(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
03 October 2019 (03.10.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/186536 A1

(51) International Patent Classification:
G06F 21/85 (2013.01) *G06F 21/83* (2013.01)
H04L 9/32 (2006.01) *G06F 21/84* (2013.01)
G06F 21/60 (2013.01) *G06F 21/82* (2013.01)

(21) International Application Number:
PCT/IL2019/050332

(22) International Filing Date:
25 March 2019 (25.03.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
258379 26 March 2018 (26.03.2018) IL

(71) Applicant: **KAZUAR ADVANCED TECHNOLOGIES LTD.** [IL/IL]; 126 Yigal Alon St., Tel-Aviv 6744332 (IL).

(72) Inventors: **FINCHELSTEIN, Daniel Mondy**; 10 Hahityashvut Street, 7583160 Rishon Lezion (IL). **PORAT, Yuval Moshe**; 20 Sderot Smuts Street, 6200932 Tel Aviv-Yafo (IL). **MARCO, Shlomi Raz**; 22 Ayalon Street, 4485100 Alfei Menashe (IL).

(74) Agent: **HAUSMAN, Ehud**; REINHOLD COHN AND PARTNERS, P.O. Box 13239, 6113102 Tel Aviv (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report (Art. 21(3))*

(54) Title: REMOTE SECURED TERMINAL

(57) Abstract: A computer implemented method for providing communication between a secured client computer and a remote computer. There is provided a client computer that includes peripheral components. Each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other peripheral components. The processor of each peripheral component is further configured to code the corresponding data of the specified data type. Each peripheral component is configured, by the processor, to establish a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with the client computer, and is further configured to code data that is communicated between the authorized remote computer and the peripheral component through the secured communication channel. The coded data being indecryptable by the processors of other of the peripheral components.

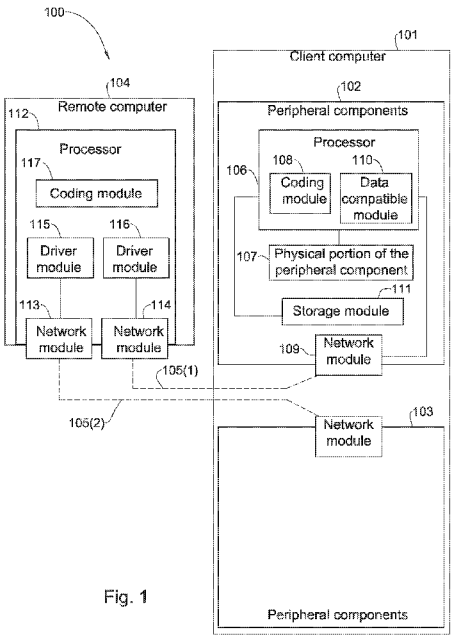


Fig. 1

WO 2019/186536 A1

REMOTE SECURED TERMINAL

TECHNICAL FIELD

The presently disclosed subject matter relates to remote secured terminals.

BACKGROUND

The ever-increasing usage of cloud-based services has increased the challenge of secured client computers (e.g. remote desktop, laptop, cellular phone and so forth) operating vis-à-vis the remote server (which may reside in the cloud) for achieving both transport security (such as a secured tunnel) and payload security (namely the content transmitted to and from the client computer and the remote server). In order to reduce or eliminate compromising of the client computer (which may adversely affect the transport security and/or the payload security), various approaches have been presented.

For instance, client computers that incorporate Intel® Skylake™ as well as later-introduced platforms, utilize the "Intel Software Guard Extension" (SGX)™ solution which is a new mode of execution of the CPU that creates an enclaved secured environment that can co-exist and co-execute with other codes such as untrusted OS (Open Source) code. The enclaved secured environment will maintain a high level of security, even if peripheral components of the client computer (such as keyboard, screen, camera and so forth) are compromised.

One of the limitations of the specified SGX™ solution is that it operates only with a given specific vendor and platform version.

SUMMARY OF THE INVENTION

In accordance with an aspect of the presently disclosed subject matter, there is presented a computer implemented method for providing communication between a secured client computer and a remote computer, comprising:

(a) providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of the at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of the data type;

the method further comprising with respect to each peripheral component of the components, by the processor:

(b) establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with the client computer; and

(c) coding data that is communicated between the authorized remote computer and the peripheral component through the secured communication channel, the coded data being undecryptable by the processors of other of the peripheral components.

In accordance with an embodiment of the presently disclosed subject matter, there is further presented a method, wherein stage (b) further includes:

i. authenticating the remote computer using a non-symmetric key that includes a public key of the remote computer;
ii. authenticating the peripheral component using a non-symmetric key that includes a private key known to the peripheral component;
iii. establishing a communication key known to the authenticated remote computer and the authenticated peripheral component,

the communication key being usable for the data coding between the client computer and the remote computer.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method wherein the coding data for communicating through the secured communication channel includes:

iv. encrypting data for transmission through the secured communication channel; or
v. decrypting data received through the secured communication channel.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method, wherein two of the at least two peripherals being keyboard and display respectively, and wherein the processor in the keyboard is configured to process corresponding data of keystrokes data type and the processor in the display is configured to process corresponding data of display data type.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method, wherein the client computer is devoid of a processor module that is separated from any of the at least two peripheral components and wherein the communication between the client computer and remote computer is achieved by means of the at least two peripheral components.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method, wherein the client computer further includes a processor module that is susceptible of being compromised and further being separated from any of the at least two peripheral components; and wherein stage (b) further includes:

establishing a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer to peer communication channel is established between the processor module and the remote computer.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method, wherein stage (c), further comprises:

C1 coding the data giving rise to coded data;

C2 transmitting the coded data to the processor module through the secured communication channel; and

for transmitting the coded data from the processor module to the authorized remote computer through the secured processor/remote computer communication channel; the coded data is not decryptable by the processor module that is susceptible to being compromised, thereby achieving secured communication between the peripheral component and authenticated remote computer irrespective of the utilization of the processor module.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method wherein for at least one group of the peripheral components, the processor is capable of translating data of a first data type associated with one module of the group to data of a second non compatible type of the other module of the group; the method further comprising:

d) establishing a secured peer to peer communication channel with other peripheral component of the group of peripheral components;

e) coding data for communicating between the one peripheral component through the secured communication channel with the other peripheral component; the coded data is undecryptable by other of the peripheral components apart from the group; and

f) translating data of the first type to a data of the second type or *vice versa*, thereby facilitating communication between the group of peripheral components in a common data type.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method, wherein the authenticated remote computer resides in the cloud.

In accordance with an aspect of the presently disclosed subject matter, there is yet further presented a computer implemented method for providing a communication between a secured client computer and a remote computer comprising:

providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by processor of other of the at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of the data type; the client computer further includes a processor module that is susceptible of being compromised and further being separated from any of the at least two peripheral components; the method further comprising with respect to each peripheral component of the modules:

establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with the client computer; the establishing secured communication channel includes establishing a communication key known to the remote computer and the peripheral component, the communication key is usable for the data coding between the peripheral component and the remote component;

establishing a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer to peer communication channel is established between the processor module and the remote computer.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method, further comprising: coding data giving rise to coded data; transmitting the coded data to the processor module through the secured communication channel; and for transmitting the coded data from the processor module to the authorized remote computer through the secured processor/remote computer communication channel; the coded data is not decryptable by the processor module that is susceptible to being compromised, thereby achieving secured communication between the client computer and authenticated remote computer, irrespective of the utilization of said processor module that is susceptible of being compromised.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a method, further comprising: receiving by the processor module providing coded data transmitted by the authorized remote computer through the secured processor/remote computer communication channel; the coded data is not decryptable by the processor module, receiving the coded data by the peripheral component through a corresponding secured communication channel, and by the processor of the peripheral component, decrypting the coded data, thereby achieving secured communication between the peripheral component and authorized remote computer, irrespective of the utilization of the processor module , irrespective of the utilization of the processor module that is susceptible of being compromised.

In accordance with an aspect of the presently disclosed subject matter, there is yet further presented a computer implemented method for providing a secured client computer, comprising: a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of the at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of the data type; wherein for at least one group of the peripheral components, the processor is capable of translating data of a first data type associated with one module of the group to data of a second non compatible type of the other module of the group, the method further comprising:

a. establishing a secured peer-to-peer communication with other peripheral component of the group of peripheral components;

b. coding data for communicating between the one peripheral component through the secured communication channel with the other peripheral component; said coded data is undecryptable by other of the peripheral components apart from the group;

c. translating data of the first type to a data of the second type or *vice versa*, thereby facilitating communication between the group of peripheral components in a common data type.

In accordance with an aspect of the presently disclosed subject matter, there is yet further presented a computer implemented system for providing communication between a secured client computer and a remote computer, comprising:

a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of the at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of the data type;

each peripheral component of the components, by the processor is configured :

to establish a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with the client computer; and

to code data that is communicated between the authorized remote computer and the peripheral component through the secured communication channel, the coded data being undecryptable by the processors of the peripheral components.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a system, wherein the client computer is devoid of a processor module that is separated from any of the at least two peripheral components and wherein the communication between the client computer and remote computer is achieved by means of the at least two peripheral components.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a system, wherein the processor of the authenticated remote computer is configured to receive, from a first authenticated peripheral component of the components and through a corresponding first trusted channel, a coded data of a first data type, decoding it using a first communication key associated with the first peripheral component and translating it to a processable data; the processor is further configured to translate processable data to data of a second data type, code it with a second communication key associated with a second authenticated peripheral

component and transmit it through a corresponding second trusted channel to the second authenticated peripheral component.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a system, wherein the authenticated remote computer resides in the cloud.

In accordance with an aspect of the presently disclosed subject matter, there is yet further presented a computer implemented system for providing a communication between a secured client computer and a remote computer comprising:

a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by processor of other of the at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of the data type; the client computer further includes a processor module that is susceptible of being compromised and further being separated from any of the at least two peripheral components;

each peripheral component of the components, by the processor is configured: to establish a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with the client computer, including establishing a communication key known to the remote computer and the peripheral component, the communication key is usable for the data coding between the peripheral component and the remote component;

to establish a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer to peer communication channel is established between the processor module and the remote computer.

In accordance with an aspect of the presently disclosed subject matter, there is yet further presented a computer implemented system for providing a secured client computer, comprising:

a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of the at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of the data type; wherein for at least one group of the peripheral components, the processor is capable of translating data of a first data type associated with one component of the group to data of a second non compatible type of the other component of the group,

a peripheral component of said components, by the processor is configured :

to establish a secured peer-to-peer communication with other peripheral component of the group of peripheral components;

to code data for communicating between the one peripheral component through the secured communication channel with the other peripheral component; the coded data is undecryptable by other of the peripheral components apart from the group;

to translate data of the first type to a data of the second type or *vice versa*, thereby facilitating communication between the group of peripheral components in a common data type.

In accordance with an embodiment of the presently disclosed subject matter, there is yet further presented a non-transitory computer-readable memory tangibly embodying a program of instructions executable by the computer for executing the method stages of the various embodiments of the presently disclosed subject matter.

Embodiments that are described within the context of an aspect of the invention may likewise be applied to other aspects of the invention, *mutatis mutandis*.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to understand the invention and to see how it can be carried out in practice, embodiments will be described, by way of non-limiting examples, with reference to the accompanying drawings, in which:

Fig. 1 illustrates a functional block diagram of a system for providing a secured client computer, in accordance with certain embodiments of the presently disclosed subject matter;

Fig. 2 illustrates a functional block diagram of a System On Chip (SOC) in accordance with certain embodiments of the presently disclosed subject matter;

Fig. 3 illustrates a generalized flow-chart of a sequence of operations in a system of Fig. 1, in accordance with certain embodiments of the presently disclosed subject matter;

Fig. 4 illustrates flow chart of a sequence of operations of establishing a secured communication channel, between a peripheral component and a remote computer, in accordance with the presently disclosed subject matter;

Fig. 5 illustrates a functional block diagram of a system for providing a secured client computer, in accordance with certain embodiments of another aspect of the presently disclosed subject matter;

Fig. 6 illustrates a generalized flow-chart of a sequence of operations for generating a secured communication channel in a system of Fig. 5, in accordance with certain embodiments of the presently disclosed subject matter;

Fig. 7 illustrates a sequence of operations for utilizing the secured communication channels established e.g. in accordance with the flow chart of Fig. 6, in accordance with certain embodiments of the presently disclosed subject matter;

Fig. 8 illustrates a sequence of operations for utilizing the secured communication channels established e.g. in accordance with the flow chart of Fig. 6, in accordance with certain other embodiments the presently disclosed subject matter;

Fig. 9 illustrates a functional block diagram of a system for providing a secured client computer, in accordance with certain embodiments of yet another aspect of the presently disclosed subject matter;

Fig. 10 illustrates a generalized flow-chart of a sequence of operations for generating a secured communication channel in a system of Fig. 9, in accordance with certain embodiments of the presently disclosed subject matter; and

Fig. 11 illustrates a sequence of operations for utilizing the secured communication channels established e.g. in accordance with the flow chart of Fig. 9, in accordance with certain embodiments of the presently disclosed subject matter.

DETAILED DESCRIPTION

In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that the presently disclosed subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, modules and circuits have not been described in detail so as not to obscure the presently disclosed subject matter.

Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "authenticating", communicating", "transmitting", "coding", translating", "facilitating", "providing", "establishing", "processing", "computing", "representing", "comparing", "generating", "assessing", "matching", "updating" or the like, refer to the action(s) and/or process(es) of a computer that manipulate and/or transform data into other data, said data represented as physical, such as electronic, quantities and/or said data representing the physical objects. The term computer or processor should be expansively construed to cover any kind of hardware-based electronic device or devices with data processing capabilities including, by way of non-limiting example client computer, remote computer, processor, the processor module discussed herein.

The term "non-transitory storage medium" used herein should be expansively construed to cover any volatile or non-volatile computer memory suitable to the presently disclosed subject matter.

The operations in accordance with the teachings herein may be performed by a computer specially constructed for the desired purposes, or by a general-purpose computer specially configured for the desired purpose, by a computer program stored in a non-transitory computer-readable storage medium.

Embodiments of the presently disclosed subject matter are not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the presently disclosed subject matter as described herein.

Bearing this in mind, attention is drawn to **Fig. 1** illustrating a functional block diagram of a system in accordance with certain embodiments of the presently disclosed subject matter. The illustrated system **100** includes a client computer **101** that by this example may include two peripheral components **102** and **103**. The client computer may be coupled to a remote computer **104** (e.g. a server residing in the cloud) through a known *per se* network (designated collectively as **105**) and is configured to provide a secured communication between the peripheral components and the remote computer **104**. Non-limiting examples of peripheral components are input components such as keyboard microphone, tracking device or combination thereof (e.g. keyboard and mouse). , output components such as display components and/or others (not necessarily input or output. Each peripheral component is configured to process a corresponding peripheral component data of a given data type. For instance, in the case of a keyboard component, the data type may be keystroke related data such as scan code or key code . Note that the data type associated with a given peripheral component (e.g. keyboard) may be different than that of one (or more than one) of other peripheral component(s) (e.g. display). In accordance with certain embodiments, there may be other two or more peripheral components (either of identical type, say two keyboards or of different types) whose data type are compatible, one with the other. In accordance with certain embodiments, the physical portion of the peripheral component **107** (e.g. screen in case of display, the physical keyboard keystrokes and the pertinent electronics/hardware) may be associated with a processor **106** for generating and processing data including the specified data type.

The processor **106** may be configured to execute a coding module **108** for coding the corresponding data of the specified data type, all as will be explained in greater detail below. The network module is configured to facilitate communication, e.g. with remote computer **104**. As will be further discussed below, the processor may be configured to execute data compatible module **110** (e.g. a driver) for translating data of a given data type, to another type which may be compatible with the other data type. Fig. 1 further illustrates storage module **111** (non-transitory computer-readable storage medium) for storing data such as private keys, all as will be explained in greater detail below.

The coding module **108** as well as the network module **109** (the latter may facilitate communication with the remote server **104** through network **105**) may reside on one or more System On Chips (SOCs), as will be explained with reference to Fig. 2 below.

Note that in accordance with certain embodiments, the peripheral components (in the example of Fig. 1 only 2 out of possibly N (N>2) are shown) may form part of a client computer **101** such as laptop, desktop, cellular device and others known *per se*, or in accordance with certain other two or more of the peripheral components may reside remotely and communicate by means of a network, thereby not necessarily residing in one physical client computer, all as known *per se*.

Peripheral component **103** may include similar blocks and modules *mutatis mutandis*. For instance, in cases where the peripheral component **103** is a display, the physical component 107 may be different and suitable for a display component.

Turning now to remote computer **104**, it includes a processor **112**, network modules **113** and **114** for communication with the respective peripherals **102** and **103**. The processor **112** may be configured to execute driver modules **114** and **115** that may form part of data compatibility module(s) for translating between non-compatible data types, e.g. the driver **115** may translate keystrokes data type received from the keyboard component **102** through network module **112** (via secured channel **105(1)**- all as will be discussed in greater detail below) for further processing by appropriate application module (not shown) running on processor **112**. Likewise, the driver **116** may translate output data processed by appropriate application module (not shown) running on processor **112** into display type data that will be transmitted through network

module **114** (via secured channel **105(2)**, all as will be discussed in greater detail below) to display component **103**. In cases where the communicated data to the remote server is coded e.g. encrypted (as will be explained in greater detail below), the remote computer may utilize the coding module **117** for, e.g. decrypting the data and/or *vice versa* for encrypting data that will be decoded by the coding module of the peripheral component. The processor is operatively coupled to a storage module (non-transitory computer- readable storage medium) - not shown in Fig. 1.

The invention is not bound by the specified architecture of the remote computer, which is provided by way of example only and any known *per se* architecture may be applicable.

Note also that whereas in the embodiments of Fig. 1, the peripheral components are accommodated in a one local client computer 101, this is not necessarily always the case, and accordingly two or more of the components may communicate through a network and therefore may not necessarily reside in the same physical location. Thus, in accordance with certain embodiments the client computer may be a local computer residing in one location, or in accordance with other embodiments not necessarily residing in one location.

Turning now to Fig. 2, this illustrates a functional block diagram of a more detailed System On Chip (SOC) **200** in accordance with certain embodiments of the presently disclosed subject matter. Thus, SOC **200** may include the processor **106** that is configured to execute data compatibility module **110** including for example driver(s) . The processor may be further configured to the coding module that by this embodiment includes cryptographic semantics module **202** capable of performing cryptographic operations. The processor is operatively coupled to the storage **111** that includes by this example a Trusted Platform Module (TPM) **203** and External Source module **204** capable of reading external validation and configuration data (e.g. from smart card, Subkey and Nitrokey, etc.). The operations of the specified modules will be explained in greater detail below. The network module **205** may be for example a communication stack, utilizing one or more of 803.11X, Bluetooth (LE) Thunderbolt and so forth. While the description with reference to Fig. 1 utilizes one SOC, it may likewise use two or more SOCs which may collectively have similar or modified functionality as the one described with reference to Fig. 2.

Thus, with reference to Figs. 1, 2 above and 5 and 9 below, the processor (**106**) (or 112, whichever the case may be) can be configured to execute several functional modules in accordance with computer-readable instructions implemented on a non-transitory computer-readable storage medium.

It is noted that the teachings of the presently disclosed subject matter are not bound by the system and/or computer and /or processor system described with reference to **Fig. 1**. Equivalent and/or modified functionality can be consolidated or divided in another manner and can be implemented in any appropriate combination of software with firmware and/or hardware and executed on a suitable device. Those skilled in the art will also readily appreciate that the data storage can be consolidated or divided in another manner; databases can be shared with other systems or be provided by other systems, including third party equipment.

For purpose of illustration only, the following description is provided for establishing secured communication between peripheral components. Those skilled in the art will readily appreciate that the teachings of the presently disclosed subject matter are, likewise, applicable to secured communication between peripheral component(s) and remote computer(s).

Bearing this in mind, attention is drawn to Fig. 3 illustrating a generalized flow-chart of a sequence of operations for establishing secured communication between the remote commuter (say **104** of Fig.) and one or more peripheral components say **102** and/or **103** (which resides, or not, in the same client's computer), in accordance with certain embodiments of the presently disclosed subject matter. Thus, at the onset, the peripheral component may establish a secured peer-to-peer communication channel between the peripheral component and the remote server computer that is authorized to communicate with the peripheral component (**301**). This may generate a secured channel (e.g. tunnel) and facilitate communication of a secured payload (e.g. the coded data) through the secured tunnel. In the example of Fig. 1, and assuming that the peripheral component **102** is for example a keyboard, the secured communication channel is depicted schematically as $\mathbf{105}_1$. As a result the communication channel between the peripheral component is secured as well as the content (even if theoretically the communication channel is compromised).

Next, the peripheral component may utilize **302** said coding module to code data that is communicated between the authorized remote server (e.g. **104**) and the peripheral component through said secured communication tunnel, said coded data (e.g. the specified coded payload) being undecryptable by the coding modules of other (in accordance with certain embodiments all other) of said peripheral components. The term un (or not or cannot etc.) decipherable (or decryptable) used herein should be construed to include: cannot be deciphered (decryptable) by using reasonably available processing power, for instance using at least 2048 bits for non-symmetric key or at least 256 bits for symmetric key. These values may vary depending upon the available reasonable processing power which is likely to improve over time.

Turning now to Fig. 4, this illustrates a flow chart of a sequence of operations of establishing a secured communication channel between a peripheral component and a remote computer that was discussed in Fig. 3, in accordance with certain embodiments of the invention. Thus, in **401** the peripheral component, say **102,** may authenticate the remote server using a non-symmetric key that includes a private key known to only the remote server. More specifically, the remote server may send a message signed by its private key, and the peripheral component may extract the corresponding public key of the remote server (extracted e.g. from external trusted source) and decipher, (using the remote server's public key), the so-encrypted message, thereby authenticating the remote server.

Then, **402** the peripheral component, using a non-symmetric key that includes a private key known to the peripheral component (and extracted e.g. from the TPM)-[and possibly known to only the peripheral component], may encrypt the message and the remote computer may then decipher the message using a corresponding public key of this particular peripheral component, thereby authenticating the peripheral component. Once dual authentication has been achieved, a secured peer-to-peer communication channel between the client computer and the remote server is established.

Note that throughout the description and Claims, encrypting using a non-symmetric key (e.g. a private key) may be construed as an example of "signing" and decryption (deciphering) using a corresponding non-symmetric key (e.g. public key) may be construed as an example of "verification".

Then, in **403** a communication key (e.g. a symmetric key) known to the authenticated remote server and the authenticated peripheral component (and possibly not to other peripheral components), is generated. The symmetric key is usable for the data coding between the client computer and the remote server. By one example, in order to establish the communication key, the peripheral component may extract proprietary data from either or both of the TPM **203** and from the external source data **204**, and combine them, thereby generating the communication key. The invention is not bound by this specific manner of generating the communication key.

In accordance with certain embodiments, in order to send the communication key to the authenticated remote server, the so generated communication key may be encrypted by the private key of the peripheral component and by the public key of the remote computer and transmitted from the authenticated peripheral component to the remote computer, through the already established secured channel (e.g. **105**) between them. Since the communication key was encrypted by the public key of the remote computer, this guarantees that only the already authenticated remote server (see stage **401**) can decipher it (using its corresponding private key, known only to it). The remote computer, in turn, will use the public key of the already authenticated peripheral component (see **401** above) in order to decipher and extract the communication key that was encrypted by the corresponding private key of the peripheral component. Thus, a communication key is established between the authenticated peripheral component and the authenticated remote computer and is known only to them for transmitting coded data (secured payload).

The invention is not bound by the specified manner of establishing the communication key. For instance, the procedure may commence from the remote computer which defines the communication key, encrypt it with its private key, and then with the public key of the authenticated peripheral component. The authenticated peripheral component, in turn, will use the authenticated remote computer public key and its own private key to decipher and extract the communication key, for transmitting code data and achieving secured payload.

The computational stages described above (at the peripheral component side) may be performed e.g. at the cryptographic semantic module **202 (Fig. 2)** running on processor **106**, and computational stages discussed above (with reference to the

remote computer) may be performed at coding module **117** running on processor **111** (**Fig. 1**).

Having established a secured communication key, it may be used **404** e.g. by the coding module **108** (e.g. cryptographic semantics module **202**) to code data communicated through the secured communication channel for achieving a secured payload. This may include encrypting data for transmission through said secured communication channel (e.g. tunnel) or decrypting data received through said secured communication tunnel.

The same holds true for the other peripheral component **103** (say a display) establishing a secured communication channel (depicted schematically as $\mathbf{105}_2$) with remote computer 104.

There follows a non-limiting example of a sequence of operations for establishing a secured communication between a keyboard peripheral component (where, as shown in Fig. 2, the physical component **107** represents a physical keypad and processor **106** processes the pertinent data and a remote server). The invention is of course not bound by this example.

a. **Keyboard - Client Side** (e.g. **102** in Fig.1)
    i. User plugs in external validation device (Smartcard, Nitrokey, etc.).
    ii. User authenticates to the device. (e.g. via biometric identification)
    iii. TPM (**203**) validates the state of the firmware, and, if valid, boots the firmware.
    iv. Firmware reads configuration data from the external validation device (**204**).
    Configuration information includes (but is not limited to):
        1. Local network configuration and credentials
        2. Remote host configuration and credentials

    The specified stages (i) to (iv) illustrate in a non-limiting manner stages of validating the chip and

authenticating the user. Some of the data may be used for later stages for instance the address of the remote computer to be authenticated and/or user data – e.g. biometric data and/or user password that may form e.g. part of the communication key.

v. Firmware provisions the device based on currently read configuration (configuration information is transient in nature). Having validated the specific keyboard peripheral component, and having extracted the component's configuration and undergone component's initialization, then

vi. The keyboard component establishes a secured channel (by this example a secure transport (e.g. VPN)) to the remote computer (server), including authenticating the peripheral component and the remote computer as described with reference to Fig. 3 and 4 above (e.g. based on provided configuration data

vii. A symmetric key (an example of communication key) is generated between the authenticated devices, as discussed with reference to Fig. 3 and 4 above, including by this example keystrokes from the keyboard are read, encrypted to a second provided key (based on the same external key store). This is to create an end-to-end encryption (payload encryption) as well as transport encryption.

viii. Encrypted payload (an example of code data) is then transmitted (using the communication key) over the secure channel (tunnel) between the keyboard component and to the remote computer.

Note, that in accordance with certain embodiments, transport layer may be terminated at an edge device (e.g. firewall, VPN concentrator, etc.), however, it can be terminated at the host operating system level.

b. **Remote Computer Side** (e.g. **104** in Fig.1)

i. Transport Layer (e.g. VPN) established. This is the corresponding secured channel part (see (vi) at client side) that is performed at the remote computer side

ii. Client Device authenticated based on client provisioned keys. (Authenticating the keyboard peripheral – as discussed above).

iii. Upon successful authentication, a virtual device is presented to the remote computer Operating System - Virtual HID (Keyboard).

(iv) Coded data is received or transmitted using the so established communication (e.g. symmetric) key (which the remote computer has participated in its generation), as discussed before. For instance, Ingress encrypted payloads (e.g. using the specified symmetric key) are decrypted by a software driver resulting in non-encrypted standard scancode.

(v) Scancodes are delivered to the OS via the device's driver.

Bearing all this in mind, coded data may be exchanged between the authenticated remote server and a given authenticated peripheral component (say **102-** e.g. keyboard) through a secured channel (e.g. $\mathbf{105_1}$) where this coded data is not decipherable by any other peripheral components. By the same token, utilizing the specified sequence of Fig. 3 (and say the specific embodiment of Fig. 4) between the remote computer and a different peripheral component (say display **103**), coded data (typically of a different type) may be exchanged between the authenticated remote server and the different peripheral component through a different secured channel (e.g. $\mathbf{105_2}$) where the coded data designated to or having originated from a given authenticated peripheral component, is not decipherable by any other peripheral component.

Considering the non-limiting scenario that two or more secured peripheral components (in the manner specified) reside in the same local computer (or even peripherals not residing in the same physical location), then a secured local computer is achieved, which is significantly more secured than, say, a local computer that utilizes

a processor that is susceptible of being compromised such as general purpose processor, that may be inherently compromised by third party hacking. This definition of a processor that is susceptible of being compromised may encompass a processor (e.g. CPU) that does not include a system/feature to restrict access to memory sections for specific processes in a way that allows only these processes to access to that memory using specific commands that are implemented by the CPU. In such CPUs, the OS kernel is able to read the contents of the computation done on the CPU at that time, hence a compromised kernel will compromise any computation done on that CPU. The invention is not bound by this definition.

Moreover, in a local computer (or even peripherals not residing in the same physical location) in accordance with certain embodiments substantially no data is retained at the client side but rather only at the secured remote server (e.g. in the cloud).

This solution in accordance with certain embodiments is also less costly and more compatible than, say, a local computer that incorporates say, the Intel® Skylake™ and later-introduced platforms which utilize the "Intel Software Guard Extension" (SGX)™ for achieving a secured environment. The invention is not bound by the specified SGX ™.

This solution is also advantageous in accordance with certain embodiments by virtue of the fact that in order to have "full picture" of the activities at the client computer there may be a need to hack not only one peripheral components but rather all (or nearly all of them) which is harder due to the fact that each peripheral component is secured independently of the other.

In the architecture utilized for example in Fig. 1, that utilizes the teachings in accordance with various embodiments of the invention, the absence of "general purpose" processing capabilities in the client computer (employing just peripheral components) may be fulfilled by the processing capacity of the remote computer which may be for example a server residing on a remote protected cloud environment.

It is noted that the teachings of the presently disclosed subject matter are not bound, neither by the flow chart illustrated in Fig. 3 and 4 , nor by the specific modules illustrated in Figs. 1 and 2. For instance, the illustrated operations can occur out of the

illustrated order. Some of the operations may be executed substantially concurrently or in the reverse order.

Attention is now drawn to **Fig. 5** illustrating a functional block diagram of a system for providing a secured client computer, in accordance with another aspect of the presently disclosed subject matter. The peripheral components (e.g. **102** and **103** - and possibly others not shown in Fig. 5) as well as the remote computer **104** are similar to those described with reference to Figs. 1 and 2, and may be accommodated in client computer **101** which, by this embodiment, may include an additional processing capacity, for instance by employing a computer module **501** that is susceptible to being compromised. The latter may be for example a commercially available CPU fitted in a client computer, such as commercially available *Intel™ or AMD™* CPUs . The term susceptible to being compromised should be construed to include a processor which is susceptible of being compromised by applying reasonable third party hacking techniques and as defined by way of non-limiting example above. As readily arises from Fig. 5, the communication between the peripheral component and the remote computer passes through the computer module **501**, and by virtue of the characteristics of susceptible to being compromised computer module **501,** any data that originates from a peripheral component and the remote server or vice versa, cannot be considered as secured because it may be hacked at processor module **501**.

Accordingly, while processor module **501** may add computational capacity to the client computer (compared, for example, to the embodiment of Fig. 1), it is susceptible to being compromised, which is a clear disadvantage. There is thus provided a method for obtaining secured communication between a client computer and a remote server in an architecture that employs also a processor module that is susceptible to being compromised.

Accordingly, in accordance with certain embodiments, each of the peripheral components may establish a secured peer-to-peer communication channel between the peripheral component (say **102**) and a remote computer (say **104**) that is authorized to communicate therewith. To this end, a secured communication channel may be established (e.g. $\mathbf{105}_1$) that includes establishing a communication key (e.g. symmetric key) known to only the remote computer (**104**) and the peripheral component (**102**), and the communication key is usable for the data coding between the

peripheral component and the remote computer, all as explained in detail above with reference to Figs. 1 to 4.

Turning now to Fig. 6, this illustrates a generalized flow-chart of a sequence of operations for generating a secured communication channel in a system of Fig. 5, in accordance with certain embodiments of the presently disclosed subject matter.

For convenience, whenever the term processor module 501 is used, it should be meant to refer to a processor module that is susceptible to being compromised in the matter discussed above.

Thus, in **601** a secured peer-to-peer communication channel (say **502(1)**) is established between the peripheral component(say **102**) and processor module (say **501**). In **602** a secured processor/remote server peer-to-peer communication channel (say **503**) is established between the processor **501** and the remote computer **104**. In a similar fashion, in **601** a secured peer-to-peer communication channel (say **502(2)**) is established between the peripheral component(say **103**) and the processor module (say **501**). Generation of the specified secured communication channel includes authenticating the respective peripheral component (**102** and **103**) and the compute (**501**), thereby achieving a secured transport ((**502(1)** and (**502(2)**, respectively) in a similar *mutatis mutandis* process of establishing a secured transport channels (**105(1)** and **105(2)** as described in detail with reference to Fig. 1 and the pertinent flow chart of Figs. 3 and 4 .

Attention is now drawn to Fig. 7, illustrating a sequence of operations of utilizing the secured communication channels established e.g. in accordance with the flow chart of Fig. 6, in accordance with the presently disclosed subject matter.

More specifically , in **701** the coding module of the peripheral component (say **102**) may be utilized to code data (say coded keyboard strokes) designated to the remote computer. Then, in **702** the coded data may be transmitted to the processor module through the secured communication channel (e.g. **502(1)**). Then, the coded data may be transmitted **703** from the processor module to the authorized remote server (say **104**) through the already established secured processor/remote server communication channel **503**.

Note that the coded data (say the coded keystrokes) may not be decrypted by the processor module because the coded data was generated by using a communication key (say symmetric key) known to the peripheral component (say **102**) (and possibly only to the peripheral component and not other peripheral components) and the remote computer (say **104**), and, accordingly, even if the processor **501** is compromised and the coded data is intercepted within the processor **501**, it cannot be deciphered and therefore a secured communication between the client computer and authorized server computer (the remote computer) is achieved , irrespective of the utilization of said processor module.

With reference to Fig. 8, a sequence of operations of utilizing the secured communication channels in accordance with the presently disclosed subject matter is shown. In this example a coded data is communicated from the remote computer (e.g. **104**) to the peripheral component (e.g. display component **103**), including (in **801**) receiving in processor module **501** coded data transmitted by the authorized remote server **104** through said secured processor/remote server communication channel **503**. As explained above, the coded data may not be decrypted by the processor module.

In **802**, the coded data is transmitted from the processor **501** to the display peripheral component **103** through the secured communication channel 502_2.

Next, in **803** the coding module of the display peripheral component is utilized to decrypt said coded data, thereby achieving secured communication between the display peripheral and authorized server computer **104**, irrespective of the utilization of said processor module **501**.

Note that whereas the peripheral components exemplified in the first aspect (described with reference to Fig. 1) and the second aspect (described with reference to Fig. 5) where one-directional by nature keyboard outgoing and display incoming are used, in accordance with other embodiments, other bi-directional peripheral components may be used for sending and receiving coded data to and from the remote computer.

Note that in the context of Figs. 6 to 8 the term coded data should be construed to include, as variants thereof, e.g. including additional data added by the processor **501**.

Note also that in accordance with certain embodiments, the two architectures (e.g. of Fig. 1 and 5) may be combined, allowing the peripheral component to communicate directly with the remote computer or through the processor module, whichever the case may be, and likewise the remote computer may communicate directly with the peripheral component, or through the computer.

It is noted that the teachings of the presently disclosed subject matter are not bound by neither any of the flow charts illustrated in Figs. 6 to 8 , nor by the specific modules illustrated in Fig 5. For instance, the illustrated operations can occur out of the illustrated order. Some of the operations may be executed substantially concurrently or in the reverse order.

Turning now to another aspect of the invention, attention is drawn to Fig. 9 illustrating a functional block diagram of a system for providing a secured client computer, in accordance with certain embodiments of the presently disclosed subject matter.

The peripheral components (e.g. **102** and **103** - and possibly others not shown in Fig. 9) are similar to those described with reference to Figs. 1 and 2, and may be accommodated in client computer **101**. Note, that by this embodiment, the usage of a processor module that is susceptible of being compromised (e.g. **501** of Fig. 5) as well as a remote computer (e.g. **104**), may be obviated.

Accordingly, in accordance with certain embodiments, each of the peripheral components (say **103**) may establish a secured peer-to-peer communication channel (**901**) directly to another peripheral component (say **102**). An establishment of such a secured communication channel may include establishing of a communication key (e.g. a symmetric key) known to only the respective group of peripheral components . The communication key is usable for the data coding between the respective peripheral components, all as explained below.

Turning now to **Fig. 10**, it illustrates a generalized flow-chart of a sequence of operations in a system of Fig. 9, in accordance with certain embodiments of the presently disclosed subject matter.

At the onset, a secured peer-to-peer communication channel is established **(1001)** between the one peripheral component (say **102**) and the other peripheral component (**102**) of the group of peripheral modules.

Next **(1002)**, the coding module (see Fig. 2) of say peripheral component **102** may be utilized to code data that is communicated between the one peripheral component through the secured communication channel with said other peripheral component; the coded data is undecryptable by the coding modules of other (in accordance with certain embodiments all other) peripheral components (not shown in Fig. 9).

The data compatibility module (see **Fig. 3**) of either or both of the peripheral components of the group may be utilized **(1003)** to translate data of said first type to a data of said second type or vice versa, thereby facilitating communication between said peripheral components in a common data type.

With reference to **Fig. 11**, a sequence of operations of utilizing the secured communication channels in accordance with the presently disclosed subject matter is shown. In this example a coded data is communicated from the first peripheral (e.g. keyboard **102**) to the peripheral component (e.g. display component **103**) including (in **1101**) transmitting coded data through secured channel **901**.

Next, in **1102** the coding module of the display peripheral component is utilized to decrypt said coded data, thereby achieving secured communication between the display peripheral and keyboard peripheral **104**.

In either of the first and second peripherals of the group, a data compatibility module may be utilized **1103** to translate the data to a common data type (in the latter example, a keyboard and display).

Note that the coded data (say the coded keystrokes) may not be decrypted by any other peripheral component (apart from the other peripheral component in the

group) because the coded data was generated by using a communication key (say a symmetric key) known to the peripheral components (say **102** and **103**) and possibly only to them.

Note that the peripheral to peripheral secured communication channel facilitates direct secured communication not through a remote computer (as was with certain embodiments of the first aspect of the invention described with reference to Figs. 3 and 4 above). Consider, for example, a password that is keyed-in in the keyboard peripheral component (say **102**) and displayed at the display peripheral component (say **103**). By virtue of the so-obtained transport security and payload security, the likelihood of compromising any of the components or of the channel, is lower than non-secured components/channels, and, therefore, in accordance with certain embodiments of the third aspect of the invention, communication of sensitive data, such as passwords, is feasible even without utilizing the remote computer. In cases where the data types between the peripherals is non compatible - say keyboard related data type vs. display related data type, the data compatibility module (say a driver) may provide common data type for translating, for instance, keystrokes into displayed pixels)- all as known *per se*.

Note also that whereas the peripheral components exemplified in the first aspect (described with reference to Fig. 1) and the second aspect (described with reference to Fig. 5) and the third aspect (described with reference to Fig. 9) where they are one-directional by nature (keyboard outgoing and display incoming), other bi-directional peripheral components may be used for sending and receiving coded data to and from the remote computer.

Note also that in accordance with certain embodiments, the two architectures (e.g. of Fig. 1 and 9) may be combined, allowing the peripheral component to communicate with another peripheral component through the remote computer, and/or directly.

Note also that the description refers a group of peripheral components (e.g. in the context of secured communication channel or e.g. sharing communication key, etc.) it may apply to two peripheral components or in accordance with certain embodiments of the presently disclosed subject matter to more than two (say three or more). Likewise

whenever reference is made to peripheral component and remote computer it likewise applies in accordance with certain embodiments of the presently disclosed subject matter to two or more peripheral components and a remote computer e.g. in the context of secured communication channel or e.g. sharing communication key.

It is appreciated that certain features of the presently disclosed subject matter, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the presently disclosed subject matter, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub-combination.

Usage of conditional language, such as "may", "can", or variants thereof should be construed as conveying that one or more examples of the subject matter may include, while one or more other examples of the subject matter may not necessarily include, certain methods, procedures, components and features. Thus such conditional language is not generally intended to imply that a particular described method, procedure, component or circuit is necessarily included in all examples of the subject matter. Moreover, the usage of non-conditional language does not necessarily imply that a particular described method, procedure, component or circuit is necessarily included in all examples of the subject matter.

It is to be understood that the invention is not limited in its application to the details set forth in the description contained herein or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Hence, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting. As such, those skilled in the art will appreciate that the conception upon which this disclosure is based may readily be utilized as a basis for designing other structures, methods, and systems for carrying out the several purposes of the presently disclosed subject matter.

It will also be understood that the system according to the invention may be, at least partly, implemented on a suitably programmed computer. Likewise, the invention contemplates a computer program being readable by a computer for executing the

method of the invention. The invention further contemplates a non-transitory computer-readable memory tangibly embodying a program of instructions executable by the computer for executing the method of the invention.

Those skilled in the art will readily appreciate that various modifications and changes can be applied to the embodiments of the invention as hereinbefore described without departing from its scope, defined in and by the appended claims.

CLAIMS

1. A computer implemented method for providing communication between a secured client computer and a remote computer, comprising:

(a) providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type;

the method further comprising with respect to each peripheral component of said components, by said processor:

(b) establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; and

(c) coding data that is communicated between the authorized remote computer and the peripheral component through said secured communication channel, said coded data being indecryptable by the processors of other of said peripheral components.

2. The method according to Claim 1, wherein said stage (b) further includes:
   i. authenticating the remote computer using a non-symmetric key that includes a public key of the remote computer;
   ii. authenticating the peripheral component using a non-symmetric key that includes a private key known to the peripheral component;
   iii. establishing a communication key known to the authenticated remote computer and the authenticated peripheral component, the communication key being usable for the data coding between the client computer and the remote computer.
3. The method according to Claims 1 or 2 wherein said coding data for communicating through said secured communication channel includes:

i. encrypting data for transmission through said secured communication channel; or

ii. decrypting data received through said secured communication channel.

4. The method according to any one of the preceding Claims, wherein two of said at least two peripherals being keyboard and display respectively, and wherein the processor in said keyboard is configured to process corresponding data of keystrokes data type and the processor in said display is configured to process corresponding data of display data type.

5. The method according to any one of the preceding Claims, wherein said client computer is devoid of a processor module that is separated from any of said at least two peripheral components and wherein the communication between said client computer and remote computer is achieved by means of said at least two peripheral components.

6. The method according to any one of the preceding Claims, wherein said client computer further includes processor module that is susceptible of being compromised and further being separated from any of said at least two peripheral components; and wherein said stage (b) further includes:

establishing a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer to peer communication channel is established between the processor module and the remote computer.

7. The method according to Claim 6, wherein said stage (c), further comprises:

C1 coding said data giving rise to coded data;

C2 transmitting said coded data to the processor module through said secured communication channel; and

for transmitting said coded data from the processor module to the authorized remote computer through said secured processor/remote computer communication channel; said coded data is not decryptable by said processor module that is susceptible to being compromised, thereby achieving secured communication between

the peripheral component and authenticated remote computer irrespective of the utilization of said processor module.

8. The method according to any one of the preceding Claims , wherein for at least one group of said peripheral components, said processor is capable of translating data of a first data type associated with one module of said group to data of a second non compatible type of the other module of said group; the method further comprising:

d) establishing a secured peer to peer communication channel with other peripheral component of said group of peripheral components;

e) coding data for communicating between the one peripheral component through said secured communication channel with said other peripheral component; said coded data is indecryptable by other of said peripheral components apart from said group; and

f) translating data of said first type to a data of said second type or *vice versa*, thereby facilitating communication between said group of peripheral components in a common data type.

9. The method according to any one of the preceding Claims, wherein said authenticated remote computer resides in the cloud.

10. A computer implemented method for providing a communication between a secured client computer and a remote computer comprising:

a. providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type; said client computer further includes a processor module that is susceptible of being compromised and further being separated from any of said at least two peripheral

components; the method further comprising with respect to each peripheral component of said modules:

b. establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; said establishing secured communication channel includes establishing a communication key known to the remote computer and the peripheral component, the communication key is usable for the data coding between the peripheral component and the remote component;

c. establishing a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer-to-peer communication channel is established between the processor module and the remote computer.

11. The method according to Claim 10, further comprising:

d. coding data giving rise to coded data;

e. transmitting said coded data to the processor module through said secured communication channel; and

for transmitting said coded data from the processor module to the authorized remote computer through said secured processor/remote computer communication channel; said coded data is not decryptable by said processor module that is susceptible to being compromised, thereby achieving secured communication between the client computer and authenticated remote computer, irrespective of the utilization of said processor module that is susceptible of being compromised.

12. The method according to Claims 10 or 11, further comprising:

f. receiving by the processor module coded data transmitted by the authorized remote computer through said secured processor/remote computer communication channel; said coded data is not decryptable by said processor module,

g. receiving said coded data by the peripheral component through a corresponding secured communication channel,

and by the processor of said peripheral component,

h. decrypting said coded data,

thereby achieving secured communication between the peripheral component and authorized remote computer, irrespective of the utilization of the processor module, irrespective of the utilization of said processor module that is susceptible of being compromised.

13. A computer implemented method for providing a secured client computer, comprising:

a. providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type; wherein for at least one group of said peripheral components, said processor is capable of translating data of a first data type associated with one module of said group to data of a second non compatible type of the other module of said group, the method further comprising:

b. establishing a secured peer-to-peer communication with other peripheral component of said group of peripheral components;

c. coding data for communicating between the one peripheral component through said secured communication channel with said other peripheral component; said coded data is indecryptable by other of said peripheral components apart from said group;

d. translating data of said first type to a data of said second type or *vice versa*, thereby facilitating communication between said group of peripheral components in a common data type.

14. A computer implemented system for providing communication between a secured client computer and a remote computer, comprising:

a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type;

each peripheral component of said components, by said processor is configured :

to establish a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; and

to code data that is communicated between the authorized remote computer and the peripheral component through said secured communication channel, said coded data being indecryptable by the processors other of said peripheral components.

15. The system according to Claim 14, wherein said client computer is devoid of a processor module that is separated from any of said at least two peripheral components and wherein the communication between said client computer and remote computer is achieved by means of said at least two peripheral components.

16. The system according to Claims 14 or 15, wherein the processor of said authenticated remote computer is configured to receive, from a first authenticated peripheral component of said components and through a corresponding first trusted channel, a coded data of a first data type, decoding it using a first communication key associated with said first peripheral component and translating it to a processable data; said processor is further configured to translate processable data to data of a second data type, code it with a second communication key associated with a second authenticated peripheral component and transmit it through a corresponding second trusted channel to said second authenticated peripheral component.

17. The system according to any one of Claims 14 to 16, wherein said authenticated remote computer resides in the cloud.

18. A computer implemented system for providing a communication between a secured client computer and a remote computer comprising:

a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type; said client computer further includes a processor module that is susceptible of being compromised and further being separated from any of said at least two peripheral components;

each peripheral component of said components, by said processor is configured :

to establish a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer, including establishing a communication key known to the remote computer and the peripheral component, the communication key is usable for the data coding between the peripheral component and the remote component;

to establish a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer to peer communication channel is established between the processor module and the remote computer.

19. A computer implemented system for providing a secured client computer, comprising:

a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the

corresponding data of said data type; wherein for at least one group of said peripheral components, said processor is capable of translating data of a first data type associated with one component of said group to data of a second non compatible type of the other component of said group,

a peripheral component of said components, by said processor is configured:

to establish a secured peer-to-peer communication with other peripheral component of said group of peripheral components;

to code data for communicating between the one peripheral component through said secured communication channel with said other peripheral component; said coded data is indecryptable by other of said peripheral components apart from said group;

to translate data of said first type to a data of said second type or *vice versa*, thereby facilitating communication between said group of peripheral components in a common data type.

20. A non-transitory computer-readable memory tangibly embodying a program of instructions executable by the computer for executing the method of any one of Claims 1 to 9.

21. A non-transitory computer-readable memory tangibly embodying a program of instructions executable by the computer for executing the method of Claim 10 to 12.

22. A non-transitory computer-readable memory tangibly embodying a program of instructions executable by the computer for executing the method of Claim 13.

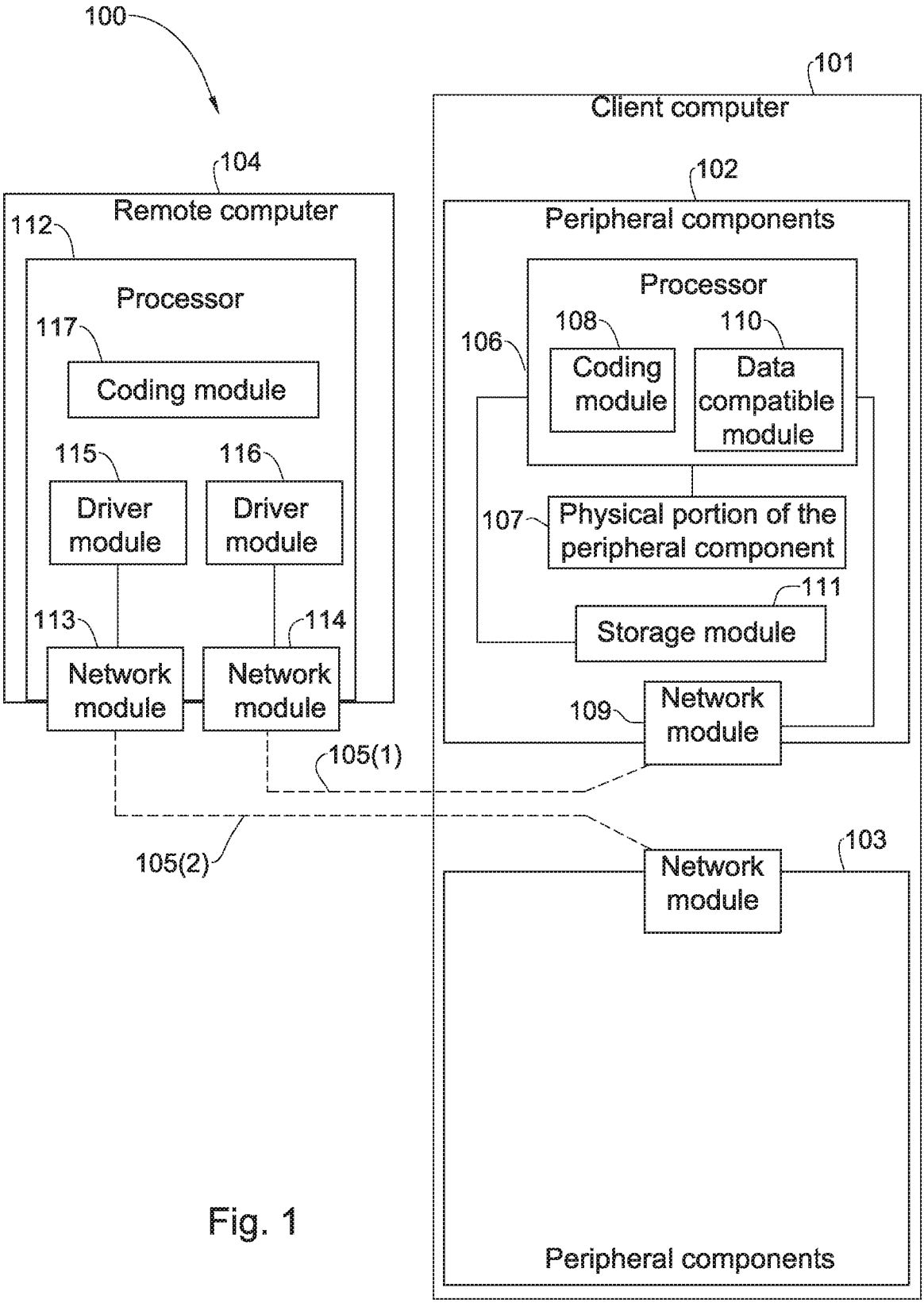

100
101
Client computer
104
Remote computer
102
Peripheral components
112
Processor
117
Coding module
115
Driver module
116
Driver module
113
Network module
114
Network module
Processor
108
110
106
Coding module
Data compatible module
107
Physical portion of the peripheral component
111
Storage module
109
Network module
105(1)
105(2)
103
Network module
Peripheral components

Fig. 1

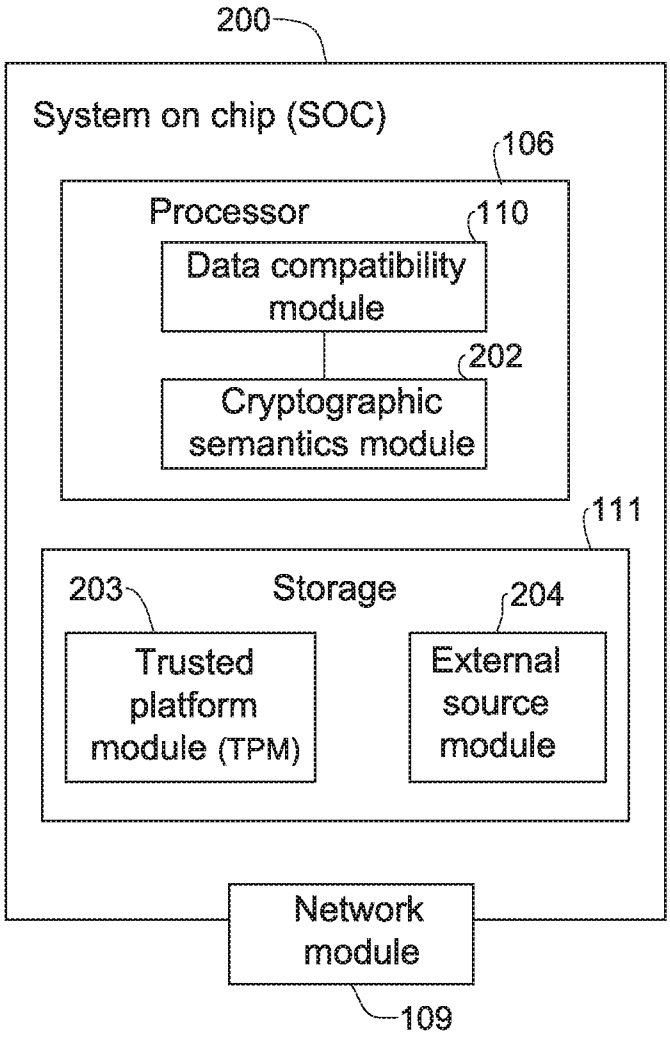

200
System on chip (SOC)
106
Processor
110
Data compatibility module
202
Cryptographic semantics module
111
203
Storage
204
Trusted platform module (TPM)
External source module
Network module
109

Fig.2

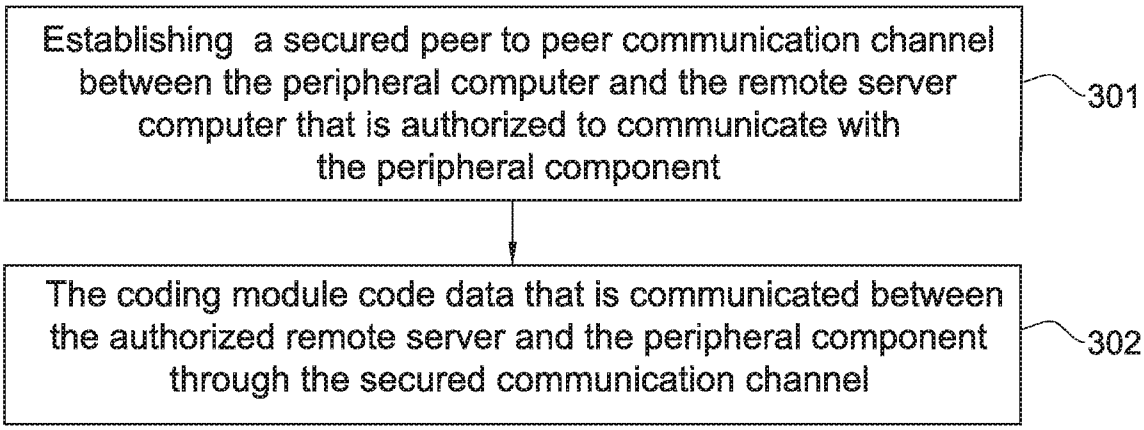

Establishing a secured peer to peer communication channel between the peripheral computer and the remote server computer that is authorized to communicate with the peripheral component
301
The coding module code data that is communicated between the authorized remote server and the peripheral component through the secured communication channel
302

Fig. 3

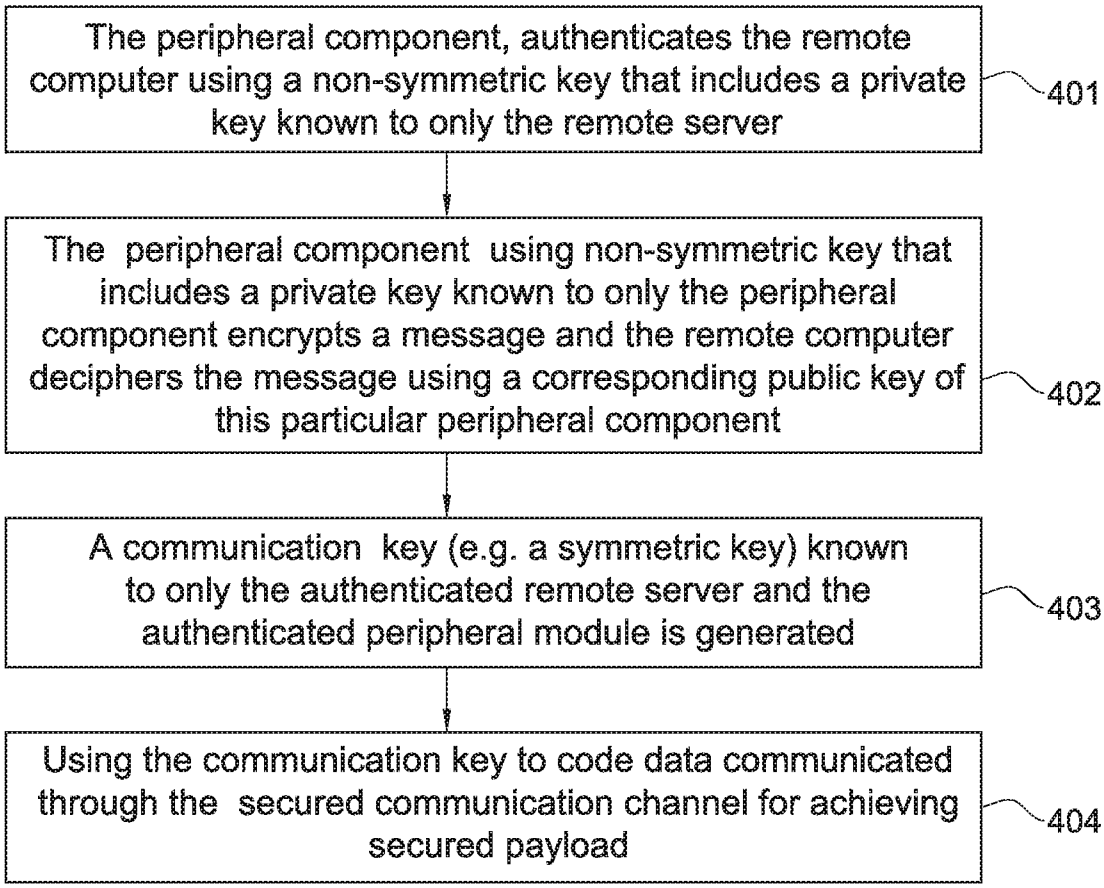

The peripheral component, authenticates the remote computer using a non-symmetric key that includes a private key known to only the remote server
401
The peripheral component using non-symmetric key that includes a private key known to only the peripheral component encrypts a message and the remote computer deciphers the message using a corresponding public key of this particular peripheral component
402
A communication key (e.g. a symmetric key) known to only the authenticated remote server and the authenticated peripheral module is generated
403
Using the communication key to code data communicated through the secured communication channel for achieving secured payload
404

Fig. 4

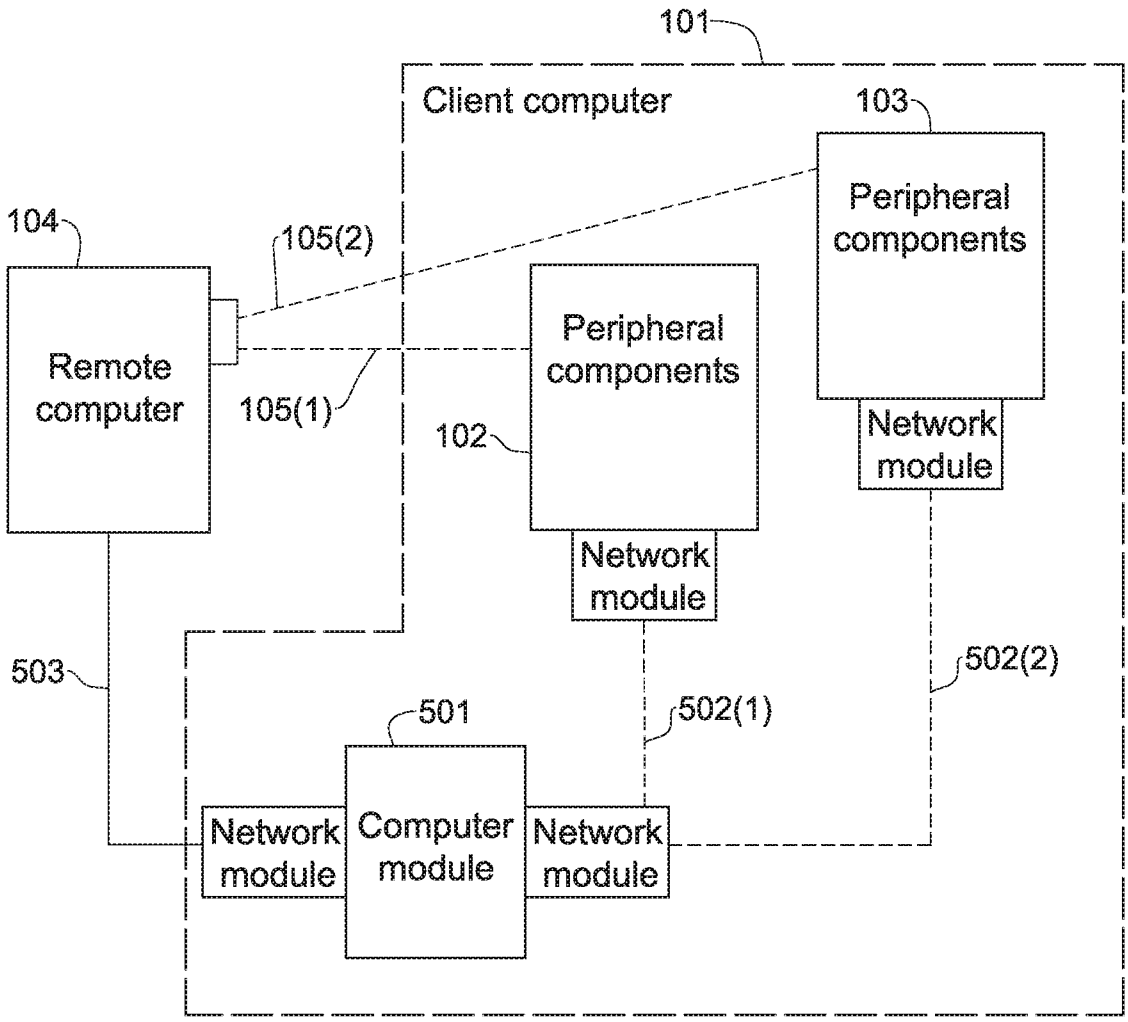

101
Client computer
103
Peripheral components
104
105(2)
Remote computer
105(1)
Peripheral components
102
Network module
Network module
503
502(2)
501
502(1)
Network module
Computer module
Network module

Fig. 5

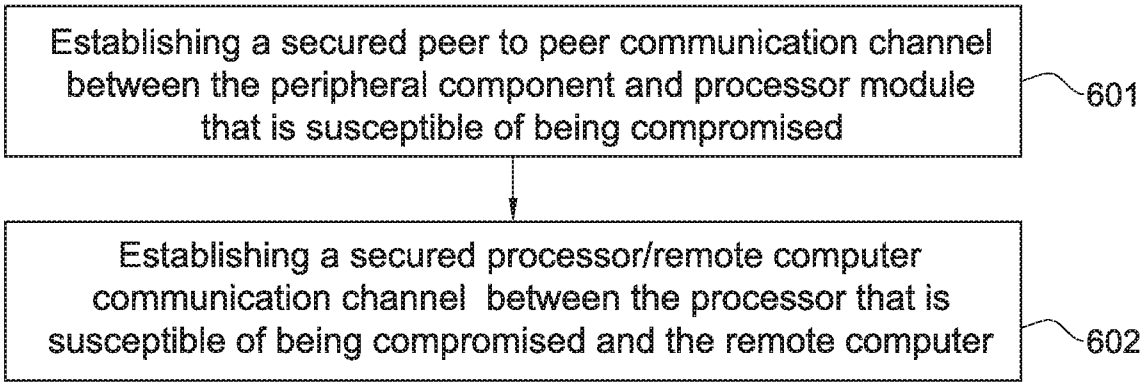


Fig. 6

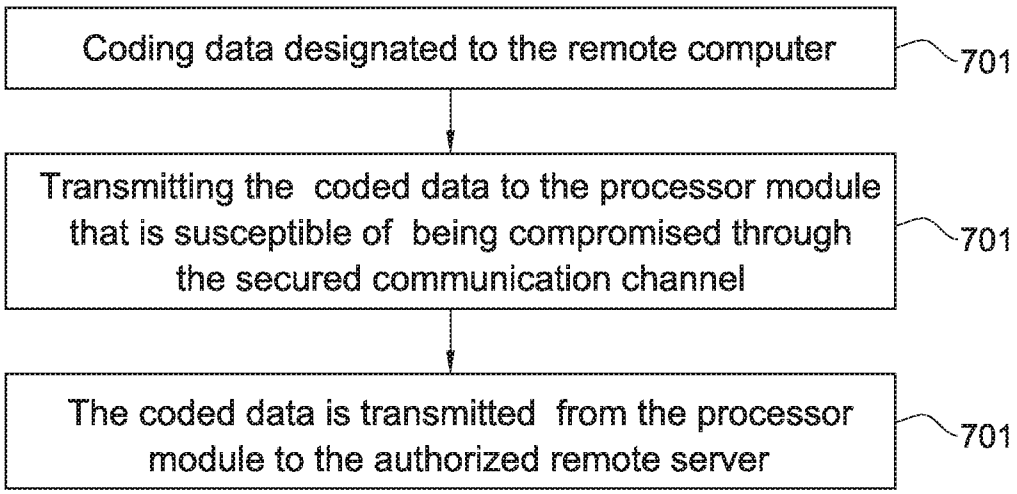


Fig. 7

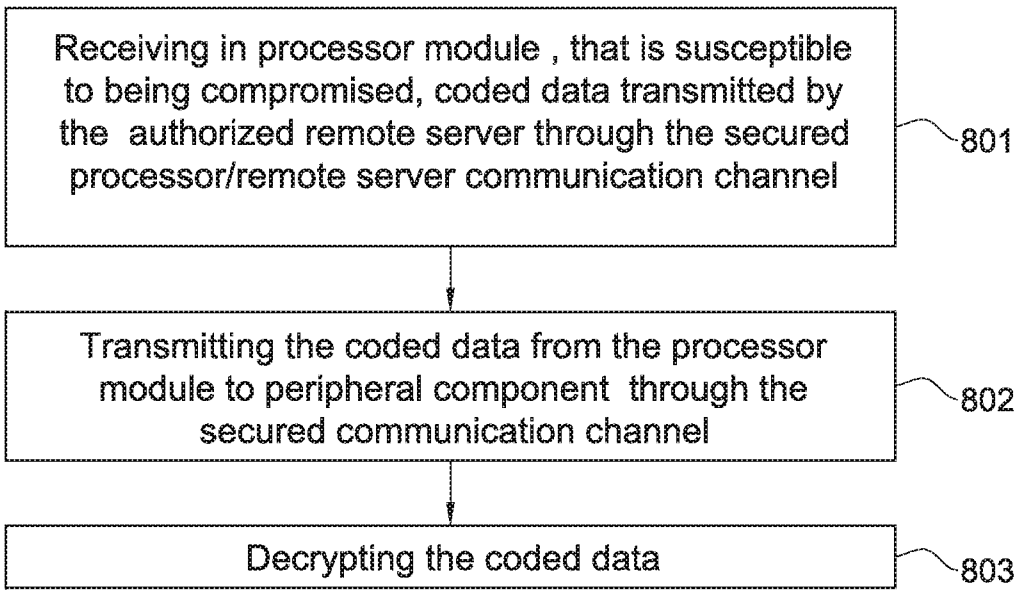


Fig. 8

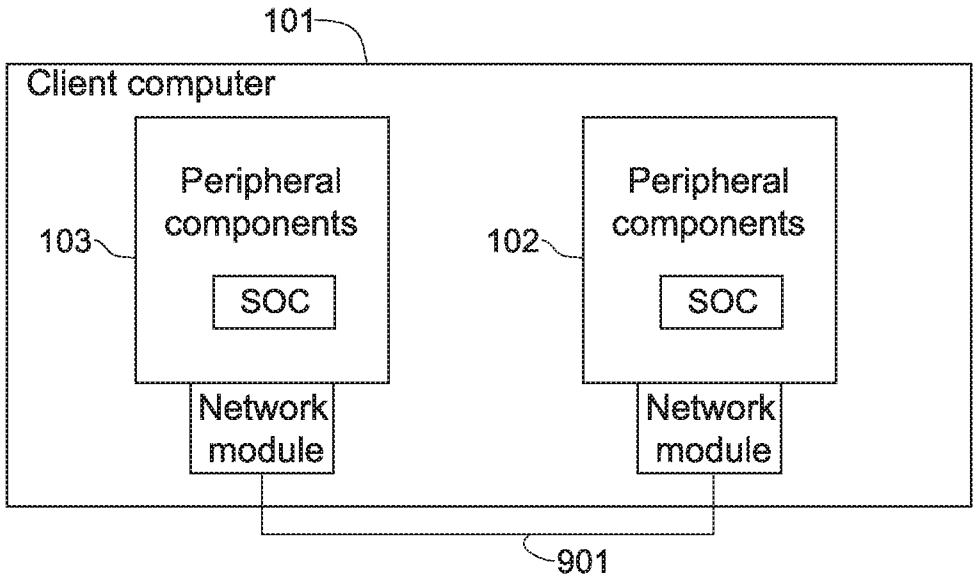


Fig. 9

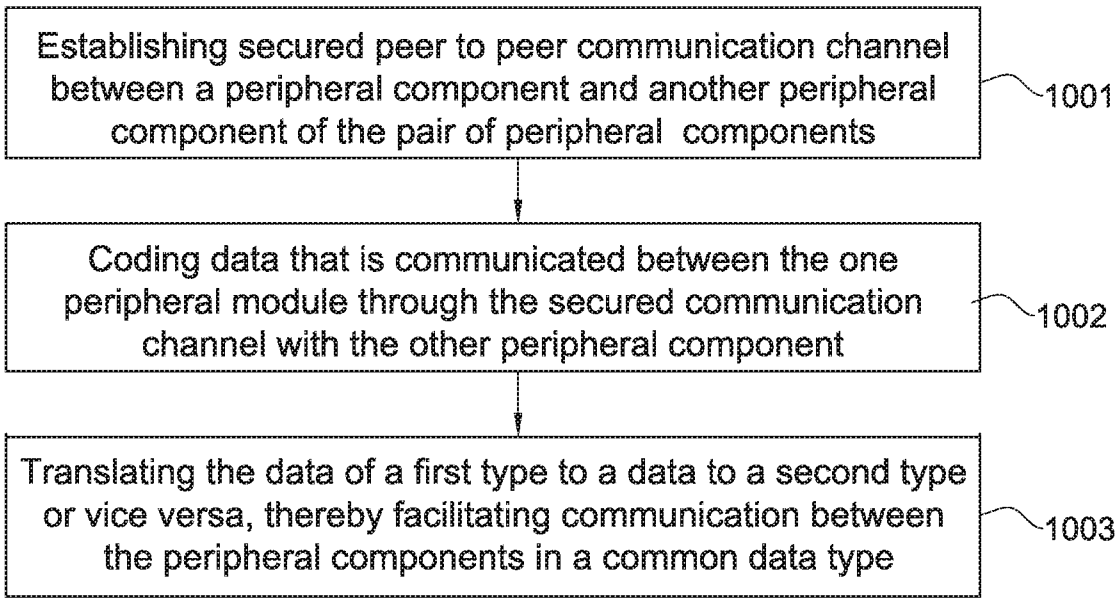


Fig. 10

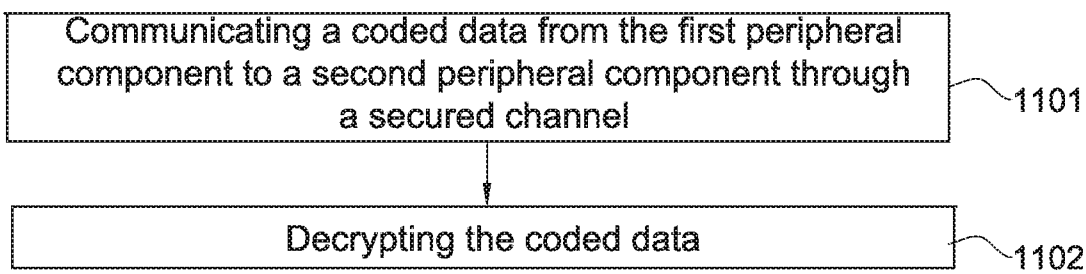


Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2019/050332

A. CLASSIFICATION OF SUBJECT MATTER

IPC (20190101) G06F 21/85, H04L 9/32, G06F 21/60, G06F 21/83, G06F 21/84, G06F 21/82

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC (20190101) G06F 21/85, H04L 9/32, G06F 21/60, G06F 21/83, G06F 21/84, G06F 21/82

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Databases consulted: Google Patents, Google Scholar, Orbit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20130179685 A1 11 Jul 2013 (2013/07/11) par. 0037, 0063, 0049, 0039, 0066, 0075	1-4,6,7,10-12,14,18
Y	par. 0037, 0063, 0049, 0039, 0066, 0075	5,8,9,13,15-17, 19-22
X	US 5596718 A 21 Jan 1999 (1999/01/21) col. 3 l. 23-33, col. 3 l. 62-65, col. 6 l. 13-28	1-4,6,7,10-12,14,18
X	US 20110154021 A1 23 Jun 2011 (2011/06/23) par. 0014-0017	1,10,14,18
Y	WO 2017021687 A1 09 Feb 2017 (2017/02/09) p. 6 l. 23-30	5,8,9,13,15-17, 19-22

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 May 2019	28 May 2019
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	Authorized officer RUSS Eran Telephone No. 972-73-3927225

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2019/050332

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20160203343 A1 14 Jul 2016 (2016/07/14) abstract, the whole doc.	1-22

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2019/050332

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 20130179685 A1	11 Jul 2013	US 2013179685 A1	11 Jul 2013
		US 8615656 B2	24 Dec 2013
		WO 2013106286 A1	18 Jul 2013
US 5596718 A	21 Jan 1999	US 5596718 A	21 Jan 1997
		AU 4672693 A	31 Jan 1994
		AU 663406 B2	05 Oct 1995
		CA 2139744 A1	20 Jan 1994
		EP 0649546 A1	26 Apr 1995
		IL 106304 D0	15 Nov 1993
		JP H07509086 A	05 Oct 1995
		US 5822435 A	13 Oct 1998
		WO 9401821 A1	20 Jan 1994
US 20110154021 A1	23 Jun 2011	US 2011154021 A1	23 Jun 2011
		US 8417941 B2	09 Apr 2013
		CA 2630388 A1	05 Nov 2009
		CA 2723747 A1	12 Nov 2009
		CA 2723747 C	06 Jan 2015
		WO 2009135324 A1	12 Nov 2009
WO 2017021687 A1	09 Feb 2017	WO 2017021687 A1	09 Feb 2017
		GB 201513811 D0	16 Sep 2015
		GB 2541000 A	08 Feb 2017
		GB 2541000 B	19 Sep 2018
US 20160203343 A1	14 Jul 2016	US 2016203343 A1	14 Jul 2016
		US 9791944 B2	17 Oct 2017
		CA 2791181 A1	01 Sep 2011
		EP 2539847 A2	02 Jan 2013

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2019/050332

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 2011208963 A1	25 Aug 2011
		WO 2011104715 A2	01 Sep 2011
		WO 2011104715 A3	05 Jan 2012