user interfaces, GUI, for enabling communication between the plurality of IoT vendors and the user,

the IoT server enabling the plurality of APIs, and comprising an artificial intelligence, AI, engine;wherein the method comprises:

establishing, by the AI engine, a baseline of the IoT system behavioral patterns;

detecting, by the AI engine, abnormal system behavior based on the baseline;

matching, by the AI engine, the detected abnormal system behavior to any of a plurality of known cyberattack patterns;

remediating, by the AI engine, any damage done that corresponds with any of the matching known cyberattack patterns; and

performing, by the AI engine, predictive analytics and anomaly detection to predict IoT device failure in the IoT system based on Meantime Between Failure (MTBF) statistics provided by the plurality of IoT device vendors .

2. The method of claim 1, further comprising:

causing the IoT server to receive a plurality of flight envelope parameters corresponding with the plurality of IoT devices from the plurality of IoT vendors and from a user of the plurality of IoT devices;

determining whether any of the plurality of IoT devices are performing outside of the plurality of flight envelope parameters;

if any of the plurality of flight envelope parameters are exceeded, activating a system reaction by a rules engine, wherein the system reaction corresponds with a plurality of operator settable rules.

3. The method of claim 2, wherein the flight envelope parameters comprise at least:

a maximum operating range parameter for each IoT device provided by the plurality of IoT vendors; and

a pre-settable operating range parameter for each IoT device provided by the user.

4. An Internet of Things (IoT) system for managing IoT devices, the IoT system comprising:

a plurality of IoT devices operable by a user;

a hub for electronically coupling the plurality of IoT devices to the user;

an IOT server for electronically coupling the plurality of IoT devices with a plurality of IoT vendors;

a plurality of application programming interfaces (API) for enabling data sharing between the plurality of IoT vendors and the plurality of IoT devices;

a plurality of dashboard graphical user interfaces (GUI) for enabling communication between the plurality of IoT vendors and the user,

the IoT server being configured to enable the plurality of APIs and comprising an artificial intelligence, AI, engine, the latter being configured to :

establish a baseline of the IoT system behavioral patterns;

detect abnormal system behavior based on the baseline;

match the detected abnormal system behavior to any of a plurality of known cyberattack patterns;

remediate any damage done that corresponds with any of the matching known cyberattack patterns; and

perform predictive analytics and anomaly detection to predict IoT device failure in the IoT system based on Meantime Between Failure (MTBF) statistics provided by the plurality of IoT device vendors.

5. The system of claim 4, wherein the IoT server further comprises:

a server repository for storing flight envelope parameters associated with the plurality of IoT devices as provided by the plurality of IoT vendors.

6. The system of claim 4 or 5, wherein the IoT server further comprises an IoT hub.

7. The system of claim 5, wherein the flight envelope parameters comprise at least:

a maximum operating range parameter for each IoT device provided by the plurality of IoT vendors; and

a pre-settable operating range parameter for each IoT device j provided by the user.

8. The system of claim 4, wherein the AI engine comprises a rules engine having a machine learning function to establish said baseline of the user's IoT devices behavioral pattern and to detect said abnormal system behavior corresponding with a cyberattack pattern.

9. The system of claim 4, wherein the plurality of APIs comprises:

an IoT marketplace function through which the user purchases a replacement IoT device from any of the plurality of IoT vendors based on an analysis of the AI engine.

10. The system of claim 4, wherein the plurality of IoT vendors comprise a plurality of IoT device vendors and a plurality of 3rd party sources.

11. The system of claim 4, wherein the hub is voice-activated.

12. The system of claim 4, wherein the plurality of dashboard graphical user interfaces comprises:

a user dashboard for retrieving IoT device information and for enabling data sharing with the plurality of IoT vendors,

an IoT vendor dashboard for retrieving and sharing data corresponding with the data sharing enabled by the user.

13. The system of claim 12, wherein the user dashboard comprises:

a plurality of sections, the plurality of sections comprising:

an IoT device information section;

an IoT device sale history table; and

an IoT device data request section, wherein the IoT device data request section includes a MTBF data request, a failure statistics request, and a real-time telemetry request.