

I Sistemi di identificazione biometrica, come alternativa all' uso dei chip RFID, sistemi non invasivi – esempi di sistemi di calcolo distribuito alternativi al cloud computing *

*di Luigi Zamprotta * **

Ipotesi e prospettive

1. Possiamo ipotizzare l' Identificazione biometrica basata su palm vein scan, come sistema unico di identificazione?

Ma quale è la situazione ad oggi?

Nell'attuale panorama dei sistemi di identificazione, spiccano fra i meno impegnativi per l'utente quelli biometrici.

Nessuna password da ricordare, nessun codice da generare. L'utente stesso è la password di autenticazione.

Le proprietà biometriche hanno le seguenti caratteristiche

- 1) Universalità: tutti devono averla
- 2) Unicità: diverse per ogni individuo
- 3) Permeanza: non deve mutare nel tempo
- 4) Collezionabilità: misurabile quantitativamente
- 5) Performance: identificazione in tempi rapidi
- 6) Accettabilità: tasso di gradimento alto fra gli utenti.

I sistemi biometrici più conosciuti sono i seguenti:

- impronte digitali
- geometria delle mani
- impronta vocale
- scansione dell'iride
- scansione della retina
- scansione delle vene della mano
- riconoscimento facciale
- firma autografa.

Il sistema a cui faccio riferimento è il **riconoscimento dei vasi sanguigni nel palmo**. La tecnologia, sviluppata da Fujitsu è nota con il nome commerciale di **PalmSecure**, ed è già impiegata da alcune aziende nel mondo.

PalmSecure consiste di un sensore grande qualche centimetro quadrato che riesce a **riconoscere la disposizione delle vene nel palmo della mano**. Esse formano un reticolo particolarmente intricato, al punto da essere diverso in ciascun essere umano. Il vantaggio rispetto ad altri metodi più diffusi, come l'impronta digitale o la scansione

del volto, è che viene sfruttato un parametro biometrico "interno", quindi **più difficile da rubare o riprodurre**.

L'utente non deve far altro che mostrare il palmo aperto al sensore per qualche istante, e il sistema si sblocca senza bisogno di password o altri sistemi di autenticazione.

Tra i vantaggi di questo sistema di riconoscimento possiamo dire che l'algoritmo di autenticazione biometrica avanzata che utilizza offre un **FAR** estremamente basso (**tasso di accettazione errato**) e **FRR** (**tasso di scarto falso**).

L'autenticazione delle vene palmari senza contatto è igienica e non invasiva permette un **repository crittografato** per archiviazione dei modelli e funzionalità di registrazione degli stessi mantenendo i dati protetti (**GDPR compliant**).

Facendo un paragone con un altro sistema biometrico, il riconoscimento dell'impronta digitale, esso ha un alto tasso di riconoscimento, ma è suscettibile alla qualità delle immagini raccolte perché le impronte digitali sono spesso danneggiate e possono essere facilmente rubate. Diversamente dal riconoscimento delle impronte digitali, il riconoscimento delle vene palmari funziona ispezionando con i raggi infrarossi l'interno del palmo della mano anziché sulla superficie del dito, così le immagini delle vene del palmo sono impossibili da replicare.

Attualmente l'autenticazione PalmSecure è riconosciuta dai principali organismi di sicurezza internazionali, tra cui l' **International Common Criteria** e il **CNIL**.

Dopo una attenta valutazione, ho constatato che l'adozione di sistemi biometrici come questo scardinerebbe di fatto l'attuale consuetudine in termini di gestione della sicurezza fatta a base di chiavi, certificati e password che scadono ciclicamente (da ricordare), oltre ai vari media utilizzati da portare con sé (smart card, token – otp e RFID).

Con un sistema simile si potrebbe pensare ad un sistema di identificazione unico: dall'apertura delle porte, ad una transazione finanziaria, alla timbratura di ingresso al lavoro, tutto con lo schema delle vene della mano.

Non è escluso che tale sistema in futuro possa effettuare la scansione di altre parti del corpo scoperte (la fronte?), aumentando gli elementi d'identificazione e riducendo le possibilità di errore.

Io penso che tale sistema possa essere facilmente implementato sui vecchi computer semplicemente con una unità esterna ed un software aggiuntivo. Nell'ambito di un qualsiasi ufficio ciò permetterebbe di gestire molti servizi, compreso quello della firma digitale nella più completa sicurezza.

Nel mio ambito professionale questo risolverebbe tutti i problemi relativi ad **accesso ai locali, l'autenticazione per l'accesso al dominio e l'autenticazione per l'accesso alle procedure**. L'unica speranza è che si arrivi presto a tutto ciò.

2. Quali sistemi alternativi al cloud computing?

In questo momento storico sembra che il cloud risolva ogni problema e che sia nei fatti l'unico sistema alternativo al possedere una server farm, un Datacenter o un piccolo CED, in poche parole dei server fisici.

Nel frattempo l'IBM ed altri colossi dell'informatica hanno appoggiato un ambizioso progetto il **Blockchain**.

Nato inizialmente per eseguire i calcoli per i Bitcoin, una valuta elettronica che ha visto negli anni accrescere il suo valore in maniera esponenziale, alla base di tutto vi è una rete di calcolatori che a livello mondiale tiene in vita questa moneta.

Analogamente mantenendo una architettura simile lo stesso sistema viene mutuato per altri scopi (industria, commercio, pubblica amministrazione).

Ma cos'è un blockchain? Si tratta di **un data base distribuito (una sorta di registro delle transazioni dove i dati non sono memorizzati su un solo computer, ma su più macchine collegate tra loro via Internet, attraverso un'applicazione dedicata che permette di interfacciarsi con la "catena") composto da blocchi di dati che memorizzano transazioni**. Per essere consolidato ogni dato, all'interno di un blocco e successivamente ogni blocco prima di essere inserito nella "catena", viene sottoposto a un **processo di validazione**.

Cosa sono e come funzionano i processi di validazione della blockchain.

Prima di procedere dobbiamo prendere dimestichezza con due termini: **nodi della blockchain** e **miner**. I primi sono i computer della rete che hanno scaricato la blockchain nella loro memoria. Chiunque può diventare un nodo, tramite l'apposito programma (Bitcoin Core per esempio per Blockchain Bitcoin). I miner sono coloro che effettuano il controllo delle transazioni, grazie a computer molto potenti e attraverso un protocollo di validazione piuttosto complesso (spiegato più avanti), e il cui lavoro viene ripagato con un premio (il termine ormai condiviso per questa operazione è "minare", italianizzando il termine inglese to mine ossia estrarre).

Il protocollo di validazione (che definisce gli algoritmi validanti e chi può essere un miner) rappresenta dunque l'elemento vitale principale della blockchain perché è proprio da questo che dipendono sostanzialmente la velocità della catena e la sua sicurezza (gli algoritmi che governano questo processo non solo validano che ogni nuova immissione risponda a determinati criteri, ma impediscono anche che possano essere manomessi i dati già presenti nella catena). È dunque in questo ambito che si vedono le principali evoluzioni e che si differenziano, dal punto di vista tecnologico, le diverse blockchain. È comunque importante sottolineare che non necessariamente un protocollo è migliore di un altro: l'utilizzo dell'uno o dell'altro dipende anche dal tipo di applicazione per la quale viene utilizzata la blockchain.

Ma facciamo un passo indietro per capire meglio che cos'è un **database distribuito**.

Nel momento in cui parliamo di Distributed Ledger, ci troviamo davanti un database che non si trova fisicamente solo su un server (computer), ma che invece si trova su più computer nello stesso momento, tutti perfettamente sincronizzati su tutti

gli stessi documenti. Ad esempio, può trovarsi su tutti i computer che sono connessi alla rete. In questo modo, l'informazione è reperibile in maniera molto rapida, in quanto la potenza di calcolo sfrutta la potenza di tutti i computer connessi.

*3. Come si colloca **il Blockchain** in una pubblica amministrazione?*

Se il **cloud externalizza** i dati e li rende fruibili garantendo un grado di sicurezza accettabile secondo i dettami della cybersecurity e permette di avere infrastrutture server virtuali ed ogni applicativo subito fruibile su internet, la Blockchain, escludendo la sua peculiarità finanziaria, può proteggere di fatto i dati da manomissione rendendo unico il dato e non copiabile.

I soggetti interessati lungo la catena determineranno o meno il consenso per l'accesso al dato.

Queste caratteristiche in una pubblica amministrazione garantirebbero l'integrità effettiva dei dati e la loro disponibilità specie quando si tratta di dati sensibili.

Riassumendo, ecco i punti principali nella sua futura applicazione:

a) Identità Digitale

Attualmente la Microsoft sta lavorando ad una tecnologia in grado di usare la Blockchain pubblica, per **rendere inviolabile la nostra identità digitale**, attraverso la crittografia. Conservare i propri dati tramite la Blockchain è sicuro: **chiunque voglia effettuare verifiche non dovrà fare altro che interrogare il registro**. Su larga scala questa applicazione rivoluzionerebbe il mondo della Pubblica Amministrazione, snellendo la burocrazia.

b) Voto Elettronico

Il problema principale del voto digitale è la sua sicurezza. I voti possono essere manomessi oppure qualcuno potrebbe addirittura scoprire per chi è stato espresso il voto. La Blockchain garantirebbe la **segretezza del voto** in totale sicurezza e trasparenza.

c) Contratti digitali

Il registro della Blockchain può anche assumere un ruolo più "attivo" in caso di contratto fra due soggetti. **Potenzialmente potrebbe, oltre che registrare le transazioni, anche eseguirle in maniera autonoma**, fornendo così una garanzia a entrambe le parti. Potrebbe, ad esempio, assicurarsi che un fornitore sia pagato regolarmente dal suo cliente.

d) Scuola e mondo accademico

Per verificare e autenticare certificati e titoli di studio. Da qui un grosso aiuto per la gestione delle risorse umane, verso la costruzione di un sistema di curriculum vitae più trasparente e facilmente verificabile.

e) Sanità

Permettono a ospedali, contribuenti e altre strutture sanitarie di condividere l'accesso ai loro network senza compromettere la sicurezza e l'integrità dei dati.

Ulteriori punti a vantaggio offerti dalla **blockchain** saranno i seguenti:

- ❑ **Decentralizzazione e automatizzazione di tutti gli archivi pubblici digitali**
- ❑ **Timestamping e proof-of- existence**
- ❑ **Protezione dei dati, privacy-by-design e trasparenza**
- ❑ **Gestione di identità digitali decentralizzate**
- ❑ **Riscossione delle imposte e gestione di fondi pubblici e pagamenti**
- ❑ **Sicurezza, resilienza sistemica e interoperabilità.**

Le architetture distribuite fondate sulla tecnologia blockchain sono particolarmente adatte alla **gestione in sicurezza di grosse moli di dati** e conferiscono alle infrastrutture della P.A. una **resilienza molto maggiore rispetto agli attuali sistemi centralizzati**. Anche in caso di violazioni o criticità del circuito, questo nell'insieme può continuare a funzionare in modo affidabile. Inoltre, le architetture distribuite possono essere progettate in modo da garantire **adeguata interoperabilità tra svariati enti e soggetti istituzionali**, migliorando la condivisione dei dati e la performance generale della P.A.

La standardizzazione dei servizi blockchain a livello internazionale richiederà presumibilmente tempi di ampio respiro e complesse verifiche d'impatto. I **TSP (Trust Service Provider)** sono però gli unici operatori che già da oggi possono garantire alla P.A. applicazioni blockchain a elevato valore innovativo, e con le necessarie condizioni di sicurezza, di conformità normativa e di governance.

Per questo fine, a livello governativo il MISE (Ministero Sviluppo Economico) nel Febbraio 2019 ha nominato un gruppo di esperti per l'analisi di come migliorare i servizi pubblici erogati dalla Pubblica Amministrazione sfruttando la tecnologia **blockchain**.

Sicuramente questo comporterà la revisione dei piani strategici dell'AgID attualmente improntati ad una politica Cloud First. A questo punto non resta che aspettare gli sviluppi.

4. L'automazione in ufficio e la gestione delle risorse umane

L'automazione d'ufficio o office automation è iniziata di fatto negli anni '80 e comprendeva i primi sistemi di videoscrittura, terminali per il data entry e sistemi di consultazione di database centralizzati.

Oggi nel 2019, tutte le applicazioni sono per la maggior parte **web oriented**, mentre le emulazioni terminale ANSI sono ridotte al minimo e la virtualizzazione di server e procedure va avanti velocemente.

L'impatto che sta avendo su una sede locale, in questo caso la sede Alfa, lo si evince nell'utilizzo delle procedure relative a processi amministrativi, tecnici o legali dell'amministrazione stessa.

Negli ultimi anni il fax è pressoché scomparso come sistema di trasmissione dei documenti ed al posto suo email e PEC eseguono la stessa funzione.

Per non penalizzare l'utenza comunque si è cercato di implementare soluzioni di fax virtuale sulla rete IP per poter ricevere i fax dall'esterno.

Ora si implementeranno anche le procedure di marchettura informatizzata delle pratiche e il protocollo informatizzato. Entrambe queste procedure sono presenti all'interno della Direzione Generale Gamma in tutte le sedi. La centralizzazione di tali processi permette un più rapido riscontro nel cercare delle operazioni eseguite sia che tratti di patenti, revisioni o immatricolazioni.

Le stampe di sistema sono erogate di norma dalla sezione stampe del CED: esso grazie alla ridondanza degli apparati dà la garanzia che le stampe giornaliere siano eseguite in totale sicurezza **garantendo** anche in caso di blackout la capacità energetica utile per l'emissione di tabulati, card e fincati onde non ridurre l'operatività dell'ufficio.

Le risorse umane, grazie ai programmi che gestiscono i turni, sono normalmente pianificate per l'ottimizzazione negli impieghi operativi. Uno degli aspetti che si potrebbe migliorare sarebbe l'adozione di un sistema di chat interno al pari dei whatsapp, giusto per fare un esempio, per permettere una connessione e comunicazione in differita di eventuali problematiche con i colleghi. Allo stato attuale il sistema VoIP ha migliorato di molto la comunicazione fra le varie sedi ma molto ancora resta da fare.

La videocomunicazione in chat risulta essere ancora considerata un evento eccezionale, niente di più sbagliato. In alcuni casi tale sistema può servire a risolvere le problematiche. Altra cosa che deve essere studiata è l'applicazione di sistemi biometrici nell'autenticazione di documenti onde ridurre lo stress dei funzionari nell'accedere a documentazione riservata.

Per quel che concerne i sistemi operativi usati sulle postazioni di lavoro standard, sono dell'avviso che occorrerebbe un sistema centralizzato localmente per la gestione dei desktop degli utenti, questo per facilitare la movimentazione degli stessi all'interno della sede.

*Luigi Zamprota***

**Questo articolo è l'ultimo paragrafo della tesi di Master universitario post lauream, intitolata "La Sicurezza nell'Ufficio moderno: Criticità, Sicurezza, Prospettive", discussa dall'autore presso l'Università degli studi 'Niccolò Cusano' Telematica Roma, in data 9 luglio 2019, per il conseguimento del Master in "Sicurezza delle Reti informatiche".*

***Ingegnere informatico (iscritto all'Ordine degli Ingegneri di Milano). Funzionario informatico del Ministero delle Infrastrutture e dei Trasporti-Motorizzazione Civile (Biella-Milano, Italia). Ingénieur en Informatique Appliquée (SNIPF-Société Nationale des Ingénieurs Professionnels de France). IUM-Ingénieur Universitaire Master (CNISF-Conseil National des Ingénieurs et Scientifiques de France)*

BIBLIOGRAFIA

- Zamprota, Luigi (1992), *Un'esperienza di organizzazione aziendale secondo le nuove tecnologie*, in *Introduzione culturale allo studio delle nuove tecnologie*, Libreria Vittorio Giovannacci, Biella
- Zamprota, Luigi (1993), *La qualité comme philosophie de la production. Interaction avec l'ergonomie et perspective futures*, Mémoire de Maîtrise, Institut d'Etudes Supérieures L'Avenir, Bruxelles, année académique 1992/93, Directeur de Maîtrise dr.prof.Francis Dessart, (Published by TIU Press, Independence, Missouri, USA, ISBN 0-89697-452-9
- Zamprota, Luigi (2019), *La sicurezza in un ufficio pubblico: criticità, problemi, prospettive*, tesi Master in *Sicurezza delle reti Informatiche*, UNICUSANO, Roma, anno accademico 2018/19