(12)Indian Patent Application

(21) Application Number: 202341010466

(22) Filing Date: 16/02/2023 (43) Publication Date: 23/08/2024

(71) Applicant(s): L&T TECHNOLOGY SERVICES LIMITED

(72) Inventor(s): Kumar, Rishi

(51) International Classifications: G06F 3/06 G11C 5/14 H04L 67/1097 G06F 11/07 H02J 7/00

(54) Title: METHOD AND SYSTEM OF CONTROLLING DATA ACCESS IN A SECURE MANNER IN AN ELECTRONIC DEVICE

(57) Abstract: A method and system for controlling data access in an electronic device is provided. A request for data access to a memory of the electronic from an external device is detected. The request may be received based on a charging connection established between the external device and the electronic device. A status of a physical data switch in the electronic device is detected and data access of the memory by the external device is enabled based on the detected status of the physical data switch.

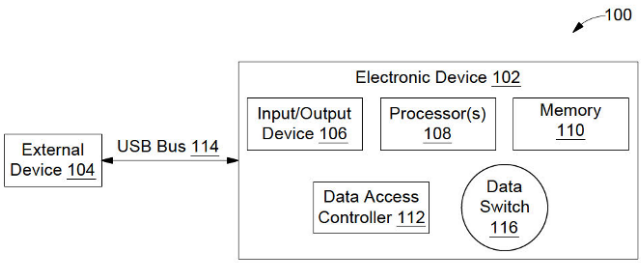

FIG. 1

FORM 2

THE PATENTS ACT 1970
(39 OF 1970)
&
The Patent Rules, 2003

Complete Specification

(See Section 10 and Rule 13)

1. TITLE OF THE INVENTION

METHOD AND SYSTEM OF CONTROLLING DATA ACCESS IN A SECURE MANNER IN AN ELECTRONIC DEVICE

2. APPLICANT(S)

(a) NAME : **L&T TECHNOLOGY SERVICES LIMITED**
(b) NATIONALITY : **INDIAN**
(c) ADDRESS : **DLF IT SEZ Park, 2nd Floor – Block 3**
1/124, Mount Poonamallee Road,
Ramapuram, Chennai – 600 089,
INDIA.

3. PREAMBLE TO THE DESCRIPTION

COMPLETE

The following specification describes the invention and the manner in which it is to be performed

DESCRIPTION

Technical Field

[001] This disclosure relates generally to access management, and more particularly to a system and a method for controlling data access in an electronic device.

BACKGROUND

[002] Most electronic devices are required to be charged using one or more charging mechanisms. In general, most devices utilize universal standards of Universal Serial Bus (USB) which establishes specifications for cables, connectors and protocols for connection, communication and power supply (interfacing) between computers, peripherals and other computers. USB acts as a common interface to connect several different types of peripheral devices such as keyboards, printers, media devices, cameras, scanners, etc. It allows for easy installation, faster transfer rates, higher quality cabling and hot-swapping. However, such USB connections to power the devices may be exploited for tampering device, or to connect to devices and clone/retrieve data from it.

[003] Therefore, there is a requirement to for a methodology to control data access in any smart or electronic device.

SUMMARY OF THE INVENTION

[004] In an embodiment, a method of controlling data access in an electronic device is provided. In an embodiment, the method comprises detecting, by an access controller located within the electronic device, a request for data access to a storage device of the electronic device from an external device. The request may be received based on a charging connection established between the external device and the electronic device. The method further comprises detecting, by the access controller, a status of a physical data switch in the electronic device. The method further comprises enabling, by the access controller, data access of the storage device by the external device based on the detected status of the physical data switch. In an embodiment, the connection between the external device and the electronic device may be established via one of a universal serial bus connector or a wireless charger. In an embodiment, the data access of the storage may be either disabled when the status of the physical data switch is detected as open or may be enabled when the status of the physical data switch is detected as close.

[005] In an embodiment, the access controller, may detect a digital authorization for the request for data access to the storage device upon detection of the status of the physical data switch as closed. Further, the method comprises enabling, by the access controller, data access of the storage device by the external device based on the digital authorization. In an embodiment, the method may further include generating, by the access controller, a unique security token based on a device ID information of the electronic device and a device ID information of the external device. The method further comprises authenticating, by the access controller, the generated unique security token based on an input of the unique security token in the electronic device by a user.

[006] In an embodiment, the unique security token may be generated by receiving, by the access controller, a device ID information associated with the external device. The access controller may receive a device ID information associated with the electronic device and create a merged ID by merging the device ID information associated with the external device and the device ID information associated with the electronic device. The access controller may then associate a private key with the merged ID. In an embodiment, the unique security token may be securely displayed on a display of the external device. In an embodiment, the external device may display a secure user interface for a user to input the securely displayed unique security token.

[007] In another embodiment, a system for controlling data access in an electronic device comprising one or more processors and a memory is provided. The memory may store a plurality of processor-executable instructions which upon execution cause the one or more processors to detect a request for data access to the memory from an external device. In an embodiment, the request may be received based on a charging connection established between the external device and the electronic device. In an embodiment, a status of a physical data switch in the electronic device may be detected and data access of the memory by the external device may be enabled based on the detected status of the physical data switch.

[008] Various objects, features, aspects and advantages of the inventive subject matter will become more apparent from the following detailed description of preferred embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles.

[010] **FIG. 1** is a block diagram of a data access controller system, in accordance with an embodiment of the present disclosure.

[011] **FIG. 2** illustrates a functional block diagram of the access controller 112 of the electronic device 102, in accordance with an embodiment of the present disclosure.

[012] **FIG. 3** is a flowchart depicting methodology of controlling data access in an electronic device using two step verification, in accordance with an embodiment of the present disclosure.

[013] **FIG. 4** is a flowchart depicting methodology of controlling data access in an electronic device, in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[014] Exemplary embodiments are described with reference to the accompanying drawings. Wherever convenient, the same reference numbers are used throughout the drawings to refer to the same or like parts. While examples and features of disclosed principles are described herein, modifications, adaptations, and other implementations are possible without departing from the scope of the disclosed embodiments. It is intended that the following detailed description be considered as exemplary only, with the true scope being indicated by the following claims. Additional illustrative embodiments are listed.

[015] Charging hubs may be provided at various places to allow easy charging of smart devices. However, unauthorized data access may be enabled in case devices are connected to charging hubs through USB connections.

[016] The present disclosure provides methods and systems for controlling data access in an electronic device. **FIG. 1** is a block diagram of a data access controller system, in accordance with an embodiment of the present disclosure.

[017] The data access controller system 100 may include an electronic device 102 comprising one or more processors 108, a memory 110, an input/output device 106, a access controller 112 and a data switch 116. The electronic device 102 may be electrically connected to an external device 104 through a bus 114 which may be a Universal Serial Bus (USB). In an embodiment, the USB bus 114 could be used in any other suitable manner. The USB bus 114 represents any suitable USB bus, such as a bus supporting USB 1.x, USB 1.1, USB 2.0, USB 3.x, USB4 and/or any other past, present, or future USB specification.

[018] The electronic device 102 may include one or more processor(s) 108 and a memory 110. In an embodiment, examples of processor(s) 108 may include, but are not limited to, Qualcomm® Sanpdragon®, Exynos®, Bionic®, Kirin®, Google® Tensor®, MediaTek®, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, FortiSOC™ system on a chip processors or other future processors. The memory 110 may store instructions that, when executed by the processor 108, cause the processor 108 to control data access of the memory 110, as discussed in greater detail below. The memory 110 may be a non-volatile memory or a volatile memory. Examples of non-volatile memory may include, but are not limited to a flash memory, a Read Only Memory (ROM), a Programmable ROM (PROM), Erasable PROM (EPROM), and Electrically EPROM (EEPROM) memory. Examples of volatile memory may include but are not limited to Dynamic Random Access Memory (DRAM), and Static Random-Access memory (SRAM).

[019] In an embodiment, the electronic device 102 may be electrically and communicatively coupled to the external device 104 through a suitable USB port (not shown) provided in the electronic device 102. The USB port (not shown) is capable of coupling an external device 104 to the USB bus 114. The external device 104 could be coupled directly to a USB port (not shown) or indirectly to the USB port, such as when the external device 104 is coupled to the USB port via a USB cable or other mechanical lock system. In an embodiment, the USB port may represent any suitable structure capable of providing access to the USB bus 114.

[020] In an embodiment, the electronic device 102 may receive a request from the external device 104 for accessing data stored in the memory 110 of the electronic device 102 through the USB bus 114. In an embodiment, the external device 104 may include, but not limited to, a smart USB flash drive, a battery charger, a docking station, a variety of computing systems, including but not limited to, a smart device, a single chip microprocessor, a charging hub station,

a printer, a laptop computer, a desktop computer, a notebook, a workstation, a portable computer, a personal digital assistant, a handheld or a mobile device.

[021] In an embodiment, a user may connect the electronic device 102 to the external device 104 in order for charging a battery (not shown) of the electronic device 102. This may include, for example, the user connecting a USB connector connected to an external device 104 to a USB port of the electronic device 102 in order to charge the battery of the electronic device 104. In an embodiment, the external device 104 may be a charging hub station provided in general in public places for users to charge their smart electronic devices.

[022] The access controller 112 of the electronic device 102 may detect a connection of the external device 104 and detects a status of the data switch 116. The data switch 116 is a physical switch connecting the memory 110 with the processor 108 and the access controller 112. The access of data stored in the memory 110 by the external device 104 may be enabled when the data switch 116 is closed thereby enabling data transmission from the memory 110 to the external device 104. The physical connection may be detected by access controller 112 based on a physical maneuvering of the data switch 116 by a user. The data switch 116 may be an electronic switch which may be connected between a data transmission path in order to connect or disconnect the data transmission path based on the state of the data switch 116. The state of the switch may be toggled between an OPEN or CLOSE state based on a manual maneuvering of a physical switch electrically coupled to the electronic switch. As will be appreciated, in some embodiment, the physical switch may be implemented in the electronic device in such as way that it is conveniently maneuverable by the user through an external manifestation on the electronic device.

[023] In case, the data switch 116 is OPEN the data transmission path may be disconnected between the memory 110 and the external device 104 and accordingly data transmission may be disabled thereby not allowing any data to be transmitted from the electronic device 102 to the external device 104.

[024] Further, the access controller 112 may enable data transmission in case the data switch 116 is CLOSE and based on a digital authorization of the external device 104. The digital authorization (as explained in detail in FIG. 2) may be performed by the access controller 112 in order to enable transmission of the data from the memory 110 of the electronic device 102 to the external device 104 based on the request for data access form the external device 104.

[025] **FIG. 2** illustrates a functional block diagram of the access controller 112 of the electronic device 102, in accordance with an embodiment of the present disclosure. Referring now to **FIG. 2**, a functional block diagram 200 of the access controller 112 comprises a data access request detection module 202, a data switch status detection module 204, a digital authorization module 206, a security token generation module 208, a private key generation module 210, a secure user interface module 212.

[026] The data access request detection module 202 may detect a request for access of data of the memory 110 of the electronic device 102 by the external device 104 being connected to the electrical device 102 via a USB bus 114. The data switch status detection module 204 of the access controller 112 may determine a status of the data switch 116 to be either CLOSE or OPEN. In an embodiment, the data switch 116 may be a physical switch provided in the electronic device 102 to be manually maneuvered between a CLOSE or OPEN positions. A user of the electronic device 102 may set the switch to be in CLOSE position in case data access to the external device 104 is to be enabled. Further, the user of the electronic device 102 may set the switch to be in OPEN position in case the data access to the external device 104 is to be disabled. In case, the data switch status detection module 204 detects that the status of the data switch 116 is set in a CLOSE position the digital authorization module 206 enables a digital authorization of the external device 104 requesting data access from the electronic device 102. In an embodiment, the access controller 112 may provide data access to the external device 104 based on successful authorization of the external device 104.

[027] The digital authorization module 206 comprises the security token generation module 208 and the private key generation module 210. The security token generation module 208 may generate a unique security token based on a device ID information of the electronic device 102 and a device ID information of the external device 104. In an embodiment, the access controller 112 may request for device ID information from the external device 104 based on the detection of the data access request and the CLOSE status of the data switch 116. In an embodiment, the device ID information of the external device 104 and the electronic device 102 may be, but not limited to, a MAC address, serial number, service Tag, an IP address or an IEMI number of the external device 104 or any unique ID depicting the identity of the external device 104 or the electronic device 102.

[028] In an embodiment, the device ID of the external device 104 may be generated using public key infrastructure (PKI) technology or other suitable mechanisms to determine if the

external device 104 is a legitimate device or contains a valid digital certificate or key. In some embodiments, the valid digital certificate or key associated with the external device 104 may be stored in a memory or portion of memory of a secure microcontroller that is not accessible or encrypted and transmitted to the access controller 112 based on a request for device ID information of the external device 104. In an exemplary scenario, the external device 104 may not transmit device ID to the electronic device 102, the access controller 112 may then display an error notification that no device ID of the external device 104 is received and may disable the data access of the external device 104 and terminate the digital authorization of the external device 104. In an embodiment, the error notification may be implemented using one or more protocols such as but not limited to, National Institute of Standards and Technology (NIST) 800-61r2 or later.

[029] In an embodiment, the device ID received from the external device 104 and the device ID of the electronic device 102 may be merged to generate a merged ID. In an embodiment, the merged ID may be generated based on one or more known in the art encryption methodology. The private key generation module 210 may generate a private key based on one or more methodology known in the art. The digital authorization module 206 may associate the private key with the merged key and the resultant may be trimmed by trimming a pre-defined number of digits from the result. In an embodiment, the 5 last digits of the result may be trimmed in order to generate a unique security token. In an embodiment, the unique security token may be, but not limited to, a 6-8 digit code or may comprise of alpha-numeric.

[030] The secure user interface module 212 may then output the unique security token on a display screen of the input/output device 106. The unique security token is securely displayed on the display screen in form of a floating screen overlapping any interface of an application running on the electronic device 102. In an embodiment, a secure user input interface may also be displayed on the electronic device 102 in form of a floating display such as a virtual keyboard comprising numeric buttons from 0-9 or a QWERTY keyboard. In an embodiment, the data access controller may input the displayed unique security token using the secure user input interface. The data access controller may validate the inputted code by the user using the secure input interface with the unique security token generated by the security token generation module 208. In case the inputted code matches the unique security token generated by the security token, the data access controller enabled data transfer of the data from the memory 110 of the electronic device 102 to the external device 104.

[031] **FIG. 3** is a flowchart depicting methodology of controlling data access in an electronic device using two step verification, in accordance with an embodiment of the present disclosure.

[032] At step 302, a request for data access to a memory 110 of the electronic device 102 may be detected by an access controller. In an embodiment, the request for data access may be received based on a charging connection established between the external device 104 and the electronic device 102. As a first step of verification, at step 304, a status of a physical data switch 116 in the electronic device 102 may be detected by the access controller 112. In case, at step 304, the status of the physical data switch 116 is detected as OPEN, the data access by the external device 104 may be disabled at step 306.

[033] In case, at step 304, the status of the physical data switch 116 is detected as CLOSE, a digital authorization of the external device 104 may be initiated by the access controller 112 at step 308 as a second step of verification.

[034] At step 310, a device ID information of the external device 104 may be requested by the access controller 112. At step 311, the access controller 112 may determine if the requested device ID information is received or not. In, case the requested device ID information of the external device is not received, the data access of the external device is disabled at step 306 and the digital authorization is stopped.

[035] In case device ID information of the external device is received by the access controller 112, the digital authorization proceeds to step 312, where a device ID information of the electronic device 102 may be determined by the access controller 112. At step 314, a merged ID may be generated by merging the device ID received from the external device 104 and the device ID determined of the electronic device 102. At step 316, a private key may be determined by the access controller 112. At step 318, a unique security token may be generated by associating the private key determined at step 316 with the merged ID generated at step 314.

[036] At step 320, the unique security token generated at step 318 may be displayed securely on a display of the electronic device 102. At step 322, a secure user interface may be provided on the electronic device 102 for a user to input the securely displayed unique security token at step 320. At step 324, the user inputted token may be validated to be same as the unique security token generated at step 318. In case, the user inputted token is same as the unique security token generated at step 318, the data access of the external device 104 may be enabled at step 326.

In case, the user inputted token is not same as the unique security token generated at step 318, the data access of the external device 104 may be disabled at step 306.

[037] **FIG. 4** is a flowchart depicting methodology of controlling data access in an electronic device, in accordance with an embodiment of the present disclosure.

[038] At step 402, a request for data access to a memory 110 of the electronic device 102 may be detected by an access controller. In an embodiment, the request for data access may be received based on a charging connection established between the external device 104 and the electronic device 102. As a first step of verification, at step 404, a status of a physical data switch 116 in the electronic device 102 may be detected by the access controller 112. In case, at step 404, the status of the physical data switch 116 is detected as CLOSE, the data access by the external device 104 may be enabled at step 406.

[039] In case, at step 404, the status of the physical data switch 116 is detected as OPEN, the data access by the external device 104 may be disabled at step 408.

[040] In light of the above-mentioned advantages and the technical advancements provided by the disclosed method and system, the claimed steps as discussed above are not routine, conventional, or well understood in the art, as the claimed steps enable the following solutions to the existing problems in conventional technologies. Further, the claimed steps clearly bring an improvement in the functioning of the device itself as the claimed steps provide a technical solution to a technical problem.

[041] The specification has described method and system of controlling data access in a secured manner in an electronic device. The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[042] It is intended that the disclosure and examples be considered as exemplary only, with a true scope of disclosed embodiments being indicated by the following claims.

WE CLAIM:

1. A method of controlling data access in an electronic device, the method comprising:

detecting, by an access controller located within the electronic device, a request for data access to a storage device of the electronic device from an external device, wherein the request is received based on a charging connection established between the external device and the electronic device;

detecting, by the access controller, a status of a physical data switch in the electronic device; and

enabling, by the access controller, data access of the storage device by the external device based on the detected status of the physical data switch.

2. The method as claimed in claim 1, wherein the connection established between the external device and the electronic device is via a universal serial bus (USB) connector.

3. The method as claimed in claim 1, wherein the data access of the storage is one of: disabled when the status of the physical data switch is detected as OPEN or enabled when the status of the physical data switch is detected as CLOSE.

4. The method as claimed in claim 3, comprising:

detecting, by the access controller, a digital authorization for the request for data access to the storage device upon detection of the status of the physical data switch as closed; and

enabling, by the access controller, data access of the storage device by the external device based on the digital authorization.

5. The method as claimed in claim 4, wherein the digital authorization comprising:

generating, by the access controller, a unique security token based on a device ID information of the electronic device and a device ID information of the external device; and

authenticating, by the access controller, the generated unique security token based on an input of the unique security token in the electronic device by a user.

6. The method as claimed in claim 5, wherein the generation of the unique security token comprises:

receiving, by the access controller, a device ID information associated with the external device;

receiving, by the access controller, a device ID information associated with the electronic device;

creating, by the access controller, a merged ID by merging the device ID information associated with the external device and the device ID information associated with the electronic device; and

associating, by the access controller, a private key with the merged ID.

7. The method as claimed in claim 6, comprising securely displaying the unique security token on a display of the electronic device.

8. The method as claimed in claim 7, comprising displaying a secure user interface to input the securely displayed unique security token.

9. A system for controlling data access in an electronic device, comprising:

one or more processors;

a memory communicatively coupled to the processors, wherein the memory stores a plurality of processor-executable instructions, which, upon execution, cause the processors to:

detect a request for data access to the memory from an external device, wherein the request is received based on a charging connection established between the external device and the electronic device;

detect a status of a physical data switch in the electronic device; and

enable data access of the memory by the external device based on the detected status of the physical data switch.

10. The system as claimed in claim 9, wherein the data access of the memory is one of: disabled when the status of the physical data switch is detected as OPEN, or enabled when the status of the physical data switch is detected as CLOSE.

Dated this 16th day of February 2023

-- Digitally Signed--
Bhanu Prasad
(INPA No: **3253**)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

ABSTRACT

METHOD AND SYSTEM OF CONTROLLING DATA ACCESS IN A SECURE MANNER IN AN ELECTRONIC DEVICE

A method and system for controlling data access in an electronic device is provided. A request for data access to a memory of the electronic from an external device is detected. The request may be received based on a charging connection established between the external device and the electronic device. A status of a physical data switch in the electronic device is detected and data access of the memory by the external device is enabled based on the detected status of the physical data switch.

[To be published with FIG. 1]

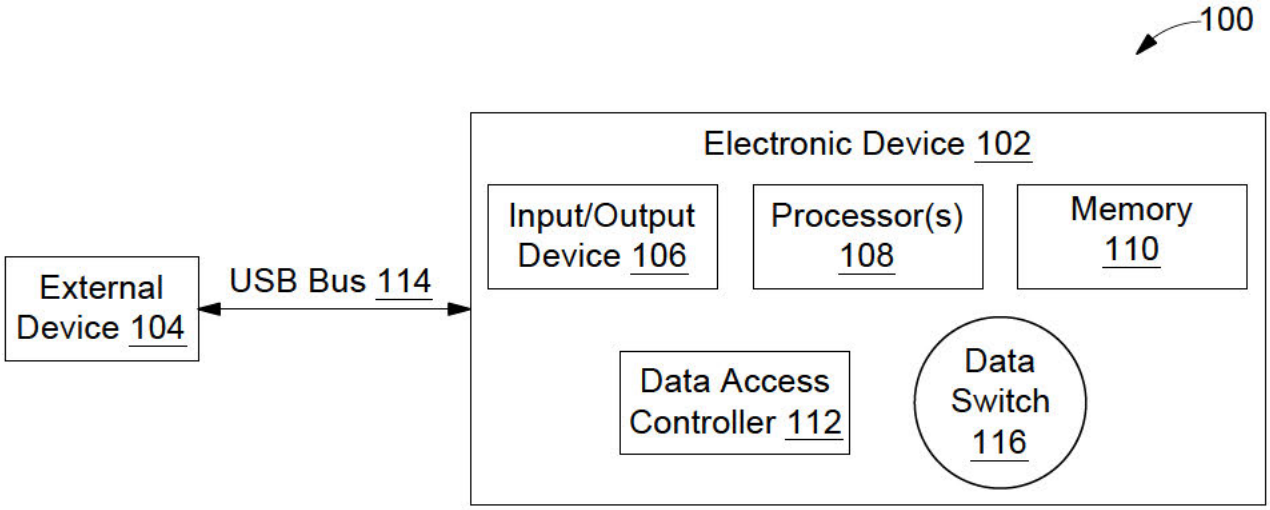

FIG. 1

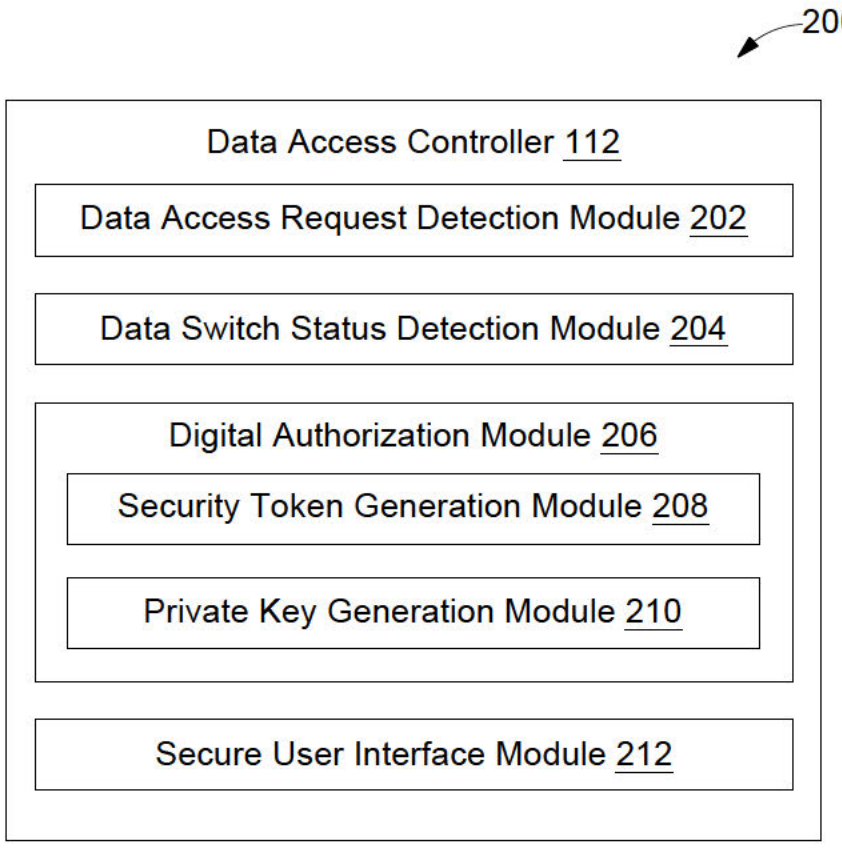

FIG. 2

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

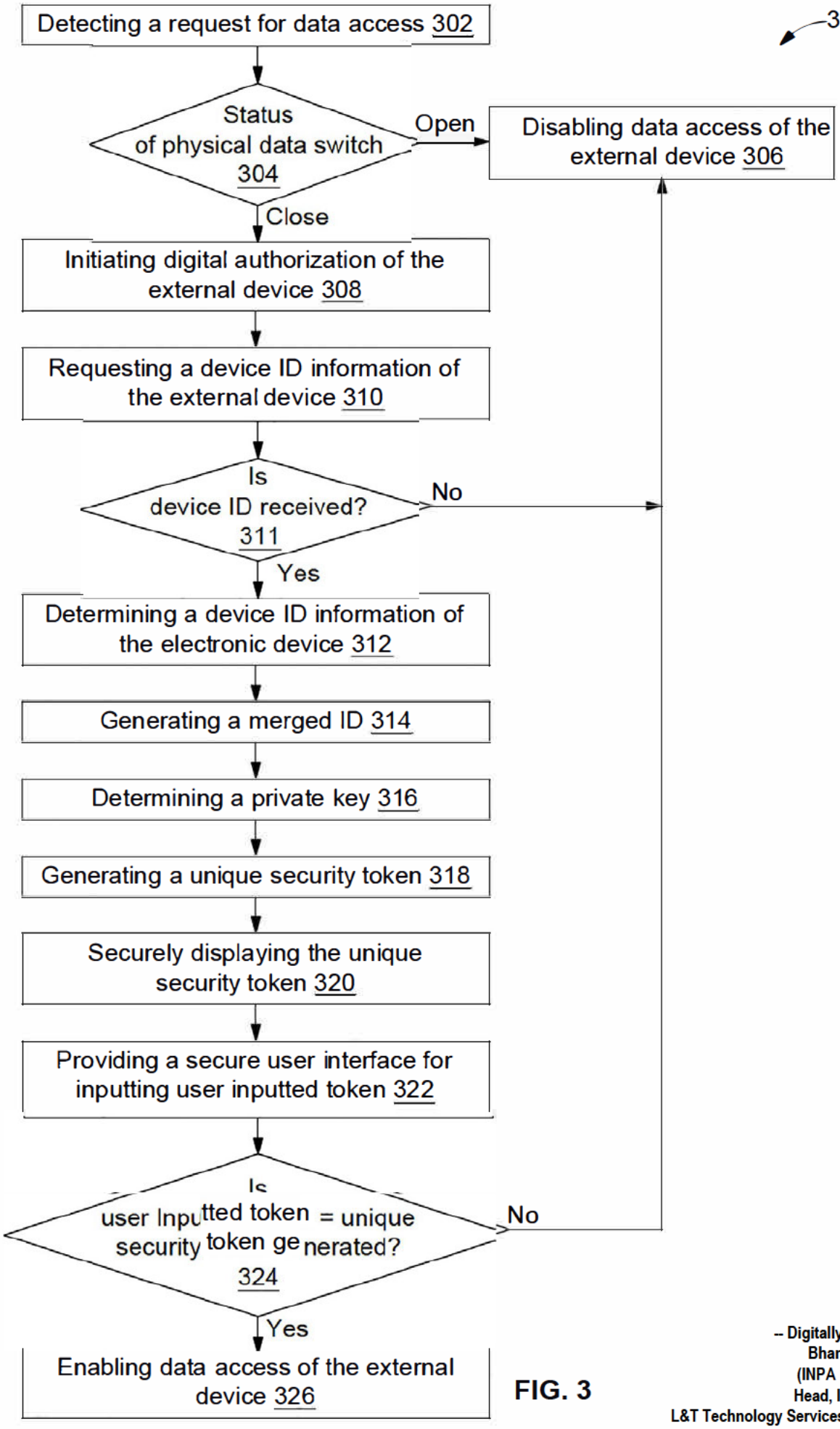

FIG. 3

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

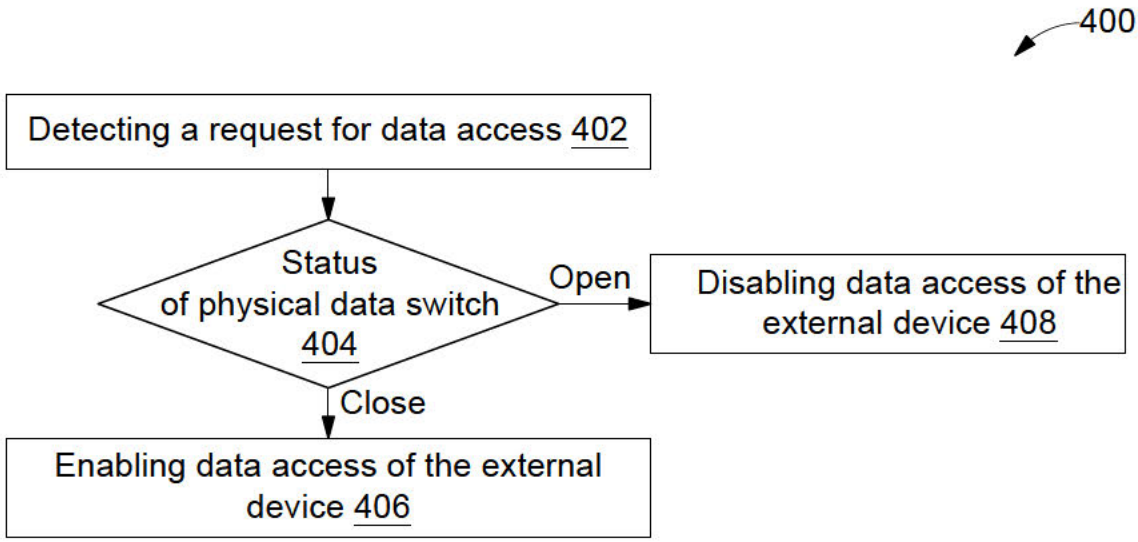

FIG. 4

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.