MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

DOMANDA DI INVENZIONE NUMERO	**102015000089367**
Data Deposito	**31/12/2015**
Data Pubblicazione	**01/07/2017**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	L	29	06

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	L	29	08

Titolo

SISTEMA DI CRIPTAZIONE PER LE COMUNICAZIONI NELL?INTERNET DELLE COSE

SISTEMA DI CRIPTAZIONE PER LE COMUNICAZIONI NELL'INTERNET DELLE COSE

***

La presente invenzione si riferisce ad un sistema di criptazione per le comunicazioni nella Internet delle Cose che consente in modo semplice, affidabile, efficiente ed economico di rendere le comunicazioni scambiate nella cosiddetta Internet delle Cose, usualmente denominata IoT (Internet of Things), sicure ed accessibili soltanto ad operatori autorizzati, garantendo la confidenzialità e la segretezza dei dati e delle informazioni oggetto delle comunicazioni stesse, consentendo opzionalmente agli operatori di selezionare il livello di sicurezza delle comunicazioni da essi generate.

Negli ultimi decenni, lo sviluppo delle strutture tecnologiche complessivamente indicate con la definizione "Internet delle cose", o IoT (Internet of Things) ha condotto all'estensione della rete Internet a strutture formate da oggetti e luoghi reali, che vengono equipaggiati con circuiti elettronici, generalmente provvisti di sensori, in grado di comunicare tra loro e con una centrale remota.

In particolare, gli oggetti più disparati vengono dotati di dispositivi elettronici, miniaturizzati e spesso autoalimentati, in grado di trasmettere informazioni ambientali o sullo stato dell'oggetto ospitante, per cui si può conferire all'oggetto stesso un certo livello di "intelligenza". L'oggetto acquisisce, quindi, un ruolo attivo trasmettendo e/o ricevendo attraverso la rete Internet una quantità di informazioni che, opportunamente elaborate ed aggregate, forniscono indicazioni importanti e risultano utili a prendere una serie di azioni conseguenti. A titolo puramente esemplificativo, e non a titolo limitativo, un orologio sveglia può riceve i dati sul traffico relativo alla tratta che l'utente deve compiere al mattino e regolare l'orario della sveglia in conformità a tale informazione, per cui, in caso di presenza di ingorghi lungo la tratta, potrebbe attivarsi con un anticipo temporale (calcolato dal medesimo orologio sveglia sulla base delle informazioni di traffico ricevute) rispetto all'orario impostato dall'utente.

La continua evoluzione, miniaturizzazione e diffusione delle tecnologie

elettroniche abilitanti, quali la microelettronica, l'informatica, le comunicazioni wireless e le reti di comunicazione, assieme alla sempre più ridotta richiesta di energia per il loro funzionamento, hanno reso possibile il tracciamento di una "mappa informatica" che rappresenta ciò che accade nel mondo reale, trasmettendo in tempo reale dati ed informazioni a bassissimi costi e senza necessità di interventi di manutenzione.

Tutto ciò ha aperto la possibilità di utilizzo della IoT ad una miriade di campi operativi ed applicazioni, quali ad esempio: la domotica; la telemetria; gli apparati e sistemi di generazione e distribuzione di energia elettrica (smart grid energetiche); le città intelligenti (smart cities); le tecnologie biomedicali; la robotica; l'industria automobilistica e, più in generale, l'industria dei trasporti; la tecnologia di monitoraggio e controllo a distanza.

L'integrazione e la sinergia delle tecnologie, assieme all'esplorazione delle varie applicazioni, si possono dire ad oggi ancora in uno stato iniziale e, pertanto, le vere potenzialità della IoT sono ancora largamente inesplorate. Più precisamente, non esiste ad oggi un "sistema integrato IoT", ma lo stato di sviluppo attuale ha reso intelligenti gli oggetti assemblando tra loro una serie di tecnologie già sviluppate per altri scopi al fine di assoggettarle anche alle necessità che il loro utilizzo nella IoT richiede.

E' per questo motivo che, allorquando si affronti l'Internet delle Cose come un sistema integrato, affiorano in realtà alcune necessità a cui a tutt'oggi non è stato fatto ancora fronte in una maniera globale.

Una di queste necessità è la confidenzialità e la segretezza dei dati e delle informazioni oggetto delle comunicazioni scambiate nella IoT, poiché le tecniche convenzionali già sviluppate per altri scopi non si adattano al contesto di un sistema integrato IoT.

Infatti, la direzione del flusso di informazioni è caratterizzata da un gerarchia di tecnologie. La rilevazione dei dati sul e dall'oggetto deve essere fatta necessariamente con elettronica minimale, bassissimi consumi, altissima affidabilità (assenza di necessità di interventi di manutenzione) e quindi costi irrisori. Tipi-

camente, i dati rilevati e trasmessi dall'oggetto reso intelligente sono ridotti al minimo indispensabile e semplificati al massimo e la trasmissione è basata su tecnologie a corto o medio raggio. Ciò richiede spesso l'adozione di un ulteriore oggetto elettronico, che nel seguito viene denominato oggetto instradatore, capace di ricezione, aggregazione dati, elaborazione e ritrasmissione verso una o più centrali remote ancora più complesse configurate per ricevere ed analizzare dati ed informazioni e/o verso una nuvola informatica, usualmente denominata "cloud", ovvero verso una struttura distribuita di apparati di memorizzazione ed elaborazione.

E' possibile utilizzare come similitudine alla gerarchia necessaria alla IoT il modo di operare della rete di comunicazione cellulare, dove il telefono cellulare dell'utente è paragonabile all'elettronica (ad esempio comprendente uno o più sensori) che è alloggiata negli oggetti della IoT. Il telefono cellulare, sia per necessità energetiche che per complessità dell'elettronica con cui è equipaggiato, necessita di comunicare con la stazione base (della cellula in cui si trova e) che è relativamente vicina, che è già più ingombrante, costosa ed energivora dal momento che è in grado di svolgere funzioni molto più complesse dello stesso telefono cellulare, oltre a capacità elaborative e di trasmissione a più lunga distanza verso una (o più) centrale di gestione delle comunicazioni cellulari che è a distanze maggiori ed a sua volta risulta più ingombrante, costosa ed energivora della stazione base (della cellula in cui si trova il telefono cellulare) in quanto svolge funzioni ancora più complesse, gestisce molto più traffico informativo ed è dotata di ben maggiori capacità di elaborazione. Analogamente, nella IoT, i singoli oggetti sono gerarchicamente relazionati agli oggetti instradatori come i telefoni cellulari sono gerarchicamente relazionati alle stazioni base, e gli oggetti instradatori sono a loro volta gerarchicamente relazionati alle centrali remote come le stazioni base sono gerarchicamente relazionate alla centrale di gestione delle comunicazioni cellulari.

Sebbene alcuni dei numerosi campi operativi ed applicazioni in cui viene utilizzata la IoT hanno scarsa o perfino nessuna necessità di proteggere la confi-

denzialità e la segretezza di dati ed informazioni scambiati con le comunicazioni nella IoT, tuttavia in molti di tali campi operativi ed applicazioni la confidenzialità di dati ed informazioni scambiati riveste vari livelli di importanza, ed in alcuni campi operativi ed applicazioni la segretezza risulta indispensabile.

Attualmente, l'adozione di tecniche volte ad assicurare la confidenzialità e la segretezza di dati ed informazioni scambiati con le comunicazioni nella IoT è ancora largamente mancante e le poche soluzioni proposte nella tecnica anteriore si basano su apparati tanto complessi e costosi da risultare incompatibili con i benefici ottenibili dall'intelligenza impiantata negli oggetti che fanno parte della IoT. Di conseguenza, anche nelle applicazioni operative della IoT che hanno la necessità di comunicare dati sensibili, questi vengono trasmessi senza alcuna protezione che ne garantisca adeguatamente la confidenzialità e la segretezza, rischiando un abuso di parte di terzi non autorizzati che possono intercettare tali dati sensibili.

Scopo della presente invenzione, quindi, è quello di consentire in modo semplice, affidabile, efficiente ed economico di rendere le comunicazioni scambiate nella IoT sicure ed accessibili soltanto ad operatori autorizzati, garantendo la confidenzialità e la segretezza dei dati e delle informazioni oggetto delle comunicazioni stesse.

Ulteriore scopo della presente invenzione, quindi, è quello di consentire opzionalmente agli operatori di selezionare il livello di sicurezza delle comunicazioni da essi generate.

Forma oggetto specifico della presente invenzione un sistema di criptazione per le comunicazioni nella IoT comprendente uno o più dispositivi elettronici criptatori-decriptatori, ognuno dei quali è provvisto di una unità di elaborazione collegata ad una memoria che memorizza chiavi ed uno o più algoritmi di criptazione e ad una interfaccia di comunicazione configurata per essere collegata ad uno o più sensori e/o uno o più attuatori, l'unità di elaborazione essendo configurata per criptare dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori, in cui ogni dispositivo elettronico criptatore-decriptatore è

collegato ad una rete di comunicazioni cui è collegata anche una piattaforma web che è configurata per selezionare, per ogni dispositivo elettronico criptatore-decriptatore, l'algoritmo di criptazione che questo utilizza per criptare dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori, ogni dispositivo elettronico criptatore-decriptatore essendo configurato per trasmettere alla piattaforma web dati criptati, la piattaforma web essendo provvista di una o più unità di elaborazione collegate ad una o più memorie che memorizzano chiavi ed uno o più algoritmi di decriptazione necessari per decriptare dati criptati provenienti da ogni dispositivo elettronico criptatore-decriptatore.

Secondo un altro aspetto dell'invenzione, la piattaforma web può essere configurata per selezionare o deselezionare una criptazione da parte dell'unità di elaborazione di un dispositivo elettronico criptatore-decriptatore dei dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori collegati all'interfaccia di comunicazione di tale dispositivo elettronico criptatore-decriptatore.

Secondo un ulteriore aspetto dell'invenzione, la piattaforma web può essere configurata per selezionare un algoritmo di criptazione che l'unità di elaborazione di un dispositivo elettronico criptatore-decriptatore è configurato per utilizzare per criptare i dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori collegati all'interfaccia di comunicazione di tale dispositivo elettronico criptatore-decriptatore, e/o un algoritmo di decriptazione che dette una o più unità di elaborazione sono configurate per utilizzare per decriptare i dati criptati provenienti da tale dispositivo elettronico criptatore-decriptatore.

Secondo un aspetto aggiuntivo dell'invenzione, la piattaforma web può essere configurata per generare dati di controllo per controllare un funzionamento e/o uno stato di uno o più sensori e/o di uno o più attuatori, per criptare detti dati di controllo mediante dette una o più unità di elaborazione secondo chiavi ed uno o più algoritmi di criptazione memorizzati in dette una o più memorie, e per trasmettere detti dati di controllo criptati ad un dispositivo elettronico criptatore-decriptatore, cui sono collegati detti uno o più sensori e/o uno o

più attuatori controllati da detti dati di controllo, la cui unità di elaborazione è configurata per decriptare, mediante chiavi ed uno o più algoritmi di decriptazione memorizzati nella sua memoria, dati di controllo criptati provenienti dalla piattaforma web.

Secondo un altro aspetto dell'invenzione, la piattaforma web può essere configurata per selezionare o deselezionare una criptazione da parte di dette una o più unità di elaborazione di detti dati di controllo.

Secondo un ulteriore aspetto dell'invenzione, la piattaforma web può essere configurata per selezionare un algoritmo di criptazione che dette una o più unità di elaborazione sono configurate per utilizzare per criptare detti dati di controllo, e/o un algoritmo di decriptazione che l'unità di elaborazione di un dispositivo elettronico criptatore-decriptatore è configurato per utilizzare per decriptare detti dati di controllo criptati provenienti dalla piattaforma web.

Secondo un aspetto aggiuntivo dell'invenzione, la piattaforma web può essere configurata per selezionare un protocollo di comunicazione che almeno parte di detti uno o più dispositivi elettronici criptatori-decriptatori e la piattaforma web debbono utilizzare per trasmettersi dati nella rete di comunicazioni.

Secondo un altro aspetto dell'invenzione, la piattaforma web può essere configurata per essere accessibile da remoto per mezzo di un'applicazione web da parte di almeno un utente autorizzato.

Secondo un ulteriore aspetto dell'invenzione, l'interfaccia di comunicazione di uno o più dispositivi elettronici criptatori-decriptatori può essere configurata per essere collegata ad uno o più sensori di tipo Grove e/o uno o più attuatori di tipo Grove.

Secondo un aspetto aggiuntivo dell'invenzione, la piattaforma web può essere configurata per aggiornare da remoto chiavi ed algoritmi di criptazione e/o algoritmi di decriptazione memorizzati nella memoria di uno o più dispositivi elettronici criptatori-decriptatori.

Secondo un altro aspetto dell'invenzione, la piattaforma web può essere configurata per aggiornare una modalità di funzionamento di uno o più dispositi-

vi elettronici criptatori-decriptatori.

La presente invenzione si basa su un innovativo arrangiamento di componenti facenti parte di una IoT integrata che è configurato per avvalersi di tecniche di crittografia e tecniche di cifratura.

Il sistema di criptazione per le comunicazioni nella IoT consente di risolvere i problemi della tecnica anteriore con riferimento alla confidenzialità e segretezza di dati ed informazioni oggetto delle comunicazioni stesse le cui caratteristiche tecniche sono integrabili in qualsiasi applicazione della IoT, opzionalmente con vari livelli di complessità e sicurezza della cifratura sia dei dati che delle loro trasmissioni, adattando le necessità di criptazione alle necessità della specifica applicazione.

La presente invenzione sarà ora descritta, a titolo illustrativo, ma non limitativo, secondo sue preferite forme di realizzazione, con particolare riferimento ai disegni dell'unica Figura allegata, indicata come Figura 1, che mostra una rappresentazione schematica di una preferita forma di realizzazione del sistema di criptazione per le comunicazioni nella IoT.

Con riferimento alla Figura 1, si può osservare che la preferita forma di realizzazione del sistema di criptazione per le comunicazioni nella IoT secondo l'invenzione comprende un dispositivo elettronico criptatore-decriptatore 100, provvisto di una unità 110 di elaborazione (e.g. un microcontrollore od un microprocessore) collegata ad una memoria 120 che memorizza chiavi ed uno o più algoritmi di criptazione per criptare i dati provenienti da uno o più (in generale una pluralità di) sensori e/o da uno o più (in generale una pluralità di) attuatori. A tale scopo, il dispositivo elettronico criptatore-decriptatore 100 è altresì provvisto di una interfaccia di comunicazione bidirezionale (non mostrata in Figura), opzionalmente wireless, collegata alla unità 110 di elaborazione e configurata per essere collegata ad uno o più sensori esterni, opzionalmente uno o più sensori di tipo Grove, e/o uno o più attuatori esterni, opzionalmente uno o più attuatori di tipo Grove; in tal modo, il dispositivo elettronico criptatore-decriptatore 100 collega tra loro i sensori e gli attuatori collegati alla sua interfaccia di comunicazio-

ne. Tale possibilità di collegamento tra dispositivo elettronico criptatore-decriptatore 100 e sensori ed attuatori esterni, in particolare quando questi sono di tipo Grove, è estremamente flessibile.

Si deve tenere presente che, benché in Figura 1 sia mostrato un solo dispositivo elettronico criptatore-decriptatore 100, il sistema secondo l'invenzione può comprendere anche una pluralità di analoghi dispositivi elettronici criptatori-decriptatori, ognuno dei quali è collegato tramite la propria interfaccia di comunicazione ad un rispettivo insieme di uno o più sensori e/o uno o più attuatori.

Come mostrato in Figura 1, nella preferita forma di realizzazione del sistema di criptazione per le comunicazioni nella IoT secondo l'invenzione, ogni dispositivo elettronico criptatore-decriptatore 100 è collegato ad una rete 200 di comunicazioni, opzionalmente la rete Internet, tramite la quale una piattaforma web 300, opzionalmente su un cloud (ovvero realizzata mediante una struttura distribuita di apparati di memorizzazione ed elaborazione), gestisce ogni dispositivo elettronico criptatore-decriptatore 100, ad esempio selezionando l'algoritmo di criptazione da utilizzare per la criptazione dei dati che quest'ultimo riceve dai sensori e/o attuatori ad esso collegati.

La piattaforma web 300 comprende una o più unità 310 di elaborazione collegate ad una o più memorie 320 che memorizzano i dati dei sensori e/o degli attuatori che provengono da ogni dispositivo elettronico criptatore-decriptatore 100, nonché le chiavi e gli algoritmi di decriptazione necessari per decriptare (se necessario) i dati e le informazioni provenienti da ogni dispositivo elettronico criptatore-decriptatore 100. In particolare, dette una o più unità 310 di elaborazione sono configurate per decriptare (se necessario) i dati e le informazioni provenienti da ogni dispositivo elettronico criptatore-decriptatore 100 e li inoltra, opzionalmente tramite uno o più specifici dispositivi 340 di comunicazione, a diverse altre piattaforme esterne utilizzando, per esempio, protocolli di comunicazione diversi; a titolo esemplificativo, e non a titolo limitativo, in Figura 1 è mostrato un apparato 340 di comunicazione della piattaforma web 300 che è configurato per trasmettere i dati e le informazioni ad una piattaforma cloud 400 che

li memorizza ed alla quale un utente (e.g. l'utente gestore dei sensori e/o degli attuatori cui si riferiscono i dati e le informazioni) può accedere per scopi di consultazione e/o controllo. In proposito, dette una o più unità 310 di elaborazione, dette una o più memorie 320 e detti uno o più specifici dispositivi 340 di comunicazione possono essere implementati da uno o più server.

Inoltre, la piattaforma web 300 è configurata per generare dati di controllo per controllare il funzionamento e/o lo stato di detti uno o più sensori e/o di detti uno o più attuatori, per criptare (mediante dette una o più unità 310 di elaborazione) tali dati di controllo secondo chiavi ed uno o più algoritmi di criptazione memorizzati in dette una o più memorie 320, e per trasmetterli al dispositivo elettronico criptatore-decriptatore 100 cui sono collegati i relativi sensori e/o attuatori secondo uno specifico protocollo di comunicazione; in tal caso, l'unità 110 di elaborazione del dispositivo elettronico criptatore 100 è configurata per decriptare, mediante chiavi ed uno o più algoritmi di decriptazione memorizzati nella memoria 120, tali dati di controllo criptati provenienti dalla piattaforma web 300.

La piattaforma web 300 è configurata per essere accessibile da remoto, per mezzo di un'applicazione web (e.g. un sito web), indicata in Figura con il numero di riferimento 330, da parte di almeno un utente autorizzato, opzionalmente mediante l'inserimento di dati di identificazione (e.g. user-id e password, certificato digitale, o dati biometrici quale un'impronta digitale), il quale può controllare il livello di sicurezza delle comunicazioni tra uno o più dispositivi elettronici criptatori-decriptatori 100 e la piattaforma web 300 (e le eventuali ulteriori piattaforme esterne 400). A titolo esemplificativo, un utente autorizzato può selezionare se criptare o meno le comunicazioni tra uno o più specifici dispositivi elettronici criptatori-decriptatori 100 e la piattaforma web 300, e, quando sia stata selezionata la criptazione dei dati, l'utente autorizzato può selezionare uno degli algoritmi di criptazione, memorizzati nella memoria 120 di uno specifico dispositivo elettronico criptatore-decriptatore 100, ed un corrispondente algoritmo di decriptazione, tra gli algoritmi di decriptazione memorizzati in dette una o

più memorie 320 della piattaforma web 300, da utilizzare per criptare i dati provenienti dai sensori, e/o può selezionare uno degli algoritmi di criptazione, memorizzati in dette una o più memorie 320 della piattaforma web 300, ed un corrispondente algoritmo di decriptazione, tra gli algoritmi di decriptazione memorizzati nella memoria 120 di uno specifico dispositivo elettronico criptatore-decriptatore 100, da utilizzare per decriptare i dati di controllo da inviare agli attuatori collegati a tale specifico dispositivo elettronico criptatore-decriptatore 100, in modo tale da selezionare; inoltre, l'utente autorizzato può selezionare un particolare protocollo di comunicazione che (almeno parte di) detti uno o più dispositivi elettronici criptatori-decriptatori 100 e la piattaforma web 300 debbono utilizzare, in modo che dati ed informazioni siano trasmessi nella rete 200 di comunicazioni (ad esempio la rete Internet) in modalità sicura, per esempio utilizzando un protocollo https. Per analogia con l'invio di comunicazioni tramite posta, è come se il contenuto della lettera venisse criptato con un algoritmo selezionato dall'utente autorizzato e poi questa lettera criptata fosse imbustata e spedita in una modalità sicura nella rete 200 di comunicazioni.

Per mezzo della piattaforma web 300, un utente autorizzato ha altresì la possibilità di controllare e monitorare il funzionamento da remoto di sensori e/o attuatori collegati ad uno o più dispositivi elettronici criptatori-decriptatori 100.

Inoltre, la piattaforma web 300 può altresì aggiornare da remoto le chiavi e gli algoritmi di criptazione e gli algoritmi di decriptazione memorizzati nella memoria 120 di uno o più dispositivi elettronici criptatori-decriptatori 100, nonché le modalità di funzionamento di questi ultimi.

Di conseguenza, il sistema di criptazione per le comunicazioni nella IoT consente di configurare il livello di sicurezza delle comunicazioni direttamente da un'applicazione web 330, adattando le necessità di criptazione (la criptazione può essere deselezionata, oppure può essere "light" oppure "strong") alle necessità di ogni specifica applicazione (i.e. alle necessità di uno o più utenti autorizzati utente (e.g. l'utente gestore dei sensori e/o degli attuatori collegati ad uno o più dispositivi elettronici criptatori-decriptatori 100).

In quel che precede sono state descritte la preferite forma di realizzazione e sono state suggerite delle varianti della presente invenzione, ma è da intendersi che gli esperti del ramo potranno apportare modificazioni e cambiamenti senza con ciò uscire dal relativo ambito di protezione, come definito dalle rivendicazioni allegate.

RIVENDICAZIONI

1. Sistema di criptazione per le comunicazioni nella IoT comprendente uno o più dispositivi elettronici criptatori-decriptatori (100), ognuno dei quali è provvisto di una unità (110) di elaborazione collegata ad una memoria (120) che memorizza chiavi ed uno o più algoritmi di criptazione e ad una interfaccia di comunicazione configurata per essere collegata ad uno o più sensori e/o uno o più attuatori, l'unità (110) di elaborazione essendo configurata per criptare dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori, in cui ogni dispositivo elettronico criptatore-decriptatore (100) è collegato ad una rete (200) di comunicazioni cui è collegata anche una piattaforma web (300) che è configurata per selezionare, per ogni dispositivo elettronico criptatore-decriptatore (100), l'algoritmo di criptazione che questo utilizza per criptare dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori, ogni dispositivo elettronico criptatore-decriptatore (100) essendo configurato per trasmettere alla piattaforma web (300) dati criptati, la piattaforma web (300) essendo provvista di una o più unità (310) di elaborazione collegate ad una o più memorie (320) che memorizzano chiavi ed uno o più algoritmi di decriptazione necessari per decriptare dati criptati provenienti da ogni dispositivo elettronico criptatore-decriptatore (100).

2. Sistema secondo la rivendicazione 1, in cui la piattaforma web (300) è configurata per selezionare o deselezionare una criptazione da parte dell'unità (110) di elaborazione di un dispositivo elettronico criptatore-decriptatore (100) dei dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori collegati all'interfaccia di comunicazione di tale dispositivo elettronico criptatore-decriptatore (100).

3. Sistema secondo la rivendicazione 1 o 2, in cui la piattaforma web (300) è configurata per selezionare un algoritmo di criptazione che l'unità (110) di elaborazione di un dispositivo elettronico criptatore-decriptatore (100) è configurato per utilizzare per criptare i dati provenienti da detti uno o più sensori e/o da detti uno o più attuatori collegati all'interfaccia di comunicazione di tale disposi-

tivo elettronico criptatore-decriptatore (100), e/o un algoritmo di decriptazione che dette una o più unità (310) di elaborazione sono configurate per utilizzare per decriptare i dati criptati provenienti da tale dispositivo elettronico criptatore-decriptatore (100).

4. Sistema secondo una qualsiasi delle precedenti rivendicazioni, in cui la piattaforma web (300) è configurata per generare dati di controllo per controllare un funzionamento e/o uno stato di uno o più sensori e/o di uno o più attuatori, per criptare detti dati di controllo mediante dette una o più unità (310) di elaborazione secondo chiavi ed uno o più algoritmi di criptazione memorizzati in dette una o più memorie (320), e per trasmettere detti dati di controllo criptati ad un dispositivo elettronico criptatore-decriptatore (100), cui sono collegati detti uno o più sensori e/o uno o più attuatori controllati da detti dati di controllo, la cui unità (110) di elaborazione è configurata per decriptare, mediante chiavi ed uno o più algoritmi di decriptazione memorizzati nella sua memoria (120), dati di controllo criptati provenienti dalla piattaforma web (300).

5. Sistema secondo la rivendicazione 4, in cui la piattaforma web (300) è configurata per selezionare o deselezionare una criptazione da parte di dette una o più unità (310) di elaborazione di detti dati di controllo.

6. Sistema secondo la rivendicazione 4 o 5, in cui la piattaforma web (300) è configurata per selezionare un algoritmo di criptazione che dette una o più unità (310) di elaborazione sono configurate per utilizzare per criptare detti dati di controllo, e/o un algoritmo di decriptazione che l'unità (110) di elaborazione di un dispositivo elettronico criptatore-decriptatore (100) è configurato per utilizzare per decriptare detti dati di controllo criptati provenienti dalla piattaforma web (300).

7. Sistema secondo una qualsiasi delle precedenti rivendicazioni, in cui la piattaforma web (300) è configurata per selezionare un protocollo di comunicazione che almeno parte di detti uno o più dispositivi elettronici criptatori-decriptatori (100) e la piattaforma web (300) debbono utilizzare per trasmettersi dati nella rete (200) di comunicazioni.

8. Sistema secondo una qualsiasi delle precedenti rivendicazioni, in cui la piattaforma web (300) è configurata per essere accessibile da remoto per mezzo di un'applicazione web (330) da parte di almeno un utente autorizzato.

9. Sistema secondo una qualsiasi delle precedenti rivendicazioni, in cui l'interfaccia di comunicazione di uno o più dispositivi elettronici criptatori-decriptatori (100) è configurata per essere collegata ad uno o più sensori di tipo Grove e/o uno o più attuatori di tipo Grove.

10. Sistema secondo una qualsiasi delle precedenti rivendicazioni, in cui la piattaforma web (300) è configurata per aggiornare da remoto chiavi ed algoritmi di criptazione e/o algoritmi di decriptazione memorizzati nella memoria (120) di uno o più dispositivi elettronici criptatori-decriptatori (100), la piattaforma web (300) essendo opzionalmente configurata per aggiornare una modalità di funzionamento di uno o più dispositivi elettronici criptatori-decriptatori (100).

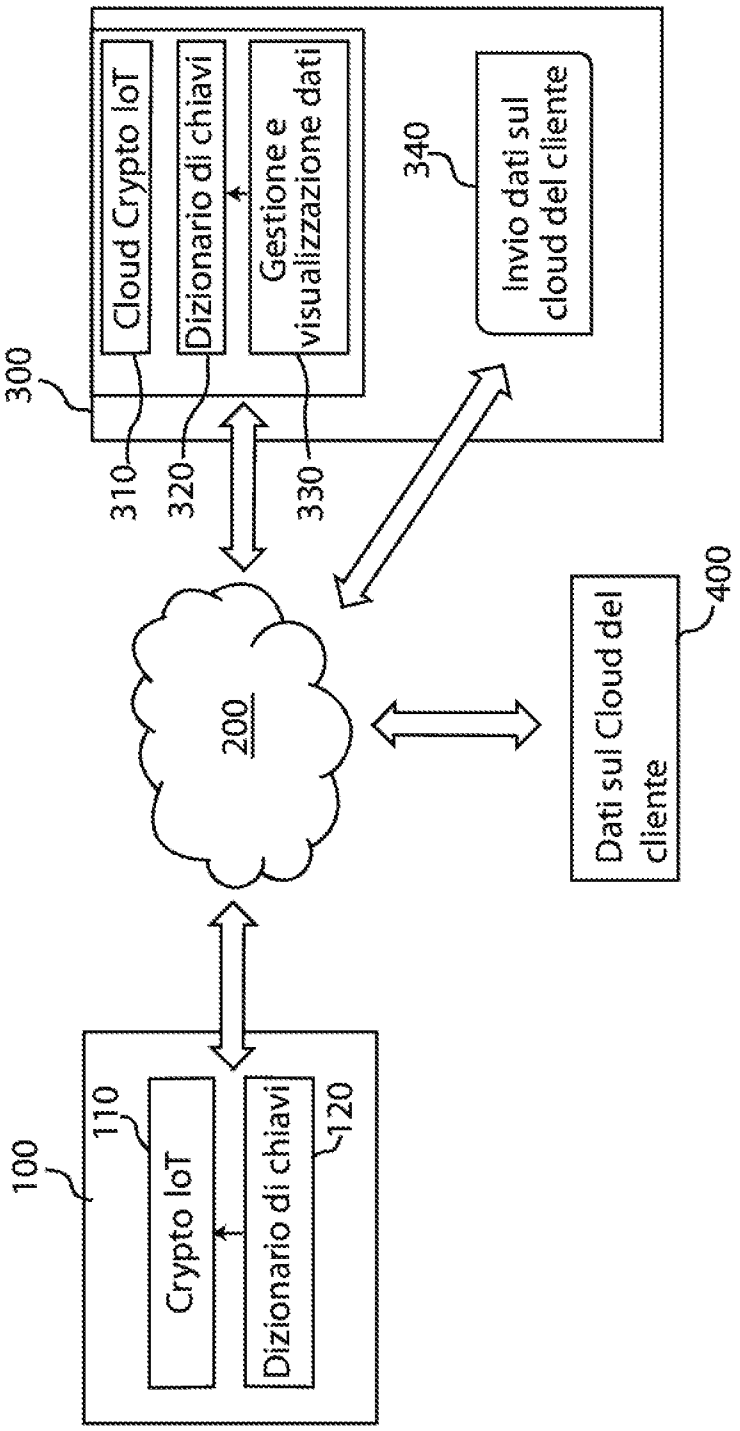
100
110
Crypto IoT
120
Dizionario di chiavi
200
300
Cloud Crypto IoT
Dizionario di chiavi
Gestione e visualizzazione dati
310
320
330
340
Invio dati sul cloud del cliente
400
Dati sul Cloud del cliente

Fig. 1