Servizi Intelligenti per il Tracciamento e l'Elaborazione di Dati Multi-Biometrici in Piattaforme di Apprendimento Digitale

Gianni Fenu e Mirko Marras

Università degli Studi di Cagliari, Dipartimento di Matematica e Informatica,
Via Ospedale 72, 09124 Cagliari, ITALIA
{mirko.marras,fenu}@unica.it

Abstract. Con la crescente pervasività delle esperienze di apprendimento digitali, cresce anche la necessità di ottimizzare usabilità ed efficacia degli strumenti impiegati, garantendo contemporaneamente un adeguato livello di sicurezza e di integrità delle attività svolte. Tracciare e trattare dati biometrici, come il volto e la voce, sta acquisendo un ruolo cruciale a tal scopo. Per esempio, questa tipologia di dati può essere analizzata per comprendere meglio le risposte cognitive ed emotive dei discenti e migliorare l'esperienza di apprendimento, ma può offrire anche una valida prova per la certificazione dell'identità del discente durante attività svolte elettronicamente. Di conseguenza, è sempre più marcata la necessità di strumenti e tecnologie in grado di catturare e manipolare questi preziosi dati. In questo articolo, proponiamo un sistema software multi-dispositivo in grado di (i) supportare il tracciamento di svariati tratti biometrici, sia fisici che comportamentali, all'interno di piattaforme di apprendimento digitale e (ii) promuovere una facile integrazione di servizi intelligenti capaci di capitalizzare tali dati per finalità specifiche. In questa direzione, mostreremo un caso di studio in cui il sistema è instanziato per fornire un servizio di autenticazione biometrica durante l'erogazione di contenuti didattici in una piattaforma digitale. Un modulo di tracciamento, integrato nella piattaforma, colleziona i dati biometrici desiderati, un modulo di elaborazione biometrica estrae caratteristiche significative dai dati tracciati e, infine, un modulo di predizione controlla in maniera continua l'identità del discente sulla base delle caratteristiche estratte e decide se il discente può continuare o meno ad interagire con la piattaforma. Con il contributo proposto, ci aspettiamo di supportare una sempre più crescente adozione di tecnologie biometriche nel settore istruzione e, in parallelo, di favorire l'integrazione di servizi che ne sfruttino le potenzialità.

Keywords: Biometria, Sistema Multi-Biometrico, Piattaforma E-Learning.

1 Introduzione

Le tecnologie per l'*analisi biometrica* sono in rapida diffusione nel settore dell'istruzione, come dimostrato da recenti studi di mercato [1]. I dati biometrici sono ottenuti mediante il tracciamento di tratti biologici fisici (es. volto, impronta, iride) o comportamentali (es. battitura, voce) degli utenti interagenti nel sistema [2]. I benefici dell'uso

della biometria nell'istruzione sono molteplici. Per esempio, recenti sviluppi hanno portato alla sua applicazione per il monitoraggio delle presenze alle lezioni e per rendere più sicuri gli accessi ai campus universitari [3,4]. Negli ambienti di apprendimento digitale, il monitoraggio biometrico aiuta a garantire l'integrità accademica, verificando l'identità degli studenti ed impedendo loro di imbrogliare durante le attività svolte online [5]. Inoltre, l'analisi biometrica supporta la valutazione dell'esperienza di apprendimento, permettendo di capire meglio le risposte cognitive ed emotive degli studenti interagenti con l'ambiente digitale [6]. Tuttavia, sebbene le tecnologie biometriche siano sempre più frequentemente adottate nell'ecosistema apprendimento, capire come potranno essere sfruttate in modo efficace, efficiente, sicuro e responsabile rappresenta ancora oggi una sfida.

Nell'ambito dell'apprendimento all'interno di piattaforme digitali, il tracciamento e l'elaborazione di dati biometrici dovrebbero essere *continui* e *trasparenti*. Questo permetterebbe di garantire la disponibilità costante di un flusso dati rappresentativo della totalità dell'esperienza digitale dello studente, senza disturbare le normali attività all'interno della piattaforma. Per esempio, in un sistema di autenticazione degli studenti, la continuità operativa aiuterebbe a ridurre il rischio di impersonazione dello studente durante l'esame, mentre la trasparenza del tracciamento permetterebbe di non appesantire l'esperienza degli utenti che operano onestamente con attività addizionali non strettamente riguardanti le finalità didattiche [7]. Similarmente, il tracciamento continuo e trasparente di dati biometrici può supportare una più ampia valutazione dell'esperienza di apprendimento, non più limitata ai soli riscontri espliciti forniti dagli studenti (es. questionari di valutazione finale), ma capace di tener conto e comprendere lo stato cognitivo ed emotivo degli studenti mentre interagiscono nella piattaforma, interferendo in maniera trascurabile con i naturali comportamenti degli stessi [8].

Il potenziale delle tecnologie biometriche nel settore dell'istruzione appare elevato, ma sono ancora pochi i sistemi capaci di capitalizzarne il valore nelle piattaforme di apprendimento. Sono ancora diverse le sfide *tecniche* e *sperimentali*, tra cui la necessità per ogni istituzione di apprendimento o fornitore di piattaforme di sviluppare da zero i propri servizi basati su analisi biometrica, quando questi non siano già disponibili sul mercato e agevolmente integrabili. Inoltre, in ambito scientifico, gli studiosi e i ricercatori, interessati ad analizzare particolari aspetti nascosti nei dati biometrici tracciati durante l'esperienza di apprendimento, si trovano spesso a dover creare da zero un modulo software capace di tracciare i dati biometrici desiderati nella piattaforma di apprendimento (es. i dati sulla battitura sulla tastiera). Oltre ad un incremento in termini di tempistiche e costi, questo processo richiede capacità tecniche che esulano dalla mera capacità di analizzare i dati, con una conseguente limitazione del progresso settoriale.

In risposta a questa emergente necessità, nell'ambito del progetto "*iLearnTV Anywhere Anytime*" [9] finanziato dal MIUR, proponiamo un sistema software in grado di supportare il tracciamento di tratti biometrici, fisici (es. volto, voce) e comportamentali (es. battitura, tocco, movimento mano), all'interno di piattaforme di apprendimento digitale, promuovendo al contempo una facile integrazione di servizi di *intelligenza artificiale* capaci di capitalizzare questi dati per finalità specifiche. Per mostrare i benefici del contributo, discuteremo un caso di studio in cui il sistema è instanziato per fornire

un servizio di autenticazione biometrica durante l'erogazione di contenuti didattici digitali. Il modulo di tracciamento integrato nella piattaforma colleziona i dati biometrici desiderati, il modulo di elaborazione biometrica estrae caratteristiche significative dai dati tracciati e, infine, il modulo di predizione controlla continuamente l'identità del discente sulla base delle caratteristiche estratte e decide, poi, se il discente può continuare ad interagire con la piattaforma. Con il nostro contributo, miriamo ad offrire agli odierni ecosistemi di apprendimento un sistema biometrico facilmente *integrabile* ed *espandibile*; al contempo, vorremmo promuovere nella comunità scientifica l'adozione di tecnologie biometriche capaci di generare impatto positivo sul *benessere comune* degli attori interagenti a vari livelli (es. studenti, docenti, istituzioni ed imprese).

Il resto dell'articolo è organizzato come segue. La *Sezione 2* mostra le attuali applicazioni delle tecnologie biometriche nelle piattaforme di apprendimento e, tra queste, approfondisce i sistemi di autenticazione di studenti, oggetto del caso di studio. Di seguito, la *Sezione 3* descrive lo schema architetturale del sistema software proposto, includendo una disamina dei dati biometrici raccoglibili, dei suoi componenti e di come questi comunicano. La *Sezione 4* mostra un caso di studio in cui il sistema proposto è instanziato per implementare un servizio di autenticazione continua di studenti e ne discute la sua valutazione sperimentale multi-browser multi-dispositivo. Infine, la *Sezione 5* presenta le conclusioni e le conseguenti linee di ricerca future.

2 Stato dell'Arte

Il tracciamento e l'elaborazione di dati biometrici sono pratiche recentemente introdotte nell'ambito delle piattaforme e-learning. Prima, forniremo una disamina di alcune delle applicazioni più significative. Di seguito, concentreremo l'attenzione su come tali pratiche sono state impiegate allo scopo di assicurare l'integrità accademica.

2.1 Tecnologie Biometriche nelle Piattaforme d'Apprendimento

Oltre ai log di tracciamento tradizionalmente impiegati [10], le piattaforme di apprendimento possono sfruttare un'ampia varietà di dati in grado di fornire loro informazioni senza precedenti su come gli studenti interagiscono con il materiale didattico: i dati biometrici. Sono svariati i modi in cui essi sono stati usati in ambito didattico [11].

Un esempio rivolto alle attività in presenza riguarda l'impiego di dati e tecnologie biometriche per semplificare ed incrementare l'efficienza di processi amministrativi che, in genere, consumano una quantità di tempo rilevante (es. controllo della frequenza scolastica svolto tramite lettori di impronte digitali o telecamere posti in aula [12]).

Negli ambienti di apprendimento a distanza, non solo queste tecnologie possono supportare il tracciamento della partecipazione degli studenti alle attività, ma possono anche aiutare a capire e predire il livello di coinvolgimento degli stessi durante la fruizione di una risorsa [13]. I docenti possono utilizzare tali informazioni al fine di definire pratiche volte a migliorare l'esperienza d'apprendimento nella piattaforma. Quest'ultima può anche impiegare tali informazioni per adattarsi in maniera automatica all'utente.

Ancora, l'analisi dei dati biometrici può essere volta alla misurazione del coinvolgimento degli studenti e alla rilevazione di difficoltà cognitive [8]. Osservare il loro comportamento, il contatto visivo e il linguaggio del corpo, può essere utile per capire come uno studente stia interagendo con il materiale, rilevare se perde interesse o ha bisogno di attività di tutoring specifiche. Tutto questo deve, al contempo, tener conto di aspetti etici e di privacy, a seconda anche della fascia di età degli studenti coinvolti.

Le tecnologie biometriche possono contribuire a garantire l'integrità delle attività svolte online, verificando l'identità degli utenti e/o impedendo loro di accedere a risorse non autorizzate [7]. Infatti, l'assenza di un docente o di un supervisore durante le attività online può dare luogo a comportamenti non etici e, quando l'integrità dei mezzi di valutazione è minacciata, si mette a rischio il raggiungimento degli obiettivi educativi. In particolare negli ambienti di apprendimento a distanza. le vulnerabilità delle piattaforme possono consentire ad utenti malintenzionati, spesso studenti stessi, di alterare le informazioni in esse registrate o violare specifici regolamenti durante gli esami [14].

Quelle sopra menzionate sono solo alcune delle possibili applicazioni delle tecnologie biometriche nell'ambito dell'istruzione. Considerato l'enorme potenziale, sta emergendo la necessità di strumenti e tecnologie in grado di facilitare la cattura e la manipolazione di dati biometrici. Nel resto dell'articolo ci focalizzeremo, come caso di studio, su un servizio di autenticazione biometrica erogato durante la fruizione di contenuti didattici e mostreremo come il sistema proposto possa supportare la collezione dei dati biometrici necessari e favorire l'integrazione del servizio in una piattaforma.

2.2 Supervisione Biometrica degli Studenti nelle Piattaforme d'Apprendimento

Le piattaforme di apprendimento iniziano sempre più frequentemente a dotarsi di misure anti-inganno per scongiurare i possibili tentativi di violazione dei regolamenti. Tenendo presente questo, illustriamo brevemente alcuni dei servizi più rappresentativi.

ProctorU [15] è un sistema di supervisione studenti basato sul diretto controllo dell'esaminando da parte di un supervisore nel corso di un esame. L'esaminato deve registrarsi nel Learning Management System (LMS). Il supervisore umano verifica l'ID studente, il suo volto e l'ambiente in cui si trova. Il sistema esegue alcuni controlli sulla velocità di internet e su qualsiasi dispositivo addizionale, come la fotocamera e il microfono. Una volta avviato l'esame, l'utente sarà costantemente monitorato dal supervisore, il quale può anche controllare la schermata del candidato. Rispetto ad altri sistemi, *ProctorU* rimane legato al bisogno di un supervisore umano, comportando poca flessibilità.

Pearson VUE (Pearson Virtual University Enterprises) [16] richiede l'identificazione tramite un ID e un'immagine del volto. Dopo un test di sistema, usato come registrazione, l'utente può iniziare l'esame mentre un supervisore umano lo monitora durante tutta la sessione. L'utente può comunicare con il supervisore per eventuali problemi di tipo tecnico. Anche se Pearson VUE non usa il riconoscimento biometrico, è ritenuto elemento rappresentativo grazie alle numerose partnership di cui è oggetto. Questo dimostra quanto ancora la supervisione svolta in maniera completa da un umano sia preferita a quella svolta in maniera automatica o semi-automatica da un software.

Uno tra i più significativi sistemi di supervisione automatizzati è *Proctorio* [17]. È un software di servizio remoto che funziona all'interno del browser web. Si occupa di monitorare i comportamenti sospetti dei partecipanti e permette di decidere in maniera dettagliata tali attività di monitoraggio (es. se l'utente deve essere monitorato solo tramite fotocamera, o anche tramite microfono; se la schermata utente deve essere registrata; se il traffico web deve essere controllato; se l'utente deve mostrare la stanza in cui sta sostenendo il test). L'esaminato può essere segnalato come sospetto a seconda del suo comportamento, ma sarà il docente a stabilire se l'esame sia valido o meno.

ProctorFree [18] è una soluzione software per la supervisione esami non richiedente l'intervento umano. Esso autentica lo studente usando il riconoscimento del viso e verifica continuamente la sua identità tramite il volto durante il corso dell'esame. Inoltre, durante l'esame, *ProctorFree* monitora una varietà di eventi, comportamenti e schemi tipicamente sospetti. Una volta completato l'esame, un dettagliato report della sessione viene inviato via e-mail all'amministratore dell'esame, spesso il docente, evidenziando minuto e secondo specifico potrebbero essersi verificati dei comportamenti sospetti.

TeSLA (Trust-Based Authentication & Authorship E-Assessment Analysis) [19] è un altro sistema, sviluppato nell'ambito di un importante progetto europeo, che consente di controllare un utente in maniera automatizzata durante lo svolgimento di un esame. Il cuore del monitoraggio è rappresentato dell'identità dell'utente a partire dalla battitura dei tasti, del volto e della voce. La battitura dei tasti viene valutata allo stesso livello del riconoscimento del volto e della voce. Un software anti-plagio verifica l'autenticità dei contenuti prodotti dallo studente in sede di esame.

Per essere applicabili, essi dovrebbero lavorare in maniera continua, affinché l'utente non possa essere impersonato, e trasparente, così da non interferire sulle normali attività. Quelli che utilizzano biometrie fisiche catturano solitamente i tratti facciali. In altri casi, vengono combinate più biometrie, ma sono spesso richieste azioni intrusive o dispositivi aggiuntivi. Quelli che utilizzano biometrie comportamentali agiscono trasparentemente, ma non sono sufficientemente affidabili da soli. Tendono poi a supportare una data modalità di interazione, come la battitura, ma ne esistono altre, tra cui quella di selezione e quella di navigazione. In aggiunta, il dispositivo impiegato delinea le soluzioni adottabili in una formazione sempre più orientata ai dispositivi mobili e la rilevazione di biometrie in tale ambito è poco esplorata.

Essere in grado di modellare questa complessità in maniera flessibile può garantire maggiore tracciabilità, integrità e controllo del percorso formativo online.

3 Sistema di Tracciamento e Elaborazione Biometrica

È delineato di seguito il sistema biometrico proposto al fine di raccogliere ed elaborare dati biometrici in piattaforme di apprendimento. Il sistema software permette di raccogliere i dati a fini di analisi biometrica mediante i sensori del dispositivo con cui si interagisce. Nell specifico, sono supportati dati provenienti da giroscopi, accelerometri, magnetometri, schermo touch, tastiera fisica e virtuale, mouse, batteria, sensori di rete,

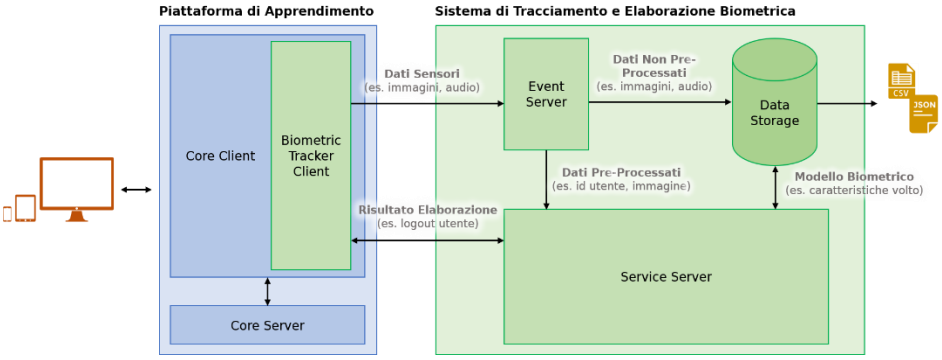

Fig. 1. Schema dell'architettura sottostante al sistema di tracciamento e elaborazione biometrica.

fotocamera, e microfono. La letteratura riconosce come i dati provenienti da tali sensori possano essere sfruttati, direttamente o indirettamente, per fornire specifici servizi [7].

L'architettura, mostrata in forma semplificata nella Figura 1, è integrabile con qualsiasi piattaforma di apprendimento sul web in pochi passaggi. È divisa nei seguenti moduli, i quali comunicano l'uno con l'altro e con la piattaforma in cui sono integrati.

Modulo di Tracciamento (Biometric Tracker Client). È rappresentato da un modulo software, sviluppato in JavaScript, capace di raccogliere tutti i dati (es. immagini, video, voce, movimento del puntatore, orientamento e movimento del dispositivo, così come dati addizionali, tra cui la durata residua della batteria e la qualità della connessione Internet) provenienti dai sensori sopra menzionati. Il modulo, agevolmente configurabile nella frequenza e varietà dei dati tracciati per lo specifico scopo, è integrabile in qualsiasi pagina web mediante l'importazione del relativo codice. Prima di iniziare il tracciamento, l'utente viene informato dello stesso e, grazie ad una apposita interfaccia generata automaticamente dal modulo software, può acconsentire o meno al tracciamento dati. Durante il tracciamento, l'utente è informato su quali dati sono raccolti mediante una barra di stato inserita in automatico dal modulo Javascript in alto nella schermata. La raccolta dati è principalmente di tipo *event-driven*: dei moduli appositi monitorano gli eventi generati dai sensori e vengono attivati quando i sensori rilevano un cambiamento di stato (es. rotazione del dispositivo o cambio orientamento dello schermo, clic di un tasto del mouse, pressione di un tasto). Diversamente, l'acquisizione di audio e video è *action-based*: la frequenza di tracciamento di tali dati viene definita in fase di configurazione, specificando un intervallo temporale di tracciamento. Il modulo può inviare i dati all'*Event Server* secondo uno dei seguenti protocolli: *online* (invio dati ad intervalli di tempi pre-stabiliti) o *offline* (i dati vengono archiviati in un'apposita memoria all'interno del browser ed inviati al termine della sessione).

Modulo di Gestione Eventi (Event Server). Il modulo è addetto allo svolgimento dei seguenti compiti: ricevere dati dal *Biometric Tracker Client*, archiviare tali dati grezzi in un apposito database qualora tale funzionalità sia configurata e necessaria (es. nel caso di creazione di dataset) e/o inviare i dati pre-processati e formattati ai *Service*

Server – moduli software con compiti di elaborazione specifici - che ne fanno richiesta. L'*Event Server* tiene, in un apposito registro, le informazioni descrittive di tutti i *Service Server* iscritti, quali dati desiderano ricevere e con quale frequenza. All'inizio del tracciamento, l'*Event Server* riceve un identificativo alfanumerico, diverso da quelli usati per il login, associato dell'utente che si sta tracciando e, durante il tracciamento, tutti i dati biometrici ad intervalli prestabiliti. Una volta formattati, i dati vengono inviati ai *Service Server* che ne hanno fatto richiesta. Il lettore noti che i *Service Server* sono in capo alla stessa istituzione o ente che si occupa della gestione della piattaforma di apprendimento. In caso di problematiche relative alla connessione di rete tra *Biometric Tracker Client* e *Event Server*, il primo provvederà a salvare in locale su una specifica memoria riservata dal client al browser i dati tracciati nel periodo critico e, una volta ristabilita la sessione, tali dati verranno inviati all'*Event Server*.

Modulo di Erogazione Servizi (Service Server). Un *Service Server* è un modulo software che riceve dati biometrici e li elabora, anche mediante algoritmi di apprendimento automatico, al fine di creare, valutare ed implementare uno specifico servizio biometrico (es. autenticazione degli studenti, misurazione del livello di coinvolgimento degli studenti e così via). Il *Service Server* può elaborare e salvare informazioni in un apposito database per usi futuri, come nel caso di un modello biometrico utile per l'autenticazione, oppure può eseguire la logica necessaria affinchè il servizio desiderato venga erogato, come nel caso del confronto tra il modello biometrico dell'utente e le caratteristiche estratte dai dati appena tracciati in un servizio di autenticazione. Il modulo ottiene i dati dell'*Event Manager* e scambia informazioni sul risultato dell'elaborazione con il *Biometric Tracker Client*. Le specifiche implementative di questo modulo dipendono dallo specifico servizio che si vuole offrire. Più *Service Server* possono essere combinati ed integrati in una stessa piattaforma di apprendimento.

4 Esempio di Utilizzo: Autenticazione Biometrica Continua

Per mostrare le potenzialità del sistema, illustriamo un caso di studio in cui esso è instanziato per fornire un servizio di autenticazione facciale continua durante l'erogazione di contenuti didattici all'interno della piattaforma di apprendimento. Il lettore noti che questo vuole solo essere un esempio di come il sistema possa essere usato per fornire un servizio biometrico nella piattaforma. Il *modulo di tracciamento* integrato nella piattaforma colleziona le immagini dalla fotocamera, il *modulo di gestione eventi* gestisce la comunicazione tra il modulo di tracciamento e l'istanza del servizio di autenticazione implementata, e uno specifico *modulo di erogazione servizi* – in questo caso autenticazione - estrae la regione dell'immagine in cui è presente il volto, ne estrae delle caratteristiche significative, controlla l'identità del discente comparando le caratteristiche estratte dai dati appena tracciati e quelle veicolate dal modello biometrico salvato per l'utente e decide, infine, se l'utente corrente può continuare ad interagire nell'area riservata della piattaforma associata all'utente legittimo.

Con attenzione al punto di vista dell'utente, nella pagina di accesso alla piattaforma, egli può scegliere di accedere alla stessa fornendo un'immagine del suo volto. Al primo

accesso viene richiesta la registrazione del proprio profilo biometrico. A tal fine, è scattata una foto dell'utente che, insieme all'indirizzo e-mail associato al suo account, viene inviato dal modulo di tracciamento al modulo di gestione eventi. L'e-mail permetterà di indicare al core della piattaforma quale utente debba essere autenticato a seguito del riconoscimento biometrico. In tutti gli accessi successivi, il modulo di tracciamento preleverà un'immagine dalla fotocamera, l'utente fornirà il suo indirizzo e-mail e, attraverso questo, il *Service Server* addetto procederà all'autenticazione. Dopo aver effettuato correttamente il login, l'utente viene reindirizzato all'area riservata della piattaforma e, se tale pagina integra il modulo di tracciamento, l'utente può vedere quali dati biometrici vengono tracciati e se sono tracciati correttamente (es. una luce verde significa che i dati biometrici sono tracciati, una luce gialla significa che i dati biometrici dovrebbero essere tracciati, ma il modulo non sta raccogliendo dati, una luce rossa significa che i dati biometrici non sono tracciati). Apposite interfacce vengono mostrate all'utente al fine di chiedere il consenso al tracciamento. Ad intervalli di tempo prestabiliti, il modulo di tracciamento cattura trasparentemente un'immagine dalla fotocamera e, lato server, viene effettuata l'autenticazione. Se l'utente non viene autenticato per un certo numero di tentativi consecutivi, viene reindirizzato alla pagina di login.

Sebbene il caso di studio riguardi la sperimentazione di soli dati biometrici facciali, la modularità e configurabilità dell'architettura rendono facile cambiare, aggiungere, rimuovere il tracciamento di un dato tratto biometrico e l'erogazione di un dato servizio. In fase preliminare, è stata analizzata in laboratorio l'operatività a regime sia lato server che lato client, variando il numero di dispositivi contemporaneamente attivi nel sistema. L'analisi dei tempi di risposta e del livello di utilizzo delle risorse computazionali ha permesso di validare con successo il caso di studio implementato, anche quando i dispositivi contemporaneamente attivi superano il centinaio di unità. È stato altresì effettuato un test su diversi browser e dispositivi, sia fissi che mobili. Questo ha permesso di identificare e risolvere particolari problematiche di incompatibilità, portando alla copertura pressoché totale dei browser e dei dispositivi esistenti.

5 Conclusioni e Lavori Futuri

In questo articolo, è stato presentato un sistema software in grado di supportare il tracciamento e il trattamento di svariati tratti biometrici all'interno di servizi integrati nelle piattaforme di apprendimento digitale. In aggiunta, è stato mostrato un caso di studio in cui il sistema biometrico proposto è stato impiegato per fornire un servizio di autenticazione biometrica degli studenti. La soluzione delineata è stata integrata con successo nella piattaforma di apprendimento promossa dal progetto "*iLearnTV Anywhere Anytime*". Le scelte progettuali garantiscono una bassa dipendenza tra il sistema biometrico e la piattaforma di apprendimento, favorendo la possibile integrazione del primo anche in altri ambienti digitali (es. Moodle). I test condotti hanno mostrato una buona capacità di gestione del carico computazionale e una buona portabilità su dispositivi fissi e mobili, auspicando un'ampia adozione del sistema in contesti reali.

Sulla base di quanto finora studiato e sperimentato, sono svariate le linee di ricerca e sviluppo che verranno investigate nel prossimo futuro. Tra queste, troviamo:

- **Modalità di Estrazione Dati**: poiché il tracciamento dei dati biometrici è il primo passo nella filiera, un errore a questo punto influirebbe sull'intero processo; tenuto conto che i sensori usati per raccogliere i dati non sono perfetti, le modalità di pre-processamento e pulizia dei dati raccolti richiedono particolare approfondimento.
- **Frequenza di Raccolta Dati**: per alcune biometrie, specialmente quelle comportamentali (es. battitura e movimento della mano), la frequenza di raccolta dei dati è elevata, quindi è necessario studiare protocolli di raccolta dati tali da garantire un uso efficiente del dispositivo client, dell'infrastruttura di rete, e dei server.
- **Modalità di Scambio Dati**: se non adeguatamente codificati, i dati in transito tra il dispositivo client e i server di gestione potrebbero essere intercettati ed utilizzati da individui non autorizzati; pertanto, è necessario applicare opportune metodologie di codifica dei dati biometrici durante la comunicazione client-server.
- **Variabilità dei Dati**: nel caso specifico dell'autenticazione degli studenti, le metodologie di riconoscimento biometrico adottate, soprattutto quelle basate su biometrie comportamentali, devono far fronte alla variabilità nei dati a seconda del contesto di tracciamento; pertanto, occorre studiare metodi robusti rispetto al contesto.
- **Capacità Operativa a Regime**: il tracciamento continuo di dati biometrici può generare un elevato carico computazionale sul dispositivo client o sui server di gestione; pertanto, al fine di poter essere impiegati in contesti applicativi reali, i metodi progettati devono saper gestire o limitare tale carico allo stretto necessario.
- **Facilità di Personalizzazione**: allo stato attuale, il sistema di tracciamento e trattamento di dati biometrici è rivolto al supporto degli sviluppatori di piattaforme di apprendimento; in futuro, si renderà necessario studiare interfacce utente che possano permettere anche ad utenti non esperti di poter personalizzare il sistema.
- **Validazione in Contesti Reali**: a seguito della prima fase sperimentale esposta nel presente articolo, si prevede di validare le soluzioni nelle organizzazioni scolastiche del territorio, coinvolgendo attivamente tutti gli attori dell'ecosistema.

In una visione ancora più ampia, la ricerca relativa all'uso di dati biometrici nel settore dell'istruzione pone tante altre sfide richiedenti studi ed applicazioni che esplorino:

- **Nuovi Ambiti Applicativi**: è necessario riflettere sui termini e gli ambiti in cui la biometria può essere usata per migliorare l'apprendimento e i servizi a supporto, in base ad osservazioni in contesti reali, oltre le puntuali applicazioni già esistenti.
- **Ricerca Multi-Disciplinare**: al fine di rispondere alle esigenze del mondo reale, è necessario includere nel processo di ricerca e sviluppo gruppi di lavoro interdisciplinari che condividano competenze teoriche, tecniche, pedagogiche e didattiche.
- **Procedure Consapevoli della Privacy**: è necessario identificare e gestire i rischi legati alla manipolazione di informazioni sensibili, come quelle biometriche, cercando di mediare tra aspetti meramente tecnici e implicazioni sociali derivanti.

Il sistema biometrico proposto rappresenta solo uno dei primi passi verso un'attività di promozione e diffusione dell'adozione delle biometrie per lo svolgimento di studi di settore e l'integrazione di servizi intelligenti che sfruttino le peculiarità di tali dati.

Ringraziamenti

Il presente articolo è stato prodotto nel Corso di Dottorato in Matematica e Informatica dell'Università degli Studi di Cagliari con il finanziamento P.O.R. SARDEGNA F.S.E. 2014-2020: ASSE III "Istruzione e Formazione", Obiettivo Tematico 10, Priorità d'investimento 10ii), Obiettivo Specifico 10.5, Azione Accordo Partenariato 10.5.12.

Le attività sono parzialmente supportate dal Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) nell'ambito del progetto "iLearnTV Anywhere Anytime" (DD n.193705.06.2014, CUP F74G14000200008 F19G14000910008).

Riferimenti Bibliografici

1. Technavio. Global Biometrics Market in Education Sector 2017-2021 (2019). Acceduto in data 2019.04.04. https://www.technavio.com/report/global-biometrics-in-education-sector.
2. Dasgupta, D., Roy, A., Nag, A. (2017). Biometrics Authentication. In: Advances in User Authentication. Springer International Publishing.
3. Taylor, E. (2013). Surveillance Schools: A New Era in Education. In Surveillance Schools: Security, Discipline and Control in Contemporary Education, 15-39. Palgrave Pivot, London.
4. Lukas, S., Mitra, A. R., Desanti, R. I., Krisnadi, D. (2016). Student attendance system in classroom using face recognition technique. In 2016 International Conference on Information and Communication Technology Convergence (ICTC), 1032-1035. IEEE.
5. Pleva, M., Bours, P., Hladek, D., & Juhar, J. (2016). Using current biometrics technologies for authentication in e-learning assessment. In :2016 International Conference on Emerging eLearning Technologies and Applications (ICETA), 269-274. IEEE.
6. Ghaleb, E., Popa, M., Hortal, E., Asteriadis, S., & Weiss, G. (2018). Towards Affect Recognition through Interactions with Learning Materials. In: 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), 372-379. IEEE.
7. Fenu, G., Marras, M., Boratto, L. (2018). A Multi-Biometric System for Continuous Student Authentication in E-Learning Platforms. Pattern Recognition Letters, 113, 83-92. Elsevier.
8. Khalfallah, J., Slama, J. B. H. (2015). Facial expression recognition for intelligent tutoring systems in remote laboratories platform. Procedia Computer Science, 73, 274-281.
9. Fenu, G., Marras, M., Barra, S., Giorgini, F., Zucchetti, D., Chesi, F. (2018). ILEARNTV: Un Ecosistema di Conoscenza Condivisa e Produzione Collaborativa per Innovare la Formazione. DIDAttica e inforMATICA-Informatica per la Didattica (DIDAMATICA), 49. AICA.
10. Fenu, G., Marras, M., Meles, M. (2017). A Learning Analytics Tool for Usability Assessment in Moodle Environments. Journal of e-Learning and Knowledge Society, 13(3). Italian E-Learning Association.
11. Gray, S. L. (2018). Biometrics in Schools. In: The Palgrave International Handbook of School Discipline, Surveillance, and Social Control, 405-424. Palgrave Macmillan, Cham.
12. Okokpujie, K. O., Noma-Osaghae, E., Okesola, O. J., John, S. N., Robert, O. (2017). Design and implementation of a student attendance system using iris biometric recognition. In: 2017 Int. Conf. on Computational Science and Computational Intelligence (CSCI), 563-567. IEEE.
13. Monkaresi, H., Bosch, N., Calvo, R. A., D'Mello, S. (2017). Automated detection of engagement using video-based estimation of facial expressions and heart rate. IEEE Tran. on Aff. Computing, 8(1), 15-28.
14. Chapman, D. W., Lindner, S. (2016). Degrees of integrity: the threat of corruption in higher education. Studies in Higher Education, 41(2), 247-268.
15. ProctorU. Acceduto il 2019.04.01. https://www.proctoru.com/.
16. Pearson VUE. Acceduto il 2019.04.01. https://home.pearsonvue.com/.
17. Proctorio. Acceduto il 2019.04.01. https://proctorio.com/.
18. ProctorFree. Acceduto il 2019.04.01. http://proctorfree.com/.
19. TeSLA. Acceduto il 2019.04.01. https://tesla-project.eu/.