

CCTV SECURITY SYSTEM AND METHOD THEREFOR

Field of the Invention

[0001] The present invention relates to closed circuit television (CCTV) system. In particular, the present invention relates to system and method for securing data of a
5 CCTV system.

Background

[0002] Closed Circuit Television (CCTV) systems are widely used for security surveillance in various settings, including residential and commercial properties, public areas, and transportation facilities. These systems consist of cameras that capture images
10 and videos of the monitored area, which are transmitted to a digital video recorder (DVR) or network video recorder (NVR) for storage and retrieval. However, the transmission of CCTV images over networks can be vulnerable to security breaches that can compromise the privacy and security of individuals and organizations.

[0003] One of the potential risks of transmitting CCTV images over networks is
15 the risk of interception and hijacking by unauthorized third parties. This can occur if the transmission is not secured with appropriate encryption methods and authentication protocols. Hackers can intercept and view the CCTV images, or even manipulate or delete them, leading to serious security breaches and privacy violations.

[0004] To address this issue, various methods have been proposed to secure the
20 transmission of CCTV images to DVRs or NVRs. One approach is to use encryption algorithms such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS) to encrypt the data in transit. This ensures that the data is protected from interception and manipulation by unauthorized parties.

[0005] Another method is to implement secure authentication protocols such as user authentication, device authentication, and access control mechanisms. This involves verifying the identity of the sender and receiver of the data and restricting access to authorized users only.

5 **[0006]** The above system and method however possess potential issues over the key management for encryption. This includes the risk of key loss or theft, as well as the risk of weak encryption keys being used. In addition, if the encryption keys are not properly managed, it can lead to problems with system compatibility and interoperation.

[0007] In addition, physical security measures such as securing network
10 infrastructure and using firewalls, intrusion detection systems, and antivirus software can help to prevent unauthorized access and mitigate the risks of security breaches.

[0008] In summary, the security of CCTV systems is of utmost importance, given the potential risks of security breaches and privacy violations. By implementing appropriate security measures such as encryption, authentication, and physical security,
15 the transmission of CCTV images can be secured and the risks of hijacking minimized.

Summary

[0009] In one aspect of the present invention, it provides a secure device adapted for CCTV network having a plurality of CCTV camera and a CCTV recorder. The secure device comprises a communication module having a socket for locally connecting to the
20 CCTV camera or the CCTV recorder to transmit data over a communication network; a microprocessor acts as a control unit for the secure device and handling the data flow; an FPGA chip operationally encrypting/decrypting the data; a secure element for handling key diversification for encrypting/decrypting the data by FPGA chip. The secure device

is connected locally to the CCTV camera or CCTV recorder, operationally, encrypting/decrypting data transmitting through the communication network, such that the data is end-to-end encrypted across the CCTV network by the secure device.

5 **[0010]** In one embodiment, the secure element is certified by Common Criteria (CC) or Federal Information Processing Standards (FIPS).

[0011] In another embodiment, the secure device may further comprise an admin authenticator for access authentication to the secure device. The admin authenticator
10 may be configured in a card form having its own secure element embedded therein. In yet another embodiment, the admin authenticator may be integrated on the secure device in a form of biometric scanner/sensor. In a further embodiment, the admin authenticator is deployed remotely from the secure device.

15 **[0012]** In another aspect of the present invention, there is provided a surveillance system having a plurality of CCTV camera connected to a CCTV recorder via a communication network. The communication network can be wired or wireless network. The surveillance system comprises a plurality of the aforesaid secure devices. The secure device is connected directly to the CCTV camera such that data passes through the secure
20 device before transmitting to the communication network, and another secure device connected directly before the CCTV recorder.

[0013] In yet another aspect of the present invention, there is provided a method for providing additional encryption/decryption for a surveillance system over a
25 communication network. The method comprises adding secured devices to the

surveillance system having CCTV cameras and CCTV recorder connected through a communication network; activating secured elements of the secured devices; encrypting data from CCTV cameras through the secured devices; transmitting the encrypted data to the central recording system through the CCTV network; and decrypting the encrypted
5 by the secured devices for processing by the central reorder. Data transmitted through the CCTV network is end-to-end encrypted by the secure devices.

[0014] In one embodiment, the end-to-end encryption is done by the aforesaid security devices.

10

Brief Description of the Drawings

[0015] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0016] FIG. 1 illustrates a block diagram of a surveillance system in accordance
15 with an embodiment of the present invention;

[0017] FIG. 2 illustrates a CCTV surveillance system in accordance with an alternative embodiment of the present invention;

[0018] FIG. 3 illustrates a process flow of a CCTV security system in accordance with an embodiment of the present invention;

20 **[0019]** FIG. 4 illustrates a schematic diagram of the surveillance system having secured devices of FIG. 1 in accordance with an embodiment of the present invention; and

FIG. 5 illustrates a block diagram of a secure device in accordance with an alternative embodiment of the present invention.

25

Detailed Description

[0020] In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0021] FIG. 1 illustrates a block diagram of a surveillance system **100** in accordance with an embodiment of the present invention. The surveillance system **100** comprises a plurality of Closed-Circuit Television (CCTV) cameras **110** connected to a central recording system **120** through a CCTV network **150**. Each of the CCTV camera is locally connected with an secured device **182** for encrypting data to be transmitted through the CCTV network **150**. The surveillance system **100** further comprises a central secured device **184** locally connected directly to the central recording system **120** for decrypting data received from the CCTV network **150**.

[0022] The secured devices **182** and the central secured device **184**, each comprises a certified secured element adopted to encrypt/decrypt data transmitting through the CCTV network **150**. The certified secured element must at least be certified under the Common Criteria (CC) and/or Federal Information Processing Standards (FIPS) certifications. It is well understood to a skilled person that CC and FIPS certifications are security standards used to evaluate the security features of a device or system, including the smart chip, also known as a secure element. These certifications evaluate a range of security features, such as access control, authentication, secure boot,

and key management, to ensure that the device or system is designed and implemented securely.

[0023] The CCTV network **150** can be any communication network, wired and/or wireless, which include local area network (LAN) or wide area network (WAN).

5 In one embodiment, the CCTV network **150** can be a cloud network. In another embodiment, it can also be a mobile communication network.

[0024] In one embodiment, the secured devices **182, 184** are adapted as a plug-and-play devices. The secured devices **182, 184** may adopt connectors compatible with the CCTV network **150**, such as the Power over Ethernet (PoE), Coax, RJ45 etc.

10 **[0025]** Data encryption is known to be one of the most secured way of protecting data, when the keys are remained protected. Most CCTV surveillance system may have their in-built security system to encrypt the data to be transmitted through the CCTV network.

[0026] It is to be noted that CCTV surveillance system and the components
15 therefor, i.e. CCTV cameras, recorders, are well known in the art. These components can be available off-the-shelf. These surveillance system are usually fitted with manufactured security features for encrypting/decrypting the data. These factory fitted security system may facilitate encryption of the data when the footage is transmitted from the CCTV cameras to the recorder. These security measures are shared among the lines
20 of products by the respective manufacturers, and therefore, it can be vulnerable to security breaches. Hence, adding additional security feature to the surveillance system would be essential to protecting the data travel over the network. It is more so when the

secured elements adopted are certified to be the most secured way possible due to the nature and the infrastructure of a secured element.

[0027] For avoidance of doubt, the secured element in this description refers to security module that is designed to provide secure storage and processing of sensitive data, such as cryptographic keys, certificates, and passwords. They are microchips embedded in a device and it is designed to provide a secure execution environment for sensitive operations, such as authentication, encryption, and decryption, and is often used in applications that require a high level of security, such as mobile payments, digital identity, and secure communications. Further, it offers a range of security features, such as secure boot, hardware-based encryption, and secure storage of cryptographic keys. These features help to protect the secured element from physical and logical attacks, such as side-channel attacks, brute-force attacks, and tampering. Secured elements are often certified by independent organizations, such as the Common Criteria (CC) or Federal Information Processing Standards (FIPS), to ensure that they meet specific security requirements. These certifications provide assurance to users and customers that the secured element has undergone rigorous testing and evaluation to ensure that it meets a high level of security.

[0028] The need for secure encryption methods in CCTV surveillance systems is well recognized. CCTV footages are highly sensitive, and if it falls into the wrong hands, it can be used for criminal activities, corporate espionage, and many other malicious purposes. In order to secure CCTV footage, encryption is one of the most effective methods that can be employed. In this embodiment, we present a secure element pair as an external device that provides encryption and decryption for CCTV footages.

[0029] Accordingly, instead of dependent on the manufacturer implemented security feature, the present invention offers an additional means to further secure the data. The advantage of having such secure element, which is external to the CCTV surveillance system is that the secure element can be customized to the owner's requirement and fully controlled by the owner. The owner may manage the entire CCTV surveillance system at their end, including managing the keys for all the encryptions. The use of separate encryption and decryption devices provides end-to-end encryption of the video footage, which ensures that the footage remains secure throughout its transmission. Further, such external devices having the secured element can be added to existing CCTV surveillance system. With this additions, the data transmissions over the CCTV network can be secured, even against manufacturers of the CCTV surveillance system.

[0030] FIG. 2 illustrates a CCTV surveillance system **200** in accordance with an alternative embodiment of the present invention. Similarly, the CCTV surveillance system **200** comprises a plurality of CCTV cameras **210** connected to a central recording system **220** through a CCTV network **250**. Each of the CCTV camera is connected with an secured device **282** for encrypting data to be transmitted through the communication network **250**. The surveillance system **200** further comprises. A central secured device **284** connected directly to the central recording system **220** for decrypting data received from the CCTV network **250**.

[0031] The secured devices **282, 284**, each comprises a secured element therein, for encrypting/decrypting data channelled into the secured devices **282, 284**. The surveillance system **200** further comprises admin authenticators **292**. The admin authenticators **292** adapted and personalised to the users carrying the admin

authenticators **292**. In one embodiment, the admin authenticators carry the user biometrics and/or passwords for authentication. The authentication is needed to operate and manage the secured devices **282, 284**. That realises a two-factors authentication (2FA) to activate and operate the secured devices **282, 284** for added security to the
 5 CCVT surveillance system **200**. Accordingly, in order to access the secured elements at upstream and downstream, authentication is required through the admin authenticator **292**. In a desired embodiments, the admin authenticators **292** also comprises a secured elements that work in conjunction with the secured devices **282, 284**. The secured devices **282, 284** may further comprise a reader that operationally perform verification
 10 and authentication of the admin authenticators **292**. The reader may equip with wired or wireless means for reading the admin authenticators **292**. In one embodiment, the admin authenticator can be in a form of card that store the admin user authentication details. In another embodiment, the admin authenticator can be integrated on the secured devices **282, 284** in a form of biometric scanner/sensor, whereby authorised personnel can
 15 accessed the secure elements **282,284** for maintenance with their registered biometric information.

[0032] With the reader equipped on the secured devices **282, 284**, the secured devices **282, 284** can be activated at first used through the admin authenticators **292**, and any subsequent maintenance shall require the admin authenticators **292** to access the
 20 secured devices **282, 284**. Accordingly, without the admin authenticators **292**, unauthorised personnel will not be able to access the secured devices **292** due to the highly secured elements embedded in the admin authenticators **292**. And even with the presence of the admin authenticators **292**, one will require an authentication factor, such

as password, biometric identification, to prove identity of the person holding the admin authenticator **292**.

[0033] The admin authenticators **292** may be a handheld device having the secured element. In another embodiment, the admin authenticators **292** may be in a form
5 of smart-chip/card, or tokens having a secured element that can be easily carried around. In one embodiment, the secured devices **282**, **284** may further comprise biometric reader and/or password keypad.

[0034] The authentication process involves the use of biometric authentication, such as fingerprint recognition or facial recognition in conjunction with the encrypted
10 credentials to offer multi-layers security measures to ensure that the keys are secured.

[0035] It is well recognized that the secured elements certified under CC and/or FIPS are highly secured. One reason for this is that these secured elements are designed with specific functionality and isolation with a limited number of commands that are strictly controlled and regulated, i.e. limited attack surface. This ensures that only
15 authorized users can access the secured devices and perform the necessary operations. Additionally, the limited number of usable commands also makes it more difficult for attackers to exploit vulnerabilities in the secured element, as there are fewer avenues for them to exploit. This limited functionality makes secured elements highly secure and provides a strong defence against a wide range of threats. Overall, secured elements that
20 have been certified under CC or FIPS are an essential component of modern security architectures and provide a crucial layer of protection for sensitive data and applications.

[0036] In another embodiment, the secured devices **282** can only be accessed through the remote authentication from through the secure device **284**, which is usually managed by the central office.

[0037] FIG. 3 illustrates a process flow a CCTV security system in accordance with an embodiment of the present invention. The process comprises adding secured devices to a surveillance system at step **302**; activating secured elements of the secured devices at step **304**; encrypting data from CCTV cameras through the secured devices at step **306**; transporting the encrypted data to the central recording system through the CCTV network at step **308**; and decrypting the encrypted by the secured devices for processing by the central reorder **312**.

[0038] At the step **302**, the secured devices are added to each CCTV camera and the central recording device of the surveillance system. Each of the secured devices comprises secured elements for securing encryption keys. Each of the secured devices can be fabricated as external or add-on devices to the surveillance system. At the step **304**, each of the secure elements shall be activated on first used by authorized administrators. The authorized administrators are usually authorized personnel from the operator or owner of the surveillance system. Only those activated secure elements can be used for encrypting/decrypting the data.

[0039] At the step **306**, all data from the CCTV cameras are encrypted by the secure element of the secured device with the encryption keys. At the step **308**, the encrypted data is transported to the central recorder through the CCTV network. It is to be noted and understood that when the encrypted data travels over the CCTV network, which may include external network, such as internet, the encrypted data is only

decryptable by the keys of the intended recipient. In the present case, the encrypted data is decryptable only by the secured device connected to the central recorder (i.e. intended recipient). At the step **312**, when the secured device receives the encrypted data from the respective CCTV camera having a secured device connected thereto, it decrypts the encryption of the encrypted data then feeds the decrypted data to the central recorder for further processing and storing the data.

[0040] FIG. 4 illustrates a schematic diagram of the surveillance system **100** having secured devices of FIG. 1 in accordance with an embodiment of the present invention. As shown, the secured devices **182** and **184** comprises a communication module **402**, a microprocessor **404** and a secured element **406**. The secured devices **182** are provided at each CCTV camera at the upstream side, and the secured device **184** is provided at the downstream side such that data from the upstream sides are encrypted before travelling across the network and decrypted by the secured device at the downstream secured device. The communication module **402** provides communication ports for interfacing the CCTV cameras and the central recorder with the network **150**. Data passes through the secured data are being processed by the microprocessor **404** to encrypt/decrypt data with the keys possessed by the secured elements **406**. In effect, surveillance videos **410** from the CCTV cameras **110** are encrypted by the secured device **182**. The encrypted data **420** is then transmitted to the central recorder **120** through the network **150**. Without the secured device **184**, the encrypted data **420** would be meaningless to the central recorder **120**. Therefore, the secured device **184** is connected to the central recorder **120** to decrypt the encrypted data **420**. The decrypted data **430** may then process and store on the central recorder **120**.

[0041] For clarity, manufacturer of the CCTV camera and the central recorder may offer inbuilt standard encryptions/decryptions to the data. Therefore, the surveillance videos **410** may have already been encrypted before channeling into the secured device **182**. The present invention offers an additional, self-managed, point-to-

5 point hardware-based encryption to secure the data over the network.

[0042] The network **150** can be a dedicated CCTV network, or public network, such as internet.

[0043] As illustrated earlier, the CCTV camera **110** captures surveillance videos **410** for transmitting to the central recorder **120**.

10 **[0044]** In another embodiment, the communication module may comprise a wireless communication means, i.e. antenna. The wireless communication means is adapted to establish communication with the admin authenticators **292** of FIG. 2. In the case of smartcard as the admin authenticators **292**, the wireless communication means may further power up the components in the smartcard when in used.

15 **[0045]** FIG. 5 illustrates a block diagram of a secure device **500** in accordance with an alternative embodiment of the present invention. The secure device **500** comprises a microprocessor **502**, a FPGA Chip **504**, a secure element **506**, an ethernet transceiver **508** and an RJ46 socket **509**.

[0046] The microprocessor **502** acts as the control unit, managing data flow,

20 high-level tasks, and etc., while also handling communication protocols for the ethernet transceiver **508**. It hands over the data to the FPGA chip **504** for performing computationally intensive encryption or decryption tasks. The FPGA chip **504** works in

conjunction with the secure element **506** that handles key diversification, ensuring that encryption keys are unique and secure. This secure element **506** operationally generates or stores cryptographic keys, making it difficult for unauthorized parties to gain access. After the FPGA chip **504**, aided by the secure element **506**, completes the encryption or decryption, the microprocessor **502** performs additional tasks such as appending metadata, error checking, or routing the encrypted data to its destination. The microprocessor can also dynamically reconfigure the FPGA to switch between different algorithms as needed and manage other security measures.

[0047] It is well understood to a skilled person that the microprocessor **502** or the server/computer can be compromised by hacker or insider leak. Hence, the data in/out through the RJ45 socket **509** then the ethernet transceiver **508** is hardware encrypted/decrypted by the FPGA chip **504**. During the encryption/decryption, the FPGA chip **504** obtained keys from the secure element **506** where key diversification is carry out. So without the key, the data would be meaningless to any hacker or intruder who obtained them.

[0048] With the secure device **500** added to the upstream (i.e. CCTV camera) and downstream (i.e. CCTV recorder) of the CCTV system, the data transmitted through the communication network can be encrypted/decrypted through the secured device **500**.

[0049] In an alternative embodiment, the Secure Element (SE) collaborates with the Field-Programmable Gate Array (FPGA) chip to automatically validate the digital signatures of all received packets, including ICMP echo requests commonly known as "ping" packets. If the digital signature of an incoming packet does not align with the cryptographic computation performed internally by the SE, the packet is deemed to be

invalid. Consequently, the SE discards this packet without issuing any response, effectively rendering the device unresponsive to unauthorized ping requests, and making its IP address invisible to potential attackers.

[0050] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

Claims

1. A secure device adapted for CCTV network having a plurality of CCTV camera and a CCTV recorder, the secure device comprising:

a communication module having a socket for locally connecting to the CCTV camera or the CCTV recorder to transmit data over a communication network;

a microprocessor acts as a control unit for the secure device and handling the data flow;

an FPGA chip operationally encrypting/decrypting the data;

a secure element for handling key diversification for encrypting/decrypting the data by FPGA chip;

wherein the secure device is connected locally to the CCTV camera or CCTV recorder, operationally, encrypting/decrypting data transmitting through the communication network, such that the data is end-to-end encrypted across the CCTV network by the secure device.

15

2. The secure device of Claim 1, wherein the secure element is certified by Common Criteria (CC) or Federal Information Processing Standards (FIPS).

3. The secure device of Claim 1, wherein the secure device further comprises an admin authenticator for access authentication to the secure device.

20

4. The secure device of Claim 3, wherein the admin authenticator is in a card form having its own secure element embedded therein.

5. The secure device of Claim 3, wherein the admin authenticator is integrated on the secure device in a form of biometric scanner/sensor.

6. The secure device of Claim 3, wherein the admin authenticator is deployed
5 remotely from the secure device.

7. A surveillance system having a plurality of CCTV camera connected to a CCTV recorder via a communication network, wherein the communication network can be wired or wireless network, the surveillance system comprising:

10 a secure device of any one of the Claims 1- 6,
wherein the secure device is connected directly to the CCTV camera such that data passes through the secure device before transmitting to the communication network, and another secure device connected directly before the CCTV recorder.

15 8. A method for providing additional encryption/decryption for a surveillance system over a communication network, the method comprising:

adding secured devices to the surveillance system having CCTV cameras and CCTV recorder connected through a communication network;

activating secured elements of the secured devices;

20 encrypting data from CCTV cameras through the secured devices;

transmitting the encrypted data to the central recording system through the CCTV network; and

decrypting the encrypted by the secured devices for processing by the central reorder,

wherein data transmitted through the CCTV network is end-to-end encrypted by the secure devices.

9. The method of Claim 8, wherein the end-to-end encryption is done by the security
5 device in accordance with any one of claim 1-6.