

Method for Processing a Secure Financial Transaction Using a Commercial Off-The-Shelf or an Internet Of Things Device

BACKGROUND

Field of invention:

[001] The subject matter in general relates to digital payments. More particularly, but not exclusively, the subject matter relates to a COTS/IoT device based secure financial payment acceptance method and a device thereof.

Discussion of related art:

[002] In the digital world with digital economy trends, user requirements for security are increasingly becoming demanding. New challenges arise, since modern systems are becoming more and more complex, open and connected. Traditional security technologies are no longer able to handle the security requirements of such architectures. This certainly is explained by latest trends to integrate trusted computing concepts into embedded systems.

[003] Specifically, for a secured processing to take place on COTS/IoT devices, especially those involved with transfer of currencies, it is often lacking in terms of trust and identification. Various efforts have been made to tackle the issue of trust, non-tampered identification and when it involves currencies movement, the compliance perspective from

governing bodies. However, most if not all the solutions proposed were mainly driven from a software protection point of view, which either involved external eco system to support, high cost and yet susceptible to be tampered.

[004] In view of the forgoing problems there is a need for a new and/or improved technique to facilitate secure financial payment acceptance using COTS/IoT devices, without compromising on the terms of trust and identity of the COTS/IoT devices processing such transactions.

SUMMARY

[005] Accordingly, an improved technique to overcome the above problems is needed. To fulfill this need, system and method for processing a secure financial transaction using a Commercial off-the-shelf (COTS) or Internet of Things (IoT) device is provided. The method comprises requesting a Trusted Application Manager (TAM) Secure Provisioning Manager (SPM) to verify the COTS/IoT device identity and executing the application on a COTS/IoT device. Upon verification, TAM-SPM installs a Trusted Application (TA) in a Trusted Execution-Environment (TEE) of the COTS/IoT Device. Further, initiating a resonance response when a tag is within a predetermined distance from the COTS/ IoT device with TA installed, and receive the tag information from the tag. Finally, processing

a secure financial transaction using the COTS/IoT device based on the received tag information by accessing the TEE.

[006] In another embodiment, the COTS/IoT device includes a distributed ledger, and wherein the distributed ledger comprises information corresponding to at least one of COTS/IoT device ownership, manufacture, and usage information.

[007] In yet another embodiment, the information corresponding to the COTS/IoT device in the distributed ledger is modified through the TEE.

[008] In yet another embodiment, the application is executed in the operating system of the COTS/IoT device.

[009] In yet another embodiment, the ~~TAM~~ Secured Provisioning Manager (SPM) is a remote system which verifies the identity of the COTS/IoT device and installs the TA in the TEE of the COTS/IoT device.

[010] In yet another embodiment, the resonance response is performed multiple times, and a distance of the tag from the COTS/IoT device is calculated for each of the multiple resonance responses.

[011] In yet another embodiment, the secure financial transaction is initiated in an event a decrease in distance is identified in subsequent resonance responses using the COTS/IoT device.

[012] In yet another embodiment, the resonance response to calculate the distance is implemented using one or more of light proximity, sound proximity or accelerator in order to determine the relative distance,

for the payment processing to begin. The relative distance is configurable and is used for the purpose of fraud detection by ensuring the payment is initiated from a trusted/genuine payment card. The distance may be adjusted to accommodate changes to the guidelines pertaining to payment schemes at present and in future.

[013] In yet another embodiment, a COTS/IoT device for processing a secure financial transaction is provided. The COTS/IoT device is configured to request using the operating system part of the processor, a ~~Trusted Application Manager (TAM)~~ Secure Provisioning Manager (SPM) to verify device identity and install a Trusted Application (TA) in a ~~Trusted Execution Environment (TEE)~~ of the COTS/IoT Device, Wherein the ~~TEE~~ is isolated from the operating system of the COTS/IoT device and runs in parallel on a ~~TEE~~ part of the processor. Further, execute an application on a COTS/IoT device. Further, initiate, using the operating system part of the processor, a resonance response when a tag is within a predetermined distance from the COTS/IoT device with TA installed, and receive the tag information from the tag. Finally process, using the ~~TEE~~ part of the processor, a secure financial transaction using the COTS/IoT device based on the received tag information with secured PIN entry is performed. The COTS/IoT device further comprises a distributed ledger, and wherein the distributed ledger comprises information corresponding to at least one of COTS/IoT device ownership, manufacture, and usage information.

[014] Other objects, features, and advantages of the present invention will become apparent from the following detailed description. It should be however understood that the detailed description and specific examples, while indicating preferred embodiments of the present invention, are given by way of illustration only and various modifications may naturally be performed without deviating from the present invention.

BRIEF DESCRIPTION OF DIAGRAMS

[015] This disclosure is illustrated by way of example and not limitation in the accompanying figures. Elements illustrated in the figures are not necessarily drawn to scale, in which like references indicate similar elements and in which:

[016] FIG. 1 is an exemplary simple architecture of a Trusted ~~Execution~~ Environment (TEE) system 100 used for secure financial transactions, in accordance with an embodiment of the invention;

[017] FIG. 2 is an exemplary flow diagram 200 for deploying a Trusted Application (TA) in the TEE environment of the COTS/IoT device, in accordance with an embodiment of the invention;

[018] FIG. 3 illustrates an exemplary block diagram of a system 300 for secure financial transactions using a COTS/IoT device with added security by incorporating a distributed ledger among the COTS/IoT devices, in accordance with an embodiment of the invention;

[019] Fig. ~~4~~ ~~4A and 4B~~ illustrates an exemplary resonance response and a tag discovery, ~~distance or resonance response time calculation,~~

~~respectively~~, in accordance with an embodiment of the invention; and

[020] FIG. 5 is a flowchart of an exemplary method 500 for processing a secure financial transaction using a COTS/ IoT device, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[021] The following detailed description includes references to the accompanying drawings, which form part of the detailed description. The drawings show illustrations in accordance with example embodiments. These example embodiments are described in enough details to enable those skilled in the art to practice the present subject matter. However, it will be apparent to one of ordinary skill in the art that the present invention may be practised without these specific details. In other instances, well-known methods, procedures and components have not been described in detail so as not to unnecessarily obscure aspects of the embodiments. The embodiments can be combined, other embodiments can be utilized or structural and logical changes can be made without departing from the scope of the invention. The following detailed description is, therefore, not to be taken as a limiting sense.

[022] In this document, the terms “a” or “an” are used, as is common in patent documents, to include one or more than one. In this document, the term “or” is used to refer to a non-exclusive “or,” such that “A or B”

includes “A but not B,” “B but not A,” and “A and B,” unless otherwise indicated.

[023] It should be understood that the capabilities of the invention described in the present disclosure and elements shown in the figures may be implemented in various forms of hardware, firmware, software, non-transitory computer readable medium or combinations thereof.

[024] The embodiments disclose techniques for secure financial transaction acceptance using a Commercial off-the-shelf (COTS) device or Internet of Things (IoT) device. For example, embodiments provide a COTS/IoT device for processing a secure financial transaction. The COTS/IoT device is configured to execute, using an operating system part of a processor, an application on a COTS/IoT device. Further, request using the OS part of the processor, a Trusted Application Manager (TAM), Secure Provisioning Manager (SPM) to verify and install a Trusted Application (TA) in a Trusted Execution-Environment (TEE) of the COTS/~~IoT~~-IoT Device.

[025] The TEE of the COTS/IoT device is isolated from the OS environment of the COTS/IoT device and both run in parallel. Further, a resonance response is initiated when a tag is within a predetermined distance from the COTS/IoT device and the tag information is received from the tag. Further a secure financial transaction is processed using the COTS/IoT device based on the received tag information by accessing the

TEE part of the processor. The COTS/IoT device further comprises a distributed ledger, which comprises information corresponding to at least one of COTS/IoT device ownership, manufacture, and usage information.

[026] FIG. 1 is an exemplary simple architecture of a Trusted Execution Environment (TEE) system 100 used for secure financial transactions, in accordance with an embodiment of the invention. As illustrated in the figure 1, the Operating System (OS) application environment and Trusted Execution Environment (TEE) co-exist in the COTS/IoT device. TEE comprises a small secure kernel that shares the processor with OS application environment. Since both critical and non-critical applications run on COTS/IoT devices, such as mobile phones, laptops, and tablets, among other devices, the sensitive elements of the critical applications may be executed in TEE in isolation from OS application environment. This facilitates extra level of security as the associated code and data may be protected from more vulnerable OS side of the COTS/IoT device. This architecture guarantees better data integrity as the data cannot be modified by unauthorized or undetected users/programs. Confidential data or code may be stored in the TEE, whereas, the same the confidential data or code may also be stored in the OS in encrypted form but doesn't guarantee the level of security provided by TEE.

[027] The execution of a Trusted Application (TA) in TEE may affect

execution of applications in OS, however, execution in the OS cannot interfere with the execution in TEE. The application running on OS may request to execute code or verify tokens/keys through the TEE client API. Further, the TEE may execute respective TA or verify keys/tokens and provide the result to the TEE client API.

[028] In an embodiment, the COTS/IoT devices may include smart phones, laptops, computers, tablets, and smart watches, among other COTS/IoT devices known in the art.

[029] FIG. 2 is an exemplary flow diagram 200 for deploying a Trusted Application (TA) in the TEE environment of the COTS/IoT device, in accordance with an embodiment of the invention. The ~~Trusted Application Manager (TAM)~~ Secure Provisioning Manager (SPM) is a remote server configured to establish communication with the TEE of the COTS/IoT device. ~~TAM-SPM~~ may also authorize the installation of the Trusted Application in the TEE of the COTS/IoT device. ~~TAM-SPM~~ may further be configured to push data or other confidential keys for a TA into the TEE.

[030] The application store may a platform on which a developer/company may host their applications for download. The users of the COTS/IoT devices may download an application from the application store. The typical examples of application store may include *Google Play* and *App Store* by Apple, among others.

[031] Referring to Fig. 2, in the flow diagram the flow 'a' indicates a developer/company involved in developing an application which is hosted in the app store. It shall be understood that, for the sake of simplicity the TAM-SPM and developer/company have been grouped into one, however it is always possible that the developer/company may be different from TAM-SPM. Also, it shall be noted that the application is signed as a Trusted Application by TAM-SPM or Manufactures before moving to TAM-SPM.

[032] The flow 'b' indicates creating a security domain after the application is downloaded and running for the first time in the COTS/IoT device. The security domain is a place where keys can be stored, where the trusted application when at rest may be encrypted to keep safe.

[033] Further, at flow 'c' the application requests the TAM-SPM to approve the installation of the TA in the TEE. The TAM-SPM at flow 'd' may perform several checks such as verifying the identity of the COTS/IoT device, verifying whether it's a trust worthy end point, and keep a track of the number of trusted applications deployed, among others, and upon positive verification issue a token/key to authorise the installation of TA in the TEE of the COTS/IoT device.

[034] Further, at flow 'e' the TA is installed in the TEE of the COTS/IoT device and is safely stored in TEE. Additionally, the TAM-SPM may also share some personalisation data to the application. The identifier 'f'

indicates the positively verified and installed TA loaded into the TEE of the COTS/IoT device.

[035] FIG. 3 illustrates an exemplary block diagram of a system 300 for secure financial transactions using a COTS/IoT device with added security by incorporating a distributed ledger among the COTS/IoT devices, in accordance with an embodiment of the invention.

[036] As illustrated in the figure 3 the system 300 includes an COTS/IoT device 1. The COTS/IoT device 1 includes an application for processing a secure payment by accessing a trusted application (TA) installed in the TEE. The TE is the secured part of the COTS/IoT devices. The TEE is isolated from the operating system of the COTS/IoT device and runs in parallel on a TEE part of the processor. Further, when a tag as illustrated in the figure is brought close to the COTS/IoT device a resonance response is initiated.

[037] In an embodiment, the tag may include, but not limited to, for example a credit card, debit card, smart watch, and a smart ring, among other devices capable of storing information pertaining to payment credentials.

[038][037] In an embodiment, the resonance response may be initiated only the tag is within a predetermined distance from the COTS/ IoT device. In response to the resonance response the TAG may share the

information corresponding to the tag with the COTS/IoT device for processing a payment.

~~[039]~~[038] Fig. ~~4 4A and 4B~~ illustrates an exemplary resonance response and a tag discovery, ~~distance or resonance response time calculation, respectively,~~ in accordance with an embodiment of the invention. As indicted in the Fig. ~~4 4A the~~ when the TAG is within the range of the actual signal strength 'm' it may be discoverable by the COTS/IoT device. However, the information for the tag may not be accepted until the tag is within the distance of 'n' form the COTS/IoT device.

~~[040]~~[039] In an embodiment, the distance of the tag is continuously monitored upon its discovery. Further, in the event the distance calculated in a first resonance response is greater than the distance calculated in the second or subsequent resonance response, and the tag is within the predetermined distance from the COTS/IoT device, the tag information may be received by the COTS/IoT device. The financial transaction may be initiated thereafter.

~~[041]~~[040] In an embodiment, different techniques may be adapted to implement a resonance response for example, but not limited to, using one or more of light proximity, sound proximity and relative distance, among other techniques known in the art.

~~[042]~~[041] Referring back to Fig. 3, as illustrated the plurality of COTS/IoT

devices may share a distributed ledger among themselves. This may be implemented using state-of-the-art distributed ledger technologies such as, but not limited to, Blockchain and Hash graph, among other technologies. The distributed ledger may include information corresponding to the unique identification number of the COTS/IoT device, ownership of the COTS/IoT device, usage information of the COTS/IoT device, and manufacture information of the COTS/IoT device, among other information.

~~[043]~~[042] The information corresponding to accessing the distributed ledger, such as the private key and other cryptos may also be stored in the TEE, through an update via ~~TAM-SPM~~ to the TA.

~~[044]~~[043] This enables tracking the ownership details of the device. Further crowd leasing may also be facilitated i.e. allowing ownership of the devices via “crowd leasing” approach and genuinely identifying individual of the lease. The duration of ownership may also be recorded, and this enables distribution of return of the leasing if desired. The usage/consumption information may include, but not limited to, estimated lifespan of the device, automation of maintenance, and charging by usage, among others.

~~[045]~~[044] FIG. 5 is a flowchart of an exemplary method 500 for processing a secure financial transaction using a COTS/ IoT device, in accordance with an embodiment of the invention. The method 500 may be

implemented in a COTS/IoT device. The COT/IoT device is embedded with a unique key during the manufacturing stage. Further, a developer application may be signed by a ~~TAM~~SPM so that the TA can be installed in the TEE of COTS/IoT. At step 502 a request to install a trusted application in the TEE of the COTs/IoT device may be send to the ~~TAM~~SPM. Further, upon positive verification the application may be executed on the COTS/IoT device at step 504.

~~[046]~~[045] Further, at step 506, a resonance response may be initiated when a tag is discovered to be within a predetermined distance from the COTS/IoT device. Thereafter, at step 508 the information from the tag is used to process a secure financial transaction using the COTS/IoT device by accessing the TEE. Further, at step 510, a distributed ledger such as blockchain or hash graph may be implemented to maintain a ledger in all the COTS/IoT devices. The distributed ledger may comprise information corresponding to ownership, usage information, and manufacturer of the COT/IoT device, among other details.

~~[047]~~[046] In the foregoing detailed description, numerous specific details, examples, and scenarios are explained in order to facilitate a thorough understanding of the present disclosure. However, the embodiments of the disclosure may be practiced without such specific details. Further, such examples and scenarios are provided for illustration, and are not intended to limit the disclosure in any way. Those of ordinary skill in the art, with the

included descriptions, should be able to implement appropriate functionality without undue experimentation. Thus, the scope of the invention should be determined by the appended claims and their legal equivalents rather than by details, examples, and scenarios provided.

~~{048}~~~~{047}~~ It shall be noted that the processes described above are described as sequence of steps; this was done solely for the sake of illustration. Accordingly, it is understood that some steps may be added, some steps may be omitted, the order of the steps may be re-arranged, or some steps may be performed simultaneously.

~~{049}~~~~{048}~~ Although embodiments have been described with reference to specific example embodiments, it will be evident that various combinations, modifications, additions, and omissions may be made to these embodiments without departing from the broader spirit and scope of the foregoing disclosure and appended claims. Accordingly, the specification and drawings are to be regarded in an illustrative sense rather than a restrictive sense. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation.

CLAIMS

I/we claim:

1. A method for processing a secure financial transaction of fiat currencies using a Commercial off-the-shelf (COTS) or Internet of

Things (IoT) device, the method comprising:

in the COTS/IoT device:

requesting a Trusted Application Manager (TAM) by the COTS/IoT device, a Secure Provisioning Manager (SPM) to verify a device identity and deploy a Trusted Application (TA) in a Trusted ~~Execution~~ Environment (TE~~E~~) of the COTS/IoT Device, wherein the TE is secured part of the COTS/IoT device where TA run; ~~Wherein~~ the TE comprises a small secure kernel that shares the processor with an OS application environment for isolating the TEE is isolated from the operating system of the COTS/IoT device, and for enabling the sensitive elements of the critical applications to be executed in TE in isolation from the OS application environment which provides protection from vulnerable OS side of the COTS/IoT device, and wherein the TE and the operating system of the COTS/IoT runs in parallel on a TE part of the processor;

executing an application on a the COTS/IoT device;

determining a distance of a tag from the COTS/IoT device;

initiating a resonance response when a the tag is determined

to be within a predetermined distance from the COTS/ IoT device with TA installed, and receive the tag information from the tag; and

processing a secure financial transaction using the COTS/IoT device based on the received tag information by accessing the TEE, wherein the resonance response is performed multiple times, and a distance of the tag from the COTS/IoT device is calculated for each of the multiple resonance responses, wherein the distance of the tag from the COTS/IoT device is continuously monitored upon its discovery, and wherein the secure financial transaction is initiated in an event a decrease in distance is identified in subsequent resonance responses using the COTS/IoT device;

wherein the predetermined distance of the tag is calculated based on the COTS/IoT device profile;

wherein the predetermined distance of the tag from the COTS/IoT device is continuously monitored upon its discovery, whereby in the event the distance calculated in a first resonance response is greater than the distance calculated in the second or subsequent resonance response, and the tag is within the predetermined distance from the COTS/IoT device, the tag information may be received by the COTS/IoT device thus the financial transaction may be initiated thereafter;

wherein the resonance response to calculate the distance is

implemented using a combination of light proximity, sound proximity or accelerator to determine the relative distance for the payment process to begin; and
wherein the distance is adjustable for fraud detection and for payment scheme compliance.

2. The method according to claim 1, wherein the COTS/IoT device includes a distributed ledger, and wherein the distributed ledger comprises information corresponding to at least one of COTS/IoT device ownership, manufacture, and usage information.

~~3. The method according to claim 2, wherein the information corresponding to the COTS/IoT device in the distributed ledger is modified through the TEE.~~

~~5. The method according to claim 1, wherein the application is executed in the operating system of the COTS/IoT device.~~

~~7.3.~~ The method according to claim 1, wherein the ~~TEM-SPM~~ is a remote system ~~which verifies configured to verify~~ the identity of the COTS/IoT device and ~~installs to install~~ the TA in the TEE of the COTS/IoT device.

~~8. The method according to claim 1, wherein the resonance response~~

~~is performed multiple times, and a distance of the tag from the COTS/IoT device is calculated for each of the multiple resonance responses; and~~

~~wherein the secure financial transaction is initiated in an event a decrease in distance is identified in subsequent resonance responses using the COTS/IoT device.~~

~~11. The method according to claim 6, wherein the resonance response to calculate the distance is implemented using one or more of light proximity, sound proximity or accelerator to determine the relative distance for the payment process to begin; wherein the distance is adjustable for fraud detection and for payment scheme compliance.~~

~~12.4. _____ A Commercial off-the-shelf (COTS) or an Internet of Things (IoT) device for processing a secure financial transaction, the COTS/IoT device is configured to comprising:~~

~~_____ a processor comprising an operating system operable to:~~

~~execute, using an operating system part of a processor, an application on a the COTS/IoT device;~~

~~request, using the operating system part of the processor, a Trusted Application Manager (TAM) a Secure Provisioning Manager (SPM) to verify device identity and install a Trusted Application (TA) in a Trusted Execution Environment (TEE) of the COTS/IoT Ddevice,~~

wherein the TE comprises a small secure kernel that shares the processor with OS application environment for isolating the TE from the operating system of the COTS/IoT device and for enabling the sensitive elements of the critical applications to be executed in TE in isolation from the OS application environment which provides protection from vulnerable OS side of the COTS/IoT device, and ~~Wherein the TEE is isolated from and the~~ operating system of the COTS/IoT ~~device and runs~~ in parallel on a TEE part of the processor; wherein the TE is secured part of the COTS/IoT device and runs:

execute an application on ~~a~~ the COTS/IoT device;

initiate, ~~using the operating system part of the processor,~~ a resonance response when a tag is within a predetermined distance from the COTS/ IoT device with TA installed, and receive the tag information from the tag; and

process, ~~using the operating system part of the processor,~~ a secure financial transaction using the COTS/IoT device based on the received tag information by accessing the TEE part of the processor, wherein the resonance response is performed multiple times, and a distance of the tag from the COTS/IoT device is calculated for each of the multiple resonance responses, the distance of the tag is continuously monitored upon its discovery, and wherein the secure financial transaction is initiated in an event

a decrease in distance is identified in subsequent resonance responses using the COTS/IoT device;

wherein the predetermined distance of the tag from the COTS/IoT device is calculated based on the COTS/IoT device profile;

wherein the predetermined distance of the tag from the COTS/IoT device is continuously monitored upon its discovery, whereby in the event the distance calculated in the second or subsequent resonance response, and the tag is within the predetermined distance from the COTS/IoT device, the tag information may be received by the COTS/IoT device thus the financial transaction may be initiated thereafter;

wherein the resonance response to calculate the distance is implemented using a combination of light proximity, sound proximity or accelerator to determine the relative distance for the payment process to begin; and wherein the distance is adjustable for fraud detection and for payment scheme compliance.

~~13.5.~~ The COTS/IOT device according to claim ~~8~~ 4, wherein the COTS/IoT device further comprises a distributed ledger, and wherein the distributed ledger comprises information corresponding to at least one of COTS/IoT device ownership, manufacture, and usage information.

~~14. The COTS/IoT device according to claim 9, wherein the information corresponding to the COTS/IoT device in the distributed ledger is modified through the TEE.~~