(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 083 528 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
14.03.2001 Bulletin 2001/11

(51) Int. Cl.[7]: **G07F 7/10**

(21) Application number: **00119269.9**

(22) Date of filing: **06.09.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **09.09.1999 SE 9903240**

(71) Applicant:
i3 micro technology ab
194 61 Upplands Väsby (SE)

(72) Inventors:
- **Landeström, Thomas**
  16763 Bromma (SE)
- **Bergman, Berth-Olof**
  19592 Märsta (SE)

(74) Representative:
Andersson, Björn E. et al
Ström & Gulliksson AB,
P.O. Box 4188
203 13 Malmö (SE)

(54) Electronic transaction apparatus

(57) An electronic transaction apparatus (30) is to be used together with a host processing device (10) and at least one remote processing device (40), where the host processing device and the remote processing device each has a processing unit (11, 41) and an interface (12, 42) and is capable of communicating I/O transactions according to a predefined protocol (20a-b) through the interface. The electronic transaction apparatus has programmable controller means (31), memory means (33) for storing a data modification procedure, first interface means (32) to be connected to the interface (12) of the host processing device (10) and second interface means (34) to be connected to the interface (42) of the remote processing device (40). The controller means is programmed to perform the following actions by executing program instructions stored in the memory means: intercepting an I/O transaction, which has been transmitted by either the host processing device or the remote processing device and is destined to the other; modifying data contained in the intercepted I/O transaction in accordance with the data modification procedure stored in the memory means; and retransmitting the intercepted I/O transaction, with its modified data and according to the predefined protocol, to either the remote processing device, in case the I/O transaction was destined to the remote processing device when intercepted, or the host processing device, in case the I/O transaction was destined to the host processing device when intercepted.

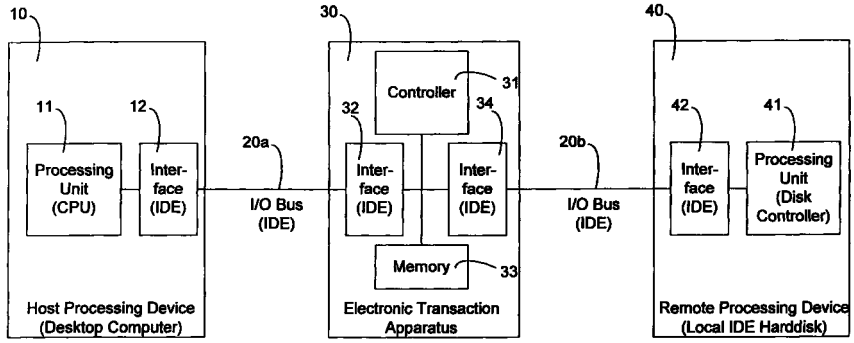

Fig 1

EP 1 083 528 A2

Description

Technical Field

[0001] The present invention relates to an electronic transaction apparatus for use together with a host processing device and a remote processing device, where the host processing device and the remote processing device each has a processing unit and an interface and is capable of communicating I/O transactions according to a predefined protocol through the interface. More specifically, the present invention relates to an electronic transaction apparatus for providing efficient and extremely good information security for data, which are stored on and read from the remote processing device.

Prior Art

[0002] Using the terminology defined above, a host processing device may for instance be any commercially available personal computer, such as a desktop computer or a laptop computer. Moreover, in this context a remote processing device may be any commercially available external computer peripheral, such as a modem (which is connected via a serial interface to the host processing device/computer) or an external hard disk (which has a disk controller and is connected via e.g. an IDE compatible interface to the host processing device/computer).

[0003] Alternatively, the host processing device may be a first portion of any commercially available personal computer, or more specifically the motherboard with its central processing unit (CPU), whereas the remote processing device will be a second portion of this computer, preferably a permanent read/write data storage device, such as a hard disk with a disk controller and disk interface (IDE compatible or other).

[0004] Still another alternative is that the host processing device is a first commercially available personal computer, and the remote processing device is a second commercially available personal computer. The first and second computers are interconnected via respective network interfaces, such as RJ45 (10Base-T) or AUI, over a network protocol, for instance TCP/IP.

[0005] Regardless of the actual realization of the host processing device and the remote processing device, information security is a major concern in all computer networks and at several levels. The first and perhaps most vulnerable level is locally at each individual workstation computer (referred to as "client" or "desktop" level in the rest of this document). Another important level is the actual network that interconnects all clients and provides access for them to central network resources, such as file server computers, application server computers, network printers, etc. Still another level is the central network resources themselves.

[0006] Recent studies in the US indicate that a majority of all US business organizations are victims of computer-related crimes. In fact, as many as two-thirds of the organizations may be subjected to such attacks every year. In the majority of these cases, it appears that the perpetrator gained access to the computer system, and the information stored therein, by masquerading as an authorized user. Moreover, a majority of the intrusions are made by employees or ex-employees of the organization itself.

[0007] While existing computer networks usually are provided with access control functionality that e.g. requires a user to log on to a particular network resource by entering a user ID and a password, the information stored locally on hard disks inside the individual client computers and servers is often not protected at all. Therefore, if a criminal is given an opportunity to physically access these computers, which is normally the case if the criminal is an employee, then network logon facilities will not prevent the criminal from reading the information from any such computer by for instance using special software or by simply removing the hard disk from its host computer and installing it in another computer for undisturbed "offline" access to the disk.

[0008] The Internet expansion, an increased understanding of the value of information, the growing distribution of computer viruses, legal requirements as regards safe handling of personal data (i.e. data linked to human individuals), and an rapidly increasing number of computer thefts are all factors that contribute to a pronounced need for securing data at the desktop level of computers.

[0009] Some prior art approaches of obtaining satisfactory information security at the desktop level use dedicated software for data encryption and authentication purposes. However, software-based approaches suffer from several serious drawbacks. Firstly, sensitive information about the encryption or authentication procedure is stored on the same medium (the hard disk) as it is intended to protect.

[0010] Secondly, encryption/authentication functionality may be affected by virus attacks on the operating system.

[0011] Moreover, any software-based encryption/authentication procedure will inevitably be dependent of the type of file system in use.

[0012] Also, operating system stability will limit the stability of the encryption/authentication functionality. In other words, an unstable or less than fully reliable operating system might crash so badly, that any encryption/authentication process run by it may be prematurely aborted or otherwise prevented from normal operation.

[0013] Finally, since the execution of the encryption/authentication process is handled by the host computer's own motherboard and its CPU, other processes - such as application programs - will be given less than

full execution performance.

The Invention

[0014] It is an object of the present invention to eliminate the drawbacks of the prior art approaches of obtaining information security for a host processing device and a remote processing device, which exchange I/O transactions according to a predefined protocol through an interface, where the host processing device preferably is any commercially available computer, or a portion thereof, and the remote processing device preferably is any commercially available computer peripheral or I/O device external or internal to the host processing device/computer.

[0015] The object has been achieved by an electronic transaction apparatus according to the enclosed independent patent claim.

[0016] More specifically, the object has been achieved by an electronic transaction apparatus, which is designed as an independent apparatus fully isolated from the host processing device and the remote processing device. The apparatus has its own controller and memory and is adapted to be connected between the host and remote processing devices, so that I/O transactions sent from the host processing device to the remote processing device, or vice versa, will be intercepted by the apparatus, modified as regards the data contained therein, and ultimately retransmitted to the remote processing device or the host processing device, respectively. The modification of data is made according to a predefined data encryption or authentication procedure, which preferably takes, as one input parameter, a unique user key code that is entered by means of e.g. a smartcard reader or a thumbprint reader. The data modification procedure will be fully transparent to the host and remote processing devices, and as an additional benefit, it may also improve I/O performance between the host and remote processing devices.

Brief Description of the Drawings

[0017] The present invention will now be described in more detail with reference to the attached drawings, in which:

FIG 1 is a schematic illustration of how the electronic transaction apparatus according to the invention is intended to operate in an environment consisting of a host processing device and a remote processing device;

FIG 2 is a more detailed illustration of the electronic transaction apparatus in a typical application inside a desktop computer, wherein the motherboard of the latter represents the host processing device and wherein the remote processing device is represented by any one of a serial interface peripheral (e.g. an external modem), a parallel interface peripheral (e.g. a printer), a permanent storage device (e.g. an internal hard disk or an internal floppy drive), or another computer, which is connected to the host processing device through a network connection interface; and

FIG 3 is a block diagram of a preferred embodiment of the electronic transaction apparatus.

Detailed Disclosure of the Invention

[0018] FIG 1 is intended to give an overall understanding of the purpose and task of an electronic transaction apparatus 30 according to the invention. The transaction apparatus 30 is connected between a host processing device 10, which is exemplified as a commercially available desktop computer, and a remote processing device 40, which is exemplified as a local IDE-compatible hard disk mounted inside the desktop computer 10. As is generally known, the local hard disk 40 has a processing unit 41 in the form of a disk controller as well as an IDE interface 42, by means of which the hard disk 40 may be connected over an I/O bus (IDE bus) 20a-b to a processing unit (CPU) 11 and an IDE interface 12 provided on a main circuit board (motherboard) of the desktop computer 10.

[0019] As shown in FIG 1, the transaction apparatus 30 comprises a controller 31 and a memory 33. Moreover, it has a first interface 32 for connection, via a first part 20a of the I/O bus, to the interface 12 of the host processing device 10. The transaction apparatus 30 also has a second interface 34 for connection, via a second part 20b of the I/O bus, to the interface 42 of the remote processing device 40.

[0020] As will be described in more detail with reference to the remaining figures, the controller 31 and memory 33 form a transaction engine, which is made up of a CPU module with an integrated real-time operating system, a BIOS and application software for performing a predefined modification of data contained in I/O transactions exchanged between the host processing device 10 and the remote processing device 40. A typical example of such data modification is data encryption/decryption for improved information security. In such a case, as will be further described with reference to FIG 3, the data contained in I/O transactions sent from the motherboard to the hard disk 40 will be encrypted by the transaction apparatus 30, while data will be decrypted for I/O transactions going the opposite direction (i.e. from the hard disk 40 to the motherboard). Consequently, the hard disk 40 will always contain encrypted data, whereas the motherboard, and the application programs run thereon, will always experience clear-text data.

[0021] Other possible data modifications involve conversion of data from one protocol to another, or hardware emulation between different types of interfaces (preferably for converting between SCSI and IDE,

between IDE and SCSI or between USB and IDE).

[0022] The purpose of the first interface 32 is to emulate the hardware or software interface to the host processing device 10 (i.e. the motherboard of the desktop computer), so that I/O transactions may be intercepted between the operating system or BIOS of the motherboard (host processing device 10) and the peripheral device 40 (remote processing device 40). In a way, the first interface 32 may be referred to as a virtual interface.

[0023] The second interface 34 is used for connecting the peripheral device 40 to the motherboard and may therefore be referred to as a physical interface. More specifically, the transaction apparatus 30 is arranged to perform interception, modification and retransmission of all I/O transactions in accordance with the existing protocol (such as IDE); consequently the presence and operation of the transaction apparatus 30 will be fully transparent to the motherboard and the peripheral device 40.

[0024] Referring now to FIG 2, an enlarged scope of application is illustrated as compared to FIG 1. Identical reference numerals in FIGs 1 and 2 represent identical or equivalent components; therefore the description of such components is not repeated hereinafter. The motherboard 15 comprises a CPU 11, a RAM memory 13, a ROM memory 14 as well as different interface ports, which are commonly designated by 12 in FIG 2.

[0025] As in FIG 1, the transaction apparatus 30 of FIG 2 is connected between the motherboard 15 of a workstation computer 10 and a local hard disk 40. Moreover, the transaction apparatus 30 of FIG 2 is also interconnected between the motherboard 15 and other peripheral devices, that all may represent the remote processing device 40 of FIG 1, to which the host processing device 10 (more precisely its motherboard 15) is connected.

[0026] More specifically, the transaction apparatus 30 is connected between a serial RS232 interface of the motherboard 15 and an external modem 50, between an IDE interface of the motherboard 15 and the local hard disk 40, between a floppy interface of the motherboard 15 and a local floppy drive 54, and between a network interface of the motherboard 15 via an external network connector 56 and a network 60 to a plurality of network client computers 62, 64, 66.

[0027] The scenario pictured in FIG 2 is intended to illustrate the wide applicability of the transaction apparatus 30 according to the invention. The meaning of the terms "host processing device" and "remote processing device" used for defining the invention in the enclosed claims shall be held to incorporate, inter alia, a case where the host processing device is a first portion (the motherboard 15) of a desktop computer 10, laptop computer etc, and the remote processing device is a second portion of such a computer, namely an external or internal peripheral in the form of a hard disk 40, a floppy drive 54 or a modem 50. The inventive concept also embraces a case where several such peripherals are used concurrently as remote processing devices in conjunction with the host processing device and the inventive transaction apparatus 30.

[0028] Alternatively, the host processing device may be a first computer (such as the desktop computer 10 of FIG 2), while the remote processing device is any network client or server computer 62, 64, 66 connected to the first computer 10 over a network 60.

[0029] As already mentioned, the controller 31 and memory 33 of the transaction apparatus 30 form a transaction engine, which is programmed to apply a predefined data modification procedure to data contained in I/O transactions, which are exchanged between the host processing device and the remote processing device and are intercepted by the transaction apparatus 30.

[0030] The data modification procedure may be any data encryption/decryption algorithm generally known per se, which is applied for instance to all data exchanged as I/O transactions between the motherboard 15 of the host processing unit 10 and the local hard disk (remote processing device) 40. Asymmetric as well as symmetric data encryption/decryption algorithms may be used for implementing the predefined data modification procedure. Particularly if an asymmetric encryption/decryption algorithm is used, such as a Blowfish 128-448 bit encryption/decryption algorithm, a secret encryption/decryption key may advantageously be input by the user to the transaction apparatus 30 through a smartcard reader 52 and an associated smartcard. As shown in FIG 2, the smartcard reader 52 may be connected to the transaction apparatus 30 through a parallel interface port. Alternatively, a secret encryption/decryption key may be input by means of for instance a thumbprint reader or any other appropriate input device known from security and alarm applications.

[0031] FIG 3 illustrates a preferred embodiment of the invention. The electronic transaction apparatus 30 of FIG 3 is implemented as a PCI expansion card 300 to be inserted at a portion 330 into a PCI expansion slot in e.g. the desktop computer 10 of FIGs 1 and 2. Moreover, the electronic transaction apparatus 30 of FIG 3 is designed to perform high-security data encryption/decryption for a permanent storage device, such as the local hard disk 40 of FIGs 1 and 2.

[0032] The card 300 comprises an STPC Client 66 MHz integrated CPU, which is Intel 80x86 compatible and is commercially available from STMicroelectronics, Scotts Valley, California, USA. A 128 KB AM29F010 flash memory expansion ROM 312 (commercially available from Advanced Micro Devices, Sunnyvale, California, USA) is designed to take control over normal BIOS functions of the host processing device 10. Consequently, the ROM 312 is operatively connected via a PCI bridge circuit 314 (Intel 21554) both to the local

CPU 301 (over a local PCI bus 329) and to the host processing device 10 (over a host PCI bus 315).

[0033] An AM29F040 512 KB flash memory 302 (commercially available from Advanced Micro Devices, Sunnyvale, California, USA) stores a customized BIOS, a customized real-time MS-DOS compatible operating system as well as customized software for defining the predefined data modification procedure (data encryption/decryption algorithm). Flash memory 302 is supplemented by a DiskOnChip memory 303 (commercially available from M-Systems, Newark, California, USA) for storing application-specific software and data. Memories 302 and 303 are connected to CPU 301 over the local PCI bus 329 and a local ISA bus 318, respectively.

[0034] A floppy interface for connecting a floppy driver to be encrypted/decrypted is formed by an SMSC FDC37C67X chip 304 (commercially available from Standard Microsystems Corporation, Hauppauge, New York, USA), a floppy header 308 and a bus 317.

[0035] Similarly, an IDE interface for connecting a hard disk (e.g. hard disk 40 of FIGs 1 and 2) to be encrypted/decrypted is formed by IDE channel connectors 306-307 and a local IDE bus 319.

[0036] A network interface is formed by an AMD PCnet-FAST III network chip 305 (commercially available from Advanced Micro Devices, Sunnyvale, California, USA), an RJ45 connector 311a, an AUI port 311b and a bus 316. The network interface may be used for encrypting/decrypting network traffic to other network clients or servers across a given network (c.f. reference numerals 56, 60, 62, 64 and 66 in FIG 2).

[0037] An authentication input device (such as the smartcard reader or thumbprint reader referred to above) may be connected at a parallel port 309 or a serial port 313. A modem may be connected at a serial port 310.

[0038] Card 300 also comprises a keyboard connector 320, a mouse connector 321, a VGA interface 322, 323 and four SIM sockets 324-327 for providing RAM memory access for CPU 301 over a DRAM interface 328.

[0039] The operation of the transaction apparatus 30/300 of FIG 3 is as follows. An emulating interface is formed by expansion ROM 312 and the host PCI bus 315. I/O transactions between the host processing device 10 (motherboard 15 of desktop computer 10) and the remote processing device 40 (local hard disk) will be intercepted by software in the expansion ROM 312 and transmitted across the PCI bridge 314 to the local CPU 301, where the data in the I/O transaction will be processed according to the predefined data modification procedure for performing the data encryption/decryption.

[0040] Assuming that an IDE hard disk 40, a network connection to any networked computer 62-66 and a modem 50 are all to be protected by data encryption/decryption, the following measures will have to be taken initially. First, the hard disk 40 is connected at e.g. the first IDE channel connector 306. Then, the network 60 is connected to e.g. the RJ45 connector 311a, and the modem 50 is connected to the serial port 310.

[0041] Whenever a write operation is to be made to the hard disk 40, the I/O transaction will be intercepted by software in the expansion ROM 312, which will forward the transaction across the PCI bridge 314 to the local CPU 301. CPU 301 executes a data encryption/decryption program stored in memory 302, wherein the write data of the I/O transaction will be encrypted. The I/O transaction is then retransmitted to the hard disk 40, which will perform the write operation without noticing that the data thereof has been encrypted. Finally, CPU 301 notifies the software in the expansion ROM 312 that the transaction has been completed.

[0042] A read operation from the hard disk 40 is carried out in an essentially reversed manner, with the obvious difference that data is decrypted by the transaction apparatus 30/300 rather than encrypted.

[0043] With the embodiment described above, no performance losses will be experienced by the desktop computer 10, since the real-time operating system of the transaction apparatus 30/300 is optimized for I/O processing. In fact, the apparatus 30/300 will provide an acceleration in performance for the operating system of the desktop computer 10 when accessing the hard disk 40, despite the fact that data is actually encrypted/decrypted in the process. The reason for this is that the transaction apparatus 30/300 will act as a disk cache in this respect. During repeated reading of disk sectors, sectors that are close to the ones actually requested may be prematurely read, decrypted and stored in memory in the apparatus 30/300 and therefore be prepared for immediate transfer to the desktop computer 10, whenever the request is made.

[0044] The transaction apparatus 30/300 may additionally be used for authenticating purposes, wherein a smartcard reader may be connected at the parallel port 309 or serial port 313. An initialization routine is invoked in the expansion ROM 312 by the ordinary BIOS of host processing device 10. The initialization routine will preferably prompt the user for a PIN code or other form of password.

[0045] Then the initialization routine will call the software of CPU 301 via the PCI bridge 314, wherein the entered PIN code or password will be verified by CPU 301 by comparing with data stored on the card 300 or, alternatively, a smartcard. The software of CPU 301 will notify the initialization routine in expansion ROM 312 of the outcome of the verification. If the verification fails, the host processing device 10 will be locked by the initialization routine.

[0046] The present invention has been described above with reference to a preferred embodiment. However, other embodiments than the illustrated one are equally possible within the scope of the invention, as is readily realized by a man skilled in the art. Specifically, all references above to hard disks are applicable to any

permanent read/write data storage device comprising a magnetic, optical, magneto-optical or electronic storage medium.

Claims

1. An electronic transaction apparatus (30) for use together with a host processing device (10) and at least one remote processing device (40), where the host processing device and the remote processing device each has a processing unit (11, 41) and an interface (12, 42) and is capable of communicating I/O transactions according to a predefined protocol (20a-b) through the interface,
characterized in that

   the electronic transaction apparatus comprises programmable controller means (31), memory means (33) for storing a data modification procedure, first interface means (32) to be connected to the interface (12) of the host processing device (10) and second interface means (34) to be connected to the interface (42) of the remote processing device (40), wherein the controller means is programmed to perform the following actions by executing program instructions stored in the memory means:
   intercepting an I/O transaction, which has been transmitted by either the host processing device or the remote processing device and is destined to the other,
   modifying data contained in the intercepted I/O transaction in accordance with the data modification procedure stored in the memory means, and
   retransmitting the intercepted I/O transaction, with its modified data and according to the predefined protocol, to either the remote processing device, in case the I/O transaction was destined to the remote processing device when intercepted, or the host processing device, in case the I/O transaction was destined to the host processing device when intercepted.

2. An apparatus as in claim 1, wherein the host processing device (10) is any commercially available computer and the remote processing device (40) is any commercially available external computer peripheral (50).

3. An apparatus as in claim 1, wherein the host processing device (10) is any commercially available computer, the processing unit (11) of the host processing device is a CPU in said computer, and the remote processing device (40) is an I/O device (40, 54) within said computer.

4. An apparatus as in any preceding claim, wherein the remote processing device (40) is a permanent read/write data storage device (40, 54) comprising a magnetic, optical, magnetooptical or electronic storage medium.

5. An apparatus as in claim 4, wherein the predefined protocol is IDE or any protocol which is compatible with IDE.

6. An apparatus as in claim 4 or 5, wherein the remote processing device (40) is a hard disk and the processing unit thereof is a disk controller (41).

7. An apparatus as in claim 2 or 3, wherein the remote processing device is a modem (50).

8. An apparatus as in claim 1, wherein the host processing device (10) and the remote processing device (62-66) are any commercially available computers operatively interconnected over any network (60) known per se.

9. An apparatus as in any preceding claim, further comprising at least one of a real-time operating system and a BIOS stored in the memory means (302).

10. An apparatus as in any preceding claim, wherein the data modification procedure incorporates a data encryption/decryption algorithm generally known per se.

11. An apparatus as in any preceding claim, wherein the data modification procedure incorporates a data conversion method generally known per se.

12. An apparatus as in any preceding claim, wherein the data modification procedure incorporates an interface emulation method, preferably for converting between SCSI and IDE, between IDE and SCSI or between USB and IDE.

13. An apparatus as in any preceding claim, wherein the data modification procedure incorporates an authenticating method.

14. An apparatus as in any preceding claim, adapted to be connected to plural remote processing devices (40, 50, 54, 62-66).

15. An apparatus as in claim 10, wherein data encryption is applied to I/O transactions which are destined to the remote processing device (40), and wherein data decryption is applied to I/O transactions which are destined to the host processing device (10).

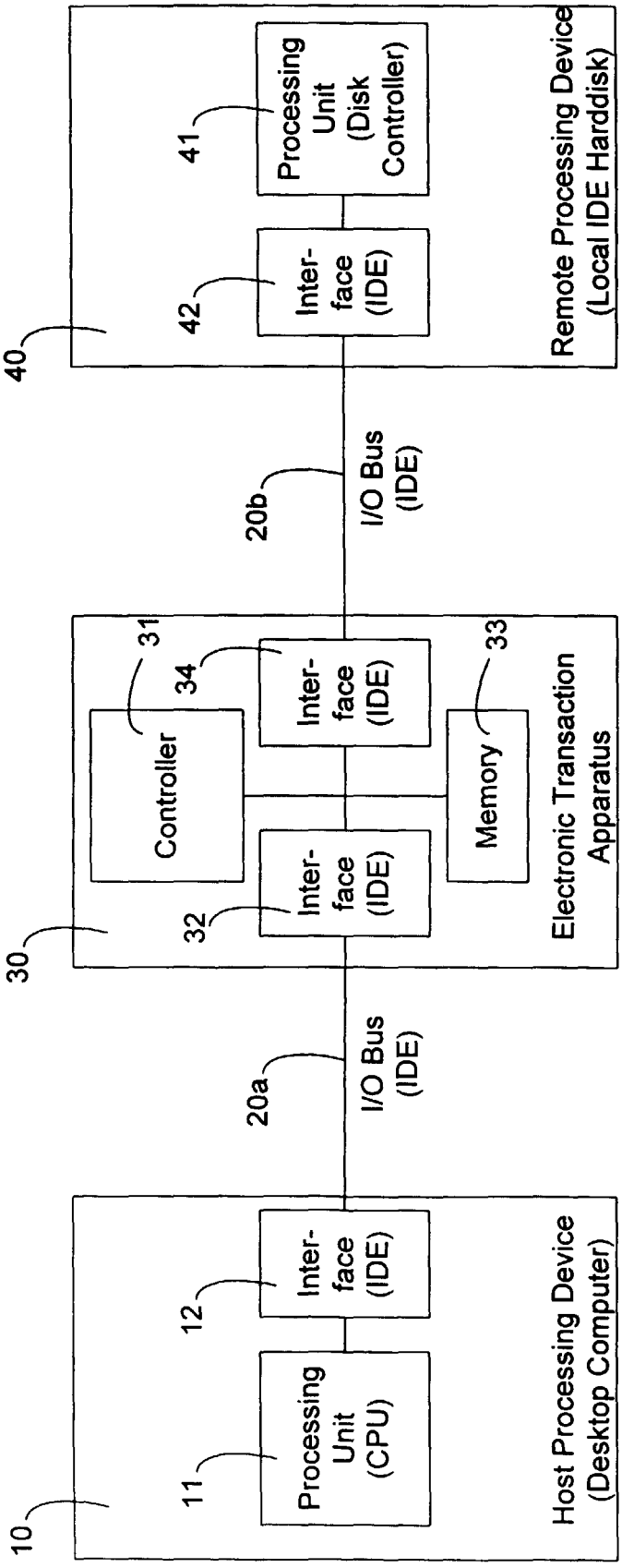
Host Processing Device
(Desktop Computer)
Processing
Unit
(CPU)
Inter-
face
(IDE)
Electronic Transaction
Apparatus
Controller
Inter-
face
(IDE)
Inter-
face
(IDE)
Memory
Remote Processing Device
(Local IDE Harddisk)
Processing
Unit
(Disk
Controller)
Inter-
face
(IDE)
I/O Bus
(IDE)
I/O Bus
(IDE)
10
11
12
30
31
32
33
34
20a
20b
40
41
42

Fig 1

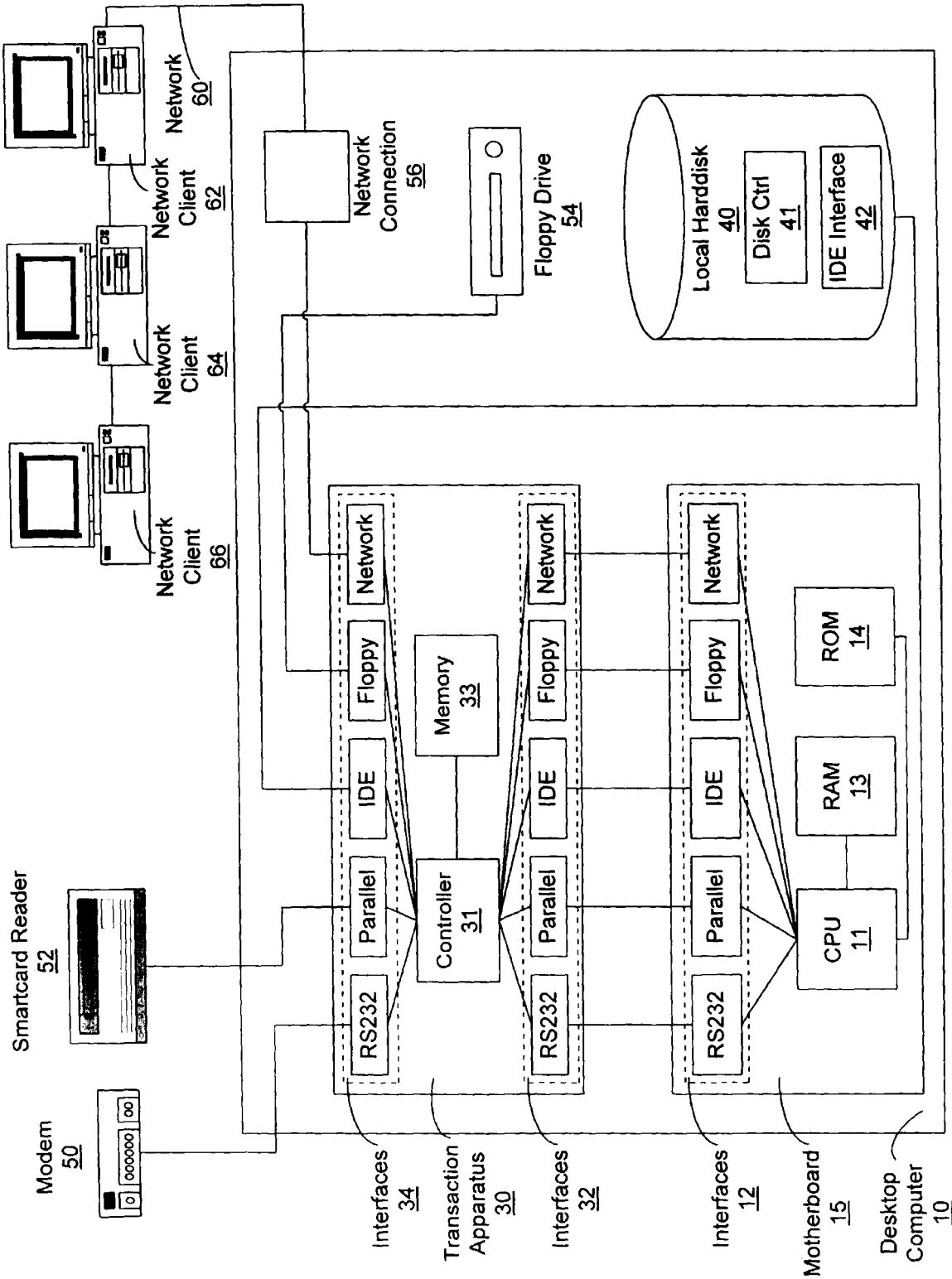
Network
60
Network
Client
62
Network
Client
64
Network
Client
66
Network
Connection
56
Floppy Drive
54
Local Harddisk
40
Disk Ctrl
41
IDE Interface
42
Smartcard Reader
52
Modem
50
RS232
Parallel
IDE
Floppy
Network
Controller
31
Memory
33
CPU
11
RAM
13
ROM
14
Interfaces
34
Transaction
Apparatus
30
Interfaces
32
Interfaces
12
Motherboard
15
Desktop
Computer
10

Fig 2

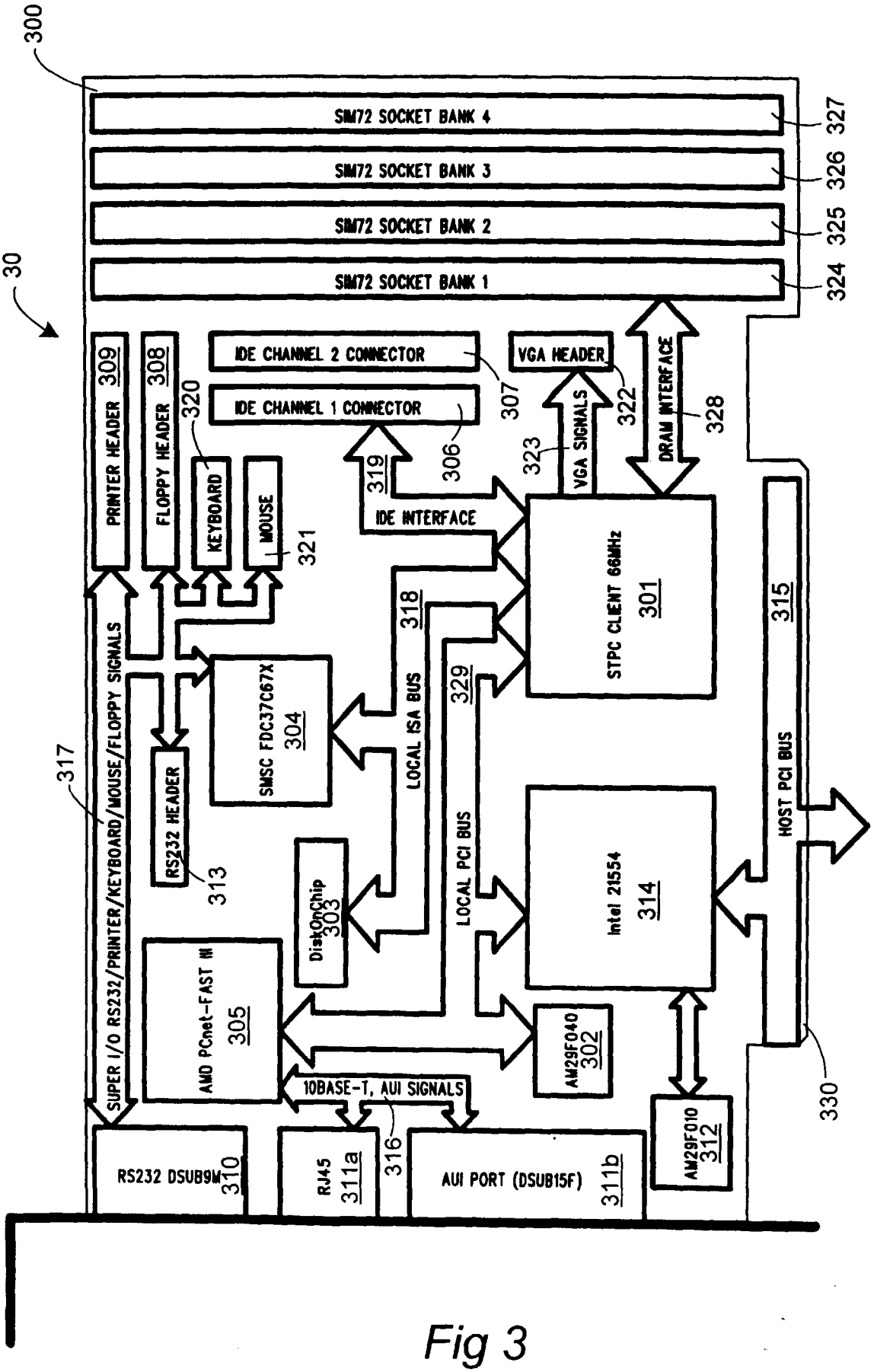
300
30
SIM72 SOCKET BANK 4
SIM72 SOCKET BANK 3
SIM72 SOCKET BANK 2
SIM72 SOCKET BANK 1
327
326
325
324
IDE CHANNEL 2 CONNECTOR
IDE CHANNEL 1 CONNECTOR
307
306
VGA HEADER
322
VGA SIGNALS
323
DRAM INTERFACE
328
PRINTER HEADER 309
FLOPPY HEADER 308
320
KEYBOARD
MOUSE
321
319
IDE INTERFACE
STPC CLIENT 66MHz
301
315
318
329
LOCAL ISA BUS
LOCAL PCI BUS
HOST PCI BUS
SMSC FDC37C67X
304
317
SUPER I/O RS232/PRINTER/KEYBOARD/MOUSE/FLOPPY SIGNALS
RS232 HEADER
313
DiskOnChip
303
Intel 21554
314
AMD PCnet-FAST III
305
AM29F040
302
10BASE-T, AUI SIGNALS
316
330
RS232 DSUB9M
310
RJ45
311a
AUI PORT (DSUB15F)
311b
AM29F010
312

Fig 3