

TAMPER PROOF TEMPERATURE MONITORING DEVICE

Field of the Invention

[0001] The present invention generally relates to devices for monitoring the temperatures of an object, and more particularly to a tamper proof temperature monitoring device that monitors the temperatures of an object continuously.

Background of the Invention

[0002] The outbreak of the severe acute respiratory syndrome (SARS) in 2003 illustrates the serious health threats that the emergence of new infectious pathogens could impose to the public globally. Due to lack of effective cures for the SARS, measuring the body temperatures has been proven to be critical in containing the spread of the SARS because suspected individuals with an elevated temperature were quarantined once they were identified. Apparently, successful containment requires continuous temperature checks and stringent quarantines of suspected individuals. However, currently available temperature measurement devices may be used for temperature checks, but demand extensive resources.

[0003] Temperature monitoring devices have been provided for different applications. For example, US 6,641,544 to Liu discloses a body temperature monitoring device that includes a processor unit connected electrically to a temperature detecting unit, a data storage unit, a display unit, and a control key unit. The device stores the body temperature information in the data storage unit and displays such information on the display unit. However, this device does not provide any means to determine whether the temperature detecting unit is properly attached to the skin of the targeted person, so that there is no way to know whether the temperature information detected by the temperature detecting unit is accurate.

[0004] US 4,819,860 to Hargrove et al. discloses a wrist-mounted pulse rate and body temperature monitor that comprises clock means, sensing means for measuring the pulse rate of an individual, means for measuring the body temperature of an individual, means for comparing the current pulse rate and body temperature of the individual to preset limits, and means for generating an emergency radio signal if the measured pulse rate and

body temperature indicate any emergency medical situation. However, the monitor also fails to provide means to determine whether the pulse rate and body temperature detected are accurate.

[0005] US 2003/0069714 A1 to Wigley et al. discloses an ambulatory skin temperature monitoring system that comprises a skin temperature sensor and an ambient temperature sensor. It also discloses that a skin conductivity sensor may be included to provide feedback indicating whether the system is properly attached to a patient. However, the disclosed system does not prevent it from tampering so that it is not suitable for many situations in which a tamper proof temperature monitoring device is required.

[0006] Therefore, there is an imperative need to have a tamper proof temperature monitoring device that can be used in many situations such as SARS outbreak. This invention satisfies this need by disclosing a tamper proof temperature monitoring device that can monitor the temperature of an object remotely and continuously. Other advantages of this invention will be apparent with reference to the detailed description.

Summary of the Invention

[0007] The present invention provides a tamper proof temperature monitoring device for continuously monitoring of the body temperature of an individual. In one embodiment of the present invention, the tamper proof temperature monitoring device comprises a secure strap with a capacitance sensor for detecting the capacitance induced within the secure strap so as to prevent the device from being tampered; and a sensor module that integrally connects with the secure strap so that the sensor module can be secured onto the individual; wherein the sensor module includes a memory unit for receiving and storing electrical information; a data process unit for receiving and processing electrical information, and transmitting processed information to the memory unit for storage; a data transmitting unit for receiving and transmitting electrical information from the memory unit and a base unit; and a skin temperature sensor for measuring the skin temperature of the individual and transmitting the signals of the skin temperature to the memory unit.

[0008] In certain embodiments of the present invention, the tamper proof temperature monitoring device may further comprises one or more sensors including a skin conductivity sensor for ensuring the skin temperature sensor is in proper contact with the

skin of the individual; an ambient temperature sensor for measuring the surrounding ambient temperature to ensure that the monitored individual is located at a correct ambient condition; an identification tag presence check unit for ensuring the device being tamper-free; a pulse sensor for checking the pulses of the individual so as to ensure the device being tamper-free; and a secure strap conductivity sensor for measuring the conductivity of the secure strap to ensure the device being tamper-free.

[0009] Another aspect of the present invention provides a method for monitoring the body temperature of an individual by using the tamper proof temperature monitoring device in accordance with the present invention. The method comprises checking the capacitance of the device by the capacitance sensor and measuring the body temperature of the individual continuously by the skin temperature sensor; thereby the device can monitor the temperature of the individual as being tamper-free. In certain aspects, the method will also check the skin contact between the device and the individual by the skin conductivity sensor for ensuring that the skin temperature sensor is in proper contact with the skin of the individual, measure the surrounding ambient temperature of the individual by the ambient temperature sensor to ensure that the monitored individual is located at a correct ambient condition, check the presence of the identification tag by the identification tag presence check unit for ensuring the device being tamper-free, check the pulses of the individual by the pulse sensor so as to ensure the device being tamper-free, and/or measure the conductivity of the secure strap by the secure strap conductivity sensor so as to ensure the device being tamper-free.

[0010] The advantages of the present invention include that the miniaturized multiple sensors ensure correct temperature readings by allowing unobtrusive, positive and conformal adhesion and contact on the body surface.

[0011] One objective of the present invention is to provide a temperature monitoring device that is secured onto an object during the period of temperature monitoring so that it can reliably measure the temperatures of the object continuously.

[0012] The objectives and advantages of the invention will become apparent from the following detailed description of preferred embodiments thereof in connection with the accompanying drawings.

Brief Description of the Drawings

[0013] Preferred embodiments according to the present invention will now be described with reference to the Figures, in which like reference numerals denote like elements.

[0014] FIG 1A is an isometric view of the tamper proof temperature monitoring device in accordance with one embodiment of the present invention.

[0015] FIG 1B is an orthographic view of the tamper proof temperature monitoring device as shown in FIG 1A.

[0016] FIG 2 is an orthographic sectional front view of the embedded layers of the secure strap of the tamper proof temperature monitoring device in accordance with one embodiment of the present invention.

[0017] FIG 3 is an orthographic sectional front view of the sensor module of the tamper proof temperature monitoring device in accordance with one embodiment of the present invention.

[0018] FIG 4 is an orthographic top view of the sensor module of the tamper proof temperature monitoring device in accordance with one embodiment of the present invention.

[0019] FIG 5 is an orthographic back view of the sensor module of the tamper proof temperature monitoring device in accordance with one embodiment of the present invention.

[0020] FIG 6 illustrates the Secure Strap capacitive check in accordance with one embodiment of the present invention.

[0021] FIG 7 is a process block flow for triggering notifications by different checks.

[0022] FIG 8 is an illustration of a typical press fitted joint in accordance with one embodiment of the present invention.

[0023] FIG 9 shows the layout of the Secure Strap Conductivity Sensor embedded in the Secure Strap as shown in FIG 2.

[0024] FIG 10 shows the layout of the Secure Strap Capacitive Sensor embedded in the Secure Strap as shown in FIG 2.

[0025] FIG 11 is a block diagram of the functional processes of the tamper proof temperature monitoring device in accordance with one embodiment of the present invention.

Detailed Description of the Invention

[0026] The present invention may be understood more readily by reference to the following detailed description of certain embodiments of the invention.

[0027] Throughout this application, where publications are referenced, the disclosures of these publications are hereby incorporated by reference, in their entirety, into this application in order to more fully describe the state of art to which this invention pertains.

[0028] The present invention provides a tamper proof temperature monitoring device that can remotely provide reliable temperature readouts for a targeted person. While the principles of the present invention will be illustrated with a detailed description of a design for being used on human wrists, it is to be appreciated that the principles are applicable to many different designs including apply to different body parts of a human or animal.

[0029] FIGS 1A and 1B provide a tamper proof temperature monitoring (TPTM) device **1** comprising a secure strap **10** and a sensor module **20**. The secure strap **10** integrally connects with the sensor module **20** so that the sensor module **20** can be secured onto the wrist of a targeted person.

[0030] The secure strap **10** according to one embodiment of the present invention is made of multiple laminated layers as shown in FIG 2. The secure strap **10** comprises an adhesive layer **11**, a first electric insulator layer **12** disposed onto the adhesive layer **11**, a first electric conductor layer **13a** disposed onto the first electric insulator layer **12**, a first dielectric layer **14a** disposed onto the first electric conductor layer **13a**, a second electric conductor layer **13b** disposed onto the first dielectric layer **14a**, a second dielectric layer **14b** disposed onto the second electric conductor layer **13b**, a third electric conductor layer **13c** disposed onto the second dielectric layer **14b**, a second electric insulator layer **15** disposed onto the third electric conductor layer **13c**, a fourth electric conductor layer **16** disposed onto the second electric insulator layer **15**, a third electric insulator layer **17** disposed onto the fourth electric conductor layer **16**, and a braided metal layer **19** disposed

onto the third electric insulator layer **17**. The electric conductor layers (**13a**, **13b**, and **13c**) and dielectric layers (**14a** and **14b**) may be employed for the Secure Strap capacitive check. The fourth electric conductor layer **16** is used for the Secure Strap conductivity check. Both checks will be described in detail hereinafter.

[0031] The laminated secure strap **10** may be fabricated by any method that is known to those skilled in the art. Existing commercially available methods/processes can be used, e.g., Cast Extrusion Lamination, Hot Melt Adhesive Lamination. The materials for making the electrical conductor layers **13a**, **13b**, **13c**, **16** may be any known material that is capable of being an electrical conductor. For example, metals including gold can be used to make the electrical conductor layer in the present invention. The materials for making the dielectric layers **14a**, **14b** may be any known material that is dielectric. For example, polymers including Teflon can be used to make the dielectric layer in the present invention. The materials for making the electrical insulator layers **12**, **15**, **17** may be any known material that is with high resistance. For example, Teflon can be used to make the electric insulator layer in the present invention. The adhesion layer **11** may be made of any commercially available hypoallergenic breathable material with good adhesion to human skin.

[0032] As shown in FIGS 1A and 1B, the two ends of the secure strap **10** is stiffened and reinforced with the molded plastic **30**. These two molded plastic ends also act as the substrate to hold connectors for connecting the Secure Strap conductivity check and Secure Strap capacitive check conductors embedded in the secure strap to the sensor module **20**. In addition, the two molded plastic ends have posts designed to fit into the uni-direction press-fit receptacles found on the sensor module **20** as shown in FIG 8.

[0033] The secure strap **10** disclosed above provides electrical integrity and physical integrity. The electrical integrity will be more evident when the Secure Strap conductive and capacitive checks are discussed in detail hereinafter. The physical integrity is demonstrated by its excellent resistance to externally induced tensile and shear forces. For instance, the braided metal layer **19** may be made of stainless steel that acts as a shield against tensile force typically applied by pulling and shear force typically induced by the action of cutting with a sharp instrument. In addition, the braided metal layer **19** has good flexure property to conform to the circular cross-sectional profile of a human limb.

Finally, the secure strap **10** may be fabricated easily and cost-efficiently because, e.g., it does not contain any electronic component.

[0034] The sensor module **20** according to one embodiment of the present invention is shown in FIGS 3, 4, and 5. The sensor module comprises components housed within the sensor module **20** as shown in FIG 3 including O-ring water tight seal **21**, conducting pins **22**, ASIC/electronics and batteries **23**, ID tag micro-scanner **24**, press fitted joint **25**, optical film **26**, and conformal material **27**. As shown in FIG 4, the top side of the sensor module **20** includes LCD display **28**, LED displays **29**, ambient temperature sensor **31**, and buzzer **32**. As shown in FIG 5, the underside of the sensor module **20** contains pulse sensor **33**, skin conductivity sensors **34**, and skin temperature sensors **35**. All the components are housed in a plastic molded house that may be fabricated by any known methods.

[0035] The sensor module **20** may attach to the secure strap through any known mechanism. In one embodiment, the sensor module **20** attaches the secure strap through the press fitted joint **25** as shown in FIG 8. Compressive force applied to the Sensor Module **20** will enable the housing of the Sensor Module to snap the Sensor Module securely to the Secure Strap via the uni-direction posts located at the reinforced molded plastic ends of the Secure Strap.

[0036] The sensor module is expected to be functional under normal living conditions including washing and bathing. The O-ring water tight seal **21** ensures that a water-resistant seal is formed around the electrical connectors leading from the secure strap.

[0037] The conformal material **27** is designed such that the underside of the sensor module will always press slightly on the skin surface when it is press-fitted to the secure strap. The thickness and dimension of the sensor module is not critical for the present invention. Any thickness and dimension of the sensor module may be suitable for the present invention. In addition, a portion of the underside of the sensor module has an adhesive surface that ensures a positive contact between the skin and the array of sensors.

[0038] The TPTM device in one preferred embodiment in accordance with the principles of the present invention provides means and methods for positive determination that the device is properly secured onto a targeted person at all monitoring period (device secure check), that the device is used in a proper environment (ambient temperature

check), and that the device is properly attached to the skin of the targeted person (skin contact check). Thus, the device will reliably monitor the targeted person's body temperature continuously.

[0039] Now the device secure check is described in detail. When the TPTM device is securely attached onto a targeted person's wrist, it is activated by a command signal transmitted from a remote base unit described later. To ensure a tamper proof design, there is no venue for user to interface with the device, i.e. no user input required. Then all the sensors within the sensor module are activated simultaneously to check the proper attachment and the proper location, and record the body temperature. For the simplicity of description, each function will be described in turn.

[0040] The device secure check in one embodiment of the present invention includes a Secure Strap conductivity check, a Secure Strap capacitive check, a pulse presence check, and an identification tag presence check. It is to be appreciated that the device secure check may be done by any one of the checks or any combination of the checks as long that the checks done are enough for its applications.

[0041] The Secure Strap conductivity check uses the conductor layer **16** embedded in the Secure Strap. It detects the continuity of the electrical conductor embedded in the Secure Strap. If the integrity of this electrical conductor is not compromised, the ASIC/electronics will detect the presence of negligible electrical resistance. When this electrical conductor is severed at any location along its length, the ASIC/electronics will detect extremely large/infinite electrical resistance. If the device is properly secured onto the targeted person's wrist, the Secure Strap conductivity sensor will detect negligible electrical resistance, resulting in non-emission of the LED. If the device is not properly secured for loss of electrical continuity, the Secure Strap conductivity sensor will detect extremely large/infinite electrical resistance, and then the microcontroller will be awakened from a sleep mode to activate the Supervisory Notification (F) function. This activation is irrespective of the status of the pulse sensor. The colored LED will flash and a pre-recorded voice message stating the nature of the fault will sound continuously for a preset period of time (e.g., 1 minute). Subsequent actions to re-strap the device will not invalidate the Supervisory Notification (F). The Secure Strap conductivity check is diagrammatically shown in FIG 9.

[0042] The Secure Strap capacitive sensor detects the capacitance induced by the remaining three conductor layers (**13a, 13b, 13c**) and two dielectric layers (**14a, 14b**). As shown in FIG 2, one embodiment of the present invention shows three conductor layers 13a, 13b, and 13c and two dielectric layers 14a, 14b disposed between the conductor layers. The arrangement of the conductor layers and dielectric layers as shown in FIG 2 results in a capacitance whose value is directly proportional to the effective length l (i.e., the overlapping length of the conductor film) as shown in FIG 6. When the continuity in electrical conductor layers is maintained, the capacitance is directly proportional to $2l$. When the discontinuity in the conductor layers happens at the left end, the capacitance is directly proportional to l only. When the discontinuity in the conductor layers happens at the right end, the capacitance is directly proportional to l that is approaching zero value. Any attempt to tamper with the secure strap (e.g., cutting) will result in the separation of the conductor layers at any region along their length. This will result in the capacitance value being reduced at least to half of its original value, thereby providing a positive indication that the secure strap has been tampered with. If the device is properly secured onto the targeted person's wrist, the capacitance sensor will detect no reduction of the capacitance value, resulting in non-emission of the LED. If the device is not properly secured for the reduction of the capacitance value, the capacitance sensor will detect a reduction of the capacitance value, and then the microcontroller will be awakened from a sleep mode to activate the Supervisory Notification (F) function. This activation is irrespective of the status of the pulse sensor. The colored LED will flash and a pre-recorded voice message stating the nature of the fault will sound continuously for a preset period of time (e.g., 1 minute). Subsequent actions to re-strap the device will not invalidate the Supervisory Notification (F). The Secure Strap capacitive check is diagrammatically shown in FIG 10.

[0043] The pulse presence check detects a targeted person's pulses by a pulse sensor. The pulse sensor **33** may be any commercially available pulse sensor (e.g., photoelectric). If the device is not properly secured for loss of detecting the human pulse but with the electrical continuity still in place, the microcontroller will be awakened from a sleep mode to activate the Failure Notification (E) function. The colored LED will flash and a pre-recorded voice message stating the nature of the fault will sound continuously for a preset period of time (e.g., 1 minute). During this period of time, the targeted person is

required to rectify the fault by ensuring that the device is properly secured. If the targeted person fails to rectify the fault within the preset period, the Supervisory Notification (F) function will be activated.

[0044] The identification tag presence check can take many forms. In one embodiment, an identification tag is in the form of a bar code imprinted on an adhesive tape made of hypoallergenic breathable water proof material (e.g., band-aid like materials). The bar code tag is then attached to the appropriate location on the targeted person's limb, and the device is so strapped that the sensor module encases the entire bar code tag. The ID tag micro-scanner **24** embedded in the sensor module will beam optical light through the optical film **26** to scan the bar code. The detection of the presence of the bar code coupled with correct bar code data positively identifies that the device has not been tampered with. In contrast, loss of the bar code signal and/or detection of incorrect bar code data positively identify that the device has been tampered with. Under such condition, the Supervisory Notification (F) function will be activated.

[0045] Now referring to FIG 4, the ambient temperature sensor **31** will be utilized for the ambient temperature check that measures the surrounding ambient temperature so that it determines whether the targeted person is located at a correct ambient condition. The measured ambient temperature from the ambient temperature sensor **31** will be compared against a preset range. If the measured ambient temperature is not within the preset range, the Failure Notification (E) function will be activated to alert the targeted person by continuously flashing the colored LED and sounding of a pre-recorded voice message stating the nature of the fault for a preset period of time (e.g., 5 minutes). During this period of time, the targeted person is required to rectify the fault by ensuring that he is located at the appropriate ambient. If the targeted person fails to rectify the fault within the preset period of time, the Supervisory Notification (F) function will be activated.

[0046] Now referring to FIG 5, the skin temperature sensor **35** will measure the body temperature of the targeted person. To ensure that the skin temperature sensor **35** is properly contacted by the skin of the targeted person, the skin contact check is performed periodically by the skin conductivity sensor **34**. If the proper contact is maintained between the device and the targeted person's skin, the skin conductivity sensor **34** will detect an electrical resistance resulting in non-emission of the LED. If the contact with the skin is not properly maintained, the skin conductivity sensor will detect an infinite

resistance. The Failure Notification (E) function will be activated to alert the targeted person to rectify the fault by continuously flashing the colored LED and sounding of a pre-recorded voice message stating the nature of the fault for a preset period of time (e.g., 5 minutes). If the targeted person rectifies the fault within the preset period of time resulting in re-establishment of the appropriate electrical resistance, the flashing LED and voice alarm will be deactivated immediately. If the targeted person fails to rectify the fault within the preset period of time, the Supervisory Notification (F) function will be activated.

[0047] The skin temperature sensor will continuously monitor the body temperature of the targeted person. If the measured skin temperature is within the acceptable range, the data will be stored in a temporary buffer for subsequent transmission to the base station. If the measured skin temperature is not within the acceptable range, the data will be stored in a temporary buffer and the Supervisory Notification (F) function will be immediately activated.

[0048] The Sensor Module **20** further comprises a central controller **40**. The central controller **40** comprises a signal preprocessing unit, a processor unit, a memory unit, a battery unit, and a I/O ports as shown in FIG 11. The Sensor Module **20** further comprises a wireless transceiver unit as shown in FIG 11. FIG 11 is a block diagram of the functional processes of the TPTM device **1**. The brain of the TPTM device **1** is an ultra low-power central controller, implemented as an application-specific integrated circuit (ASIC), which functions as a centralized coordinating unit that manages the functions and sensor data with respect to the TPTM device. All the sensors (ambient temperature sensor **21**, skin conductivity sensors **34**, skin temp sensors **35**, ID tag microscanner **24**, pulse sensor **33**, secure strap electrical conductivity sensor and secure strap capacitance sensor) are coupled to the central controller such that the signals gathered by these sensors are conditioned and preprocessed by a signal preprocessing unit before passing through to the processor unit. The signal preprocessing unit includes analog to digital conversion capabilities that allow multiple analog sensor signals to be converted to digital forms, which can be processed by the processor unit. The processor unit is normally operating in ultra low-power mode such as sleep mode, awakened only at periodic intervals to poll, gather, process and transmit data from the sensors, such as temperature data from the skin temperature sensors **35**, or to update output interfaces such the LCD display **28** and LED displays **29**. The processor unit can also be awakened by hardware interrupts generated by

specific events, including but not limited to, the loss of electrical continuity in the secure strap (which may indicate possible tampering), or on interrogation by the remote base unit, which communicates with the central controller through a suitable wireless transceiver unit.

[0049] The prior description has mentioned two notification functions: failure notification and supervisory notification. Now a more detailed description for them is provided. The failure notification (E) function is to alert the targeted person of the fault and to allow the targeted person to rectify the fault within a preset period of time. The failure notification function is activated during the device secure check for loss of human pulses, the skin contact check, and the ambient temperature check. The supervisory notification (F) function is to inform the authority of the nature of the fault and the time of occurrence. For instance, if the supervisory notification function is triggered by the skin temperature check, it shows that the targeted person is having an elevated body temperature. The relationships between different checks and the notifications are illustrated in FIG 7.

[0050] The sensor module **20** also provides a data transmission means. The TPTM device provides a two-way data transmission means to a remote base unit via a wireless RF transceiver unit. The communication and encoding-decoding protocols used can be any known industry-standard protocols, such as those used in electronic house arrest systems. The base unit, powered from the mains supply, but with internal battery backup, may receive and transmit data to the supervising authority via the telephone line using modem dial-up or other known data transmission implementations such as GPRS. The temperature data stored within the memory unit of the sensor module can be transmitted to a remote base unit. Thus, the tamper proof temperature monitoring device and the base unit is composed of a tamper proof temperature monitoring system. The base unit capable of two-way wireless communication between itself and the device is connected to a socket of a fixed telephone line.

[0051] In one preferred embodiment, there are three transmission modes: transmit at will; transmit at fixed schedule; and transmit at event trigger. If the transmission mode is set to "Transmit at Will" of the designated monitoring authority, data stored in the device buffer will be transmitted from the device to the base unit once the interrogation signal is sent by the base unit and detected by the device. If the transmission mode is set to

“Transmit at Fixed Schedule”, data in the device buffer will be transmitted to the base unit according to the scheduled time. If the transmission mode is set to “Transmit at Event Trigger”, data in the device buffer will be transmitted to the base unit only when the skin temperature of the targeted person exceeds a preset value.

[0052] Notwithstanding the type of Data Transmission selected, the base unit will always interrogate the device at a pre-set regular interval (e.g., every 5 minutes) by pulsing an electrical signal with a strength that corresponds to a radial distance that can be received by the device. The device then acknowledges the interrogation by returning an electrical signal. In the event that the acknowledgment signal is not received by the preset duration, the Supervisory Notification (F) function will be activated and the authority monitoring the functions of the device will be informed of the nature and time of the occurrence. This regular interrogation also monitors the location of the targeted person and confines the targeted person to specified vicinity.

[0053] The tamper proof temperature monitoring device of the present invention has broad and diversified applications. For example, the monitoring device may be designed for different activities (e.g., indoor or outdoor), different age groups (e.g., infants, toddlers, adults), different objects (e.g., human, and dogs), or different situations (e.g., quarantine, or military training).

[0054] While the present invention has been described with reference to particular embodiments, it will be understood that the embodiments are illustrative and that the invention scope is not so limited. Alternative embodiments of the present invention will become apparent to those having ordinary skill in the art to which the present invention pertains. Such alternate embodiments are considered to be encompassed within the spirit and scope of the present invention. Accordingly, the scope of the present invention is described by the appended claims and is supported by the foregoing description.

CLAIMS

What is claimed is:

1. A tamper proof temperature monitoring device for continuously monitoring of the body temperature of an individual, comprises:
 - a secure strap with a capacitance sensor for detecting the capacitance induced within the secure strap so as to prevent the device from being tampered; and
 - a sensor module that integrally connects with the secure strap so that the sensor module can be secured onto the individual;
 - wherein the sensor module includes:
 - a memory unit for receiving and storing electrical information;
 - a data process unit for receiving and processing electrical information, and transmitting processed information to the memory unit for storage;
 - a data transmitting unit for receiving and transmitting electrical information from the memory unit and a base unit;
 - a skin temperature sensor for measuring the skin temperature of the individual and transmitting the signals of the skin temperature to the memory unit; and
 - an ambient temperature sensor for measuring the surrounding ambient temperature to ensure that the monitored individual is located at a correct ambient condition.
2. The tamper proof temperature monitoring device of claim 1, wherein the sensor module further comprises a skin conductivity sensor for ensuring the skin temperature sensor is in proper contact with the skin of the individual.
3. The tamper proof temperature monitoring device of claim 1, wherein the sensor module further comprises an identification tag presence check unit for ensuring the device being tamper-free; wherein the identification tag present check unit includes an identification tag attached to the individual, and a ID tag micro-scanner disposed within the sensor module, wherein the ID tag micro-scanner will be able to scan the identification tag and transmit the identification information to the data process unit if the device is properly attached to the individual.

4. The tamper proof temperature monitoring device of claim 1, wherein the sensor module further comprises a pulse sensor for checking the pulses of the individual so as to ensure the device being tamper-free.
5. The tamper proof temperature monitoring device of claim 1, wherein the secure strap further comprise a secure strap conductivity sensor for measuring the conductivity of the secure strap to ensure the device being tamper-free.
6. The tamper proof temperature monitoring device of claim 5, wherein the secure strap conductivity sensor is comprised of at least one electric conductive layer embedded in the secure strap.
7. A tamper proof temperature monitoring device for continuously monitoring of the body temperature of an individual, comprises:
 - a secure strap with a capacitance sensor for detecting the capacitance induced within the secure strap so as to prevent the device from being tampered; and
 - a sensor module that integrally connects with the secure strap so that the sensor module can be secured onto the individual;
 - wherein the sensor module includes:
 - a memory unit for receiving and storing electrical information;
 - a data process unit for receiving and processing electrical information, and transmitting processed information to the memory unit for storage;
 - a data transmitting unit for receiving and transmitting electrical information from the memory unit and a base unit; and
 - a skin temperature sensor for measuring the skin temperature of the individual and transmitting the signals of the skin temperature to the memory unit;
 - wherein the capacitance sensor comprises at least one pair of electrical conductive layer and at least one dielectric layer; thereby the at least one pair of electrical conductive layer and the at least one dielectric layer form the capacitance within the secure strap.

8. A tamper proof temperature monitoring device for continuously monitoring of the body temperature of an individual, comprises:

- a secure strap; and

- a sensor module that integrally connects with the secure strap so that the sensor module can be secured onto the individual;

- wherein the sensor module includes:

- a memory unit for receiving and storing electrical information;

- a data process unit for receiving and processing electrical information, and transmitting processed information to the memory unit for storage;

- a data transmitting unit for receiving and transmitting electrical information from the memory unit and a base unit;

- a skin temperature sensor for measuring the skin temperature of the individual and transmitting the signals of the skin temperature to the memory unit; and

- an identification tag presence check unit for ensuring the device being tamper-free; wherein the identification tag present check unit includes an identification tag attached to the individual, and a ID tag micro-scanner disposed within the sensor module, wherein the ID tag micro-scanner will be able to scan the identification tag and transmit the identification information to the data process unit if the device is properly attached to the individual.

9. A tamper proof temperature monitoring device for continuously monitoring of the body temperature of an individual, comprises:

- a secure strap; and

- a sensor module that integrally connects with the secure strap so that the sensor module can be secured onto the individual;

- wherein the sensor module includes:

- a memory unit for receiving and storing electrical information;

- a data process unit for receiving and processing electrical information, and transmitting processed information to the memory unit for storage;

- a data transmitting unit for receiving and transmitting electrical information from the memory unit and a base unit;

a skin temperature sensor for measuring the skin temperature of the individual and transmitting the signals of the skin temperature to the memory unit;

an identification tag presence check unit for ensuring the device being tamper-free; wherein the identification tag present check unit includes an identification tag attached to the individual, and a ID tag micro-scanner disposed within the sensor module, wherein the ID tag micro-scanner will be able to scan the identification tag and transmit the identification information to the data process unit if the device is properly attached to the individual; and

an ambient temperature sensor for measuring the surrounding ambient temperature to ensure that the monitored individual is located at a correct ambient condition.

10. The tamper proof temperature monitoring device of claim 9, wherein the sensor module further comprises a skin conductivity sensor for ensuring the skin temperature sensor is in proper contact with the skin of the individual.

11. The tamper proof temperature monitoring device of claim 9, wherein the sensor module further comprises a capacitance sensor for detecting the capacitance induced within the secure strap so as to prevent the device from being tampered.

12. The tamper proof temperature monitoring device of claim 9, wherein the sensor module further comprises a pulse sensor for checking the pulses of the individual so as to ensure the device being tamper-free.

13. The tamper proof temperature monitoring device of claim 9, wherein the secure strap further comprise a secure strap conductivity sensor for measuring the conductivity of the secure strap to ensure the device being tamper-free.

14. The tamper proof temperature monitoring device of claim 13, wherein the secure strap conductivity sensor is comprised of at least one electric conductive layer embedded in the secure strap.

15. A tamper proof temperature monitoring device for continuously monitoring of the body temperature of an individual, comprises:

- a secure strap; and
- a sensor module that integrally connects with the secure strap so that the sensor module can be secured onto the individual;
- wherein the sensor module includes:
 - a memory unit for receiving and storing electrical information;
 - a data process unit for receiving and processing electrical information, and transmitting processed information to the memory unit for storage;
 - a data transmitting unit for receiving and transmitting electrical information from the memory unit and a base unit;
 - a skin temperature sensor for measuring the skin temperature of the individual and transmitting the signals of the skin temperature to the memory unit; and
 - an identification tag presence check unit for ensuring the device being tamper-free;
 - wherein the identification tag present check unit includes an identification tag attached to the individual, and a ID tag micro-scanner disposed within the sensor module, wherein the ID tag micro-scanner will be able to scan the identification tag and transmit the identification information to the data process unit if the device is properly attached to the individual;
 - wherein the sensor module further comprises a capacitance sensor for detecting the capacitance induced within the secure strap so as to prevent the device from being tampered; and
 - wherein the capacitance sensor comprises at least one pair of electrical conductive layer and at least one dielectric layer; thereby the at least one pair of electrical conductive layer and the at least one dielectric layer form the capacitance within the secure strap.

16. A method for monitoring the body temperature of an individual by using a tamper proof temperature monitoring device of claim 1, said method comprising of:

- checking the capacitance of the device by the capacitance sensor; and
- measuring the body temperature of the individual continuously by the skin temperature sensor; thereby the device can monitor the temperature of the individual as being tamper-free.

17. The method of claim 16, wherein the sensor module of the tamper proof temperature monitoring device further comprises a skin conductivity sensor; and wherein said method further comprises checking the skin contact between the device and the individual by the skin conductivity sensor for ensuring that the skin temperature sensor is in proper contact with the skin of the individual.

18. The method of claim 16, wherein the sensor module of the tamper proof temperature monitoring device further comprises an ambient temperature sensor; and wherein said method further comprises measuring the surrounding ambient temperature of the individual by the ambient temperature sensor to ensure that the monitored individual is located at a correct ambient condition.

19. The method of claim 16, wherein the sensor module of the tamper proof temperature monitoring device further comprises an identification tag presence check unit; wherein said method further comprises checking the presence of the identification tag by the identification tag presence check unit for ensuring the device being tamper-free.

20. The method of claim 16, wherein the sensor module of the tamper proof temperature monitoring device further comprises a pulse sensor; wherein said method further comprises checking the pulses of the individual by the pulse sensor so as to ensure the device being tamper-free.

21. The method of claim 16, wherein the secure strap of the tamper proof temperature monitoring device further comprises a secure strap conductivity sensor; wherein said method further comprises measuring the conductivity of the secure strap by the secure strap conductivity sensor so as to ensure the device being tamper-free.