RESPONSE TO NON-FINAL OFFICE ACTION
Application No.: 17/741194
Filing Date: 05/19/2022
Art Unit: 2645
Examiner: OBAYANJU, OMONIYI
Title: HOME DISASTER MONITOR
Applicant: Daniel Kenney (Pro Se)
Date of Response: [Insert date of filing]

PRELIMINARY REMARKS

Applicant respectfully submits this response to the Office Action dated March 12, 2025, and hereby amends the claims and provides remarks in response to the rejections under 35 U.S.C. § 103.

As a pro se applicant, I respectfully request that this application's examination be subject to **MPEP § 707.07(j)**, which, as you know, encourages examiners to assist unrepresented inventors in understanding and overcoming procedural or substantive issues.

AMENDMENTS TO THE CLAIMS

Claims 1 through 7 are amended and presented in full below.

1. A method of remotely authorizing and configuring a communication-enabled electronic device via short message service (SMS), the method comprising:

- providing a device comprising:
    - a communication module with the capability to send and receive SMS messages routed through the cellular telephone network;
    - a processor; and
    - optionally, one or more sensors or actuators;
- receiving, at the communication module, an SMS message transmitted through the cellular telephone network, the message comprising a device-specific authorization code, pre-associated with the device and stored in a manner retrievable by the processor, the storage comprising either a non-volatile memory or a hardware-encoded identifier such as a DIP switch configuration or equivalent fixed logic setting;
- authenticating the device-specific authorization code using the processor;
- upon successful authentication of the first received valid authorization code:
    - storing the sender's telephone number as the primary authorized user;

    - enabling subsequent authenticated senders to be stored as additional authorized users, subject to access controls defined by the primary user;

- receiving, from an authorized user, one or more SMS messages comprising configuration parameters and/or operational commands;

- applying the configuration parameters or executing the operational commands to modify the operation of the device;

- enabling the primary user to manage the list of authorized users, including the ability to add, remove, or restrict users;

- and implementing one or more protections against automated or brute-force attempts to submit authorization codes, including:

    - delaying further authorization attempts after a defined number of failures;

    - detecting and filtering rapid or repeated submission attempts;

    - and applying verification heuristics that do not rely solely on originating telephone number, in recognition of potential caller ID spoofing.

2. The method of claim 1, wherein the configuration parameters include threshold values or behavioral rules for one or more sensors or actuators.

3. The method of claim 1, wherein the operational commands include enabling, disabling, or triggering specific functions of the device.

4. The method of claim 1, wherein the processor is further configured to reject SMS messages originating from sources not stored as authorized users.

5. The method of claim 1, wherein the processor limits authentication attempts based on timing or submission behavior rather than solely by message origin.

6. The method of claim 1, wherein the device operates without requiring a user-facing application, but remains compatible with third-party software that transmits configuration parameters or operational commands via SMS.

7. A system for remote authorization and control of a communication-enabled electronic device, comprising:

- a power source;

- optionally, one or more environmental sensors or output modules;

- a communication module comprising:

    - a GSM modem; and

    - a SIM card with an active telephone number;
- a processor; and
- a memory;

wherein the processor is configured to:

- receive an SMS message comprising a device-specific authorization code, pre-associated with the device and stored in a manner retrievable by the processor, the storage comprising either a non-volatile memory or a hardware-encoded identifier such as a DIP switch configuration or equivalent fixed logic setting;
- authenticate the code and:
    - if the first valid code, associate the sender's number as the primary authorized user;
    - otherwise, allow additional users to be added subject to access control by the primary user;
- store and enforce permissions associated with each authorized user;
- receive further SMS messages from authorized users comprising configuration parameters and/or operational commands;
- modify system behavior or execute operations based on the received messages;
- enable the primary user to manage the list of authorized users;
- and detect, delay, or reject repeated failed authorization attempts using behavioral analysis and verification mechanisms not solely dependent on originating phone number.

REMARKS

Applicant acknowledges that earlier claims may have overlapped substantially with prior art, and regrets any undue burden this may have placed on the Examiner's time. Having now assumed direct responsibility for prosecution, Applicant has reevaluated the invention's novel aspects as described in the specification. No changes have been made to the specification; instead, substantially restructured claims are presented to focus on the actual inventive contribution. Applicant hopes this will assist in advancing the examination efficiently and respectfully.

A. Response to §103 Rejections Based on Balaji, McCrosky, Dizengof, Ward, and Catlin

The newly submitted claims are directed to a method of remote user authorization and device configuration via direct SMS, not merely to a hardware system for monitoring. The cited art does not teach or suggest the claimed combination of:

- Receiving an inbound SMS from a user with a unique code;
- Authenticating that user and binding their device to the monitor;
- Allowing subsequent configuration and command via direct SMS without the need for an app, interface, or prior pairing.

While Balaji et al. may relate to disaster communications, and McCroskey may teach GSM-based telemetry, none of the references disclose or suggest this method of one-time code-based pairing via SMS for the purpose of secure, UI-free ownership and configuration.

Specifically:

- Balaji lacks any GSM or SMS-based configuration logic.
- McCroskey uses a GSM modem but lacks any user-initiated authorization model.
- Dizengof preselects a carrier but is silent on dynamic SMS-based binding or control.
- Ward addresses trace water sensing, but not system setup through SMS system.
- Catlin includes additional sensor types, but not control logic or authorization methods.

Thus, while the cited references cover various physical system components, the user interaction model—the core of the invention—is absent.

The method as claimed is not a mere rearrangement of known parts. It provides a new way to establish trust, control, and usability for non-technical users and rapid deployment scenarios, particularly in disaster contexts or among vulnerable populations. No cited reference teaches this, and therefore the rejection under 35 U.S.C. § 103 is respectfully traversed.

B. Pro Se Request for Examiner Assistance

As a pro se applicant, I respectfully request the Examiner's assistance in ensuring that this response and amended claims are fully and fairly considered in light of MPEP § 707.07(j). If any additional guidance or clarification is required to advance prosecution, I welcome such feedback.

CONCLUSION

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and withdrawal of the current rejections. If the Examiner believes that allowable subject matter exists in dependent form, Applicant is willing to accept a telephone interview or examiner's amendment to expedite prosecution.

Respectfully submitted,

Daniel Kenney (Pro Se)

dankenney524@gmail.com

321-298-8999
[Today’s date]