Corso di Laurea in Informatica
Relazione tecnica del progetto di Modelli e Metodi per la Sicurezza delle Applicazioni:

Prototipo per la gestione degli accessi con sensore di impronta digitale basato su Arduino UNO

Professore:
Donato Impedovo

Studente:
Vincenzo Maria Giulio Martemucci

INDICE DEGLI ARGOMENTI

INTRODUZIONE E OBIETTIVI DEL PROGETTO

Oggi è possibile, con un po' di inventiva, una scheda con microcontrollore, componenti e capacità di scrivere del codice, cimentarsi nella realizzazione di svariati prototipi, da progetti casalinghi, fino ad applicazioni più complesse. Questa nuova tendenza, a mio parere molto interessante e stimolante, permette con relativa economicità, di realizzare molte idee.

Ad esempio, uno dei primi progetti che ho visto realizzare, sviluppati con una scheda di tipo Arduino, riguardava una pianta "capace" di inviare SMS.
Detto così suona strano, ma una volta analizzate componenti e funzioni di questo sistema, tutto diventa più comprensibile: un sensore di umidità viene posizionato nel terreno in cui è messa a dimora la pianta, quando l'umidità scende sotto una certa soglia, il sistema sfrutta un modulo gsm per inviare un sms in cui si comunica al proprietario della pianta, che la stessa necessita di essere annaffiata.

L'obiettivo di questo progetto è stato quello di mettere in pratica gli insegnamenti del corso di Esame di Modelli e Metodi per la Sicurezza della Applicazioni tenuto dal Professor Donato Impedovo.
Parte del programma di questo corso, è incentrato sulla conoscenza di sistemi biometrici, sul loro sviluppo, sulle differenze fra i vari tratti biometrici. Questa relazione ha quindi come proposito, la progettazione e la realizzazione di un prototipo di un sistema per la gestione degli accessi automatizzato, a basso costo, che permetta di riconoscere una persona autorizzata e garantirle l'accesso tramite la sua impronta digitale.

Il tratto biometrico scelto è quindi quello dell'impronta digitale che verrà immagazzinata, riconosciuta e utilizzata per stabilire se effettivamente l'utente che tenta l'accesso è autorizzato o meno. Questa tecnica è generalmente affidabile, pur presentando, come tutti i tratti biometrici, certi vantaggi e svantaggi.

L'impronta digitale, è un tratto biometrico che a confronto con altri tratti biometrici, ha caratteristiche ottimali, se considerate nel loro insieme. (Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability, Spoof).

POTENZIALITÀ E FUNZIONALITÀ DI SCHEDE TIPO ARDUINO UNO

Arduino nasce nel 2005 da un gruppo di ricerca dell' Interaction Design Institute di Ivrea, che ha progettato e realizzato una piattaforma elettronica di sviluppo, open source, basata su microcontrollore.

La versatilità di queste schede, unita alla loro economicità ha fatto sì che diventassero molto utili sia a scopi didattici che a scopi di ricerca o di prototipazione.

Le schede tipo ARDUINO, permettono non solo il caricamento di programmi su una memoria flash incorporata, ma consentono anche di utilizzare funzionalità di input/output. Infatti, oltre all'hardware, Arduino include un proprio IDE, dove è possibile scrivere i programmi che verranno caricati ed eseguiti dal microcontrollore.
Questi programmi prendono il nome di *sketch*.

Grazie alle funzionalità di input, la scheda accoglie i segnali raccolti dai sensori esterni, opportunamente connessi alla stessa. In base ai segnali raccolti, il micro-controller gestirà il comportamento della scheda coerentemente con le istruzioni determinate dal programma in esecuzione in quel momento sulla scheda. Il programma, quindi, gestirà anche la fase di output, per mezzo dei canali di output connessi alla scheda.

Una caratteristica molto utile ed interessante di queste schede è l'espandibilità. Infatti, tramite apposite *shields* è possibile espandere le funzionalità delle schede ARDUINO.
Anche questi componenti seguono l'idea base di ARDUINO, ovvero sono economiche e relativamente facili da montare.
Esiste una grande varietà di *shields*, dai già menzionati sensori di umidità, a sensori di temperatura, pressione, schermi LED, moduli wi-fi, moduli gsm, gps, e tanto altro ancora.

Per questo progetto mi sono avvalso di una scheda tipo **ARDUINO UNO**.

COMPONENTI UTILIZZATI

- Scheda SMRAZA UNO R3, basa su ARDUINO UNO, con le seguenti specifiche tecniche:

TECH SPECS

Microcontroller	ATmega328P
Operating Voltage	5V
Input Voltage	7–12V(recommended) / 6–20V(limit)
Digital I/O Pins	14 (of which 6 provide PWM output)
Analog Input Pins	6
DC Current per I/O Pin	20 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB (ATmega328P) of which 0.5 KB used by bootloader
Clock Speed	16 MHz

Figura A - Scheda Tecnica SMRAZA UNO R3

Figura B - Scheda SMRAZA UNO R3

- Modulo di scansione delle impronte digitali di tipo ottico

Si tratta di un modulo integrato, perché unisce il percorso di acquisizione delle impronte e la parte della verifica delle stesse.
Il sistema memorizza le impronte digitali autorizzate in un database interno, assegnando un ID ad ognuna di queste impronte.
Dopo la lettura di una nuova impronta digitale, questa viene confrontata con quelle in memoria per autorizzare o meno l'utente che ha provato l'accesso

Power	DC 3.6V-6.0V	**Interface**	UART(TTL logical level)/ USB 1.1
Working current	Typical: 100mA Peak: 150mA	**Matching Mode**	1:1 and 1:N
Baud rate	(9600*N)bps. N=1～12 (default N=6)	**Character file size**	256 bytes
Image acquiring time	<1s	**Template size**	512 bytes
Storage capacity	120/ 375/ 880	**Storage size**	127 id
FAR	<0.001%	**FRR**	<0.1%
Average searching time	< 1s (1:880)	**Window dimension**	14mm*18mm
Working environment	Temp: -10℃- +50℃	**Storage environment**	Temp: -40℃- +85℃
	RH: 40%-85%		RH: <85%
Outline Dimention	Split type	Module: 42*25*8.5mm (install dimension: 31.5*19mm) Sensor:56*20*21.5mm	
	Integral type	56*20*21.5mm	

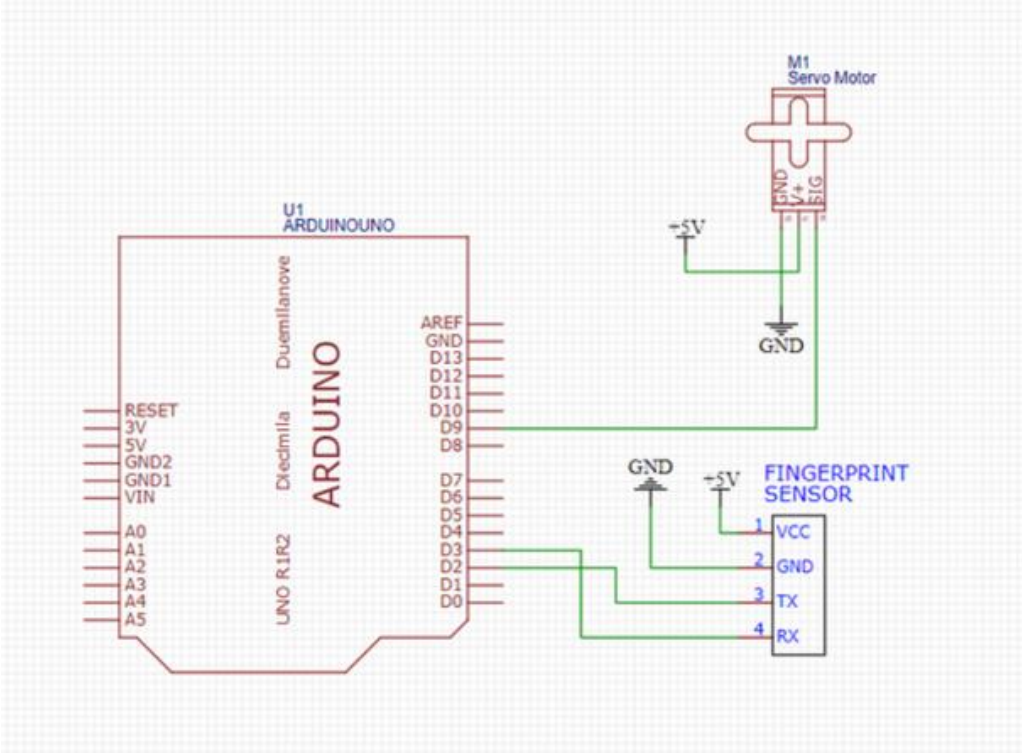
Figura C scheda tecnica del sensore di impronte

Questa scheda tecnica, presenta anche delle indicazioni sulle performance di verifica e identificazione delle impronte da parte del lettore.
FAR (False Acceptance Rate) e FRR (False Rejection Rate).

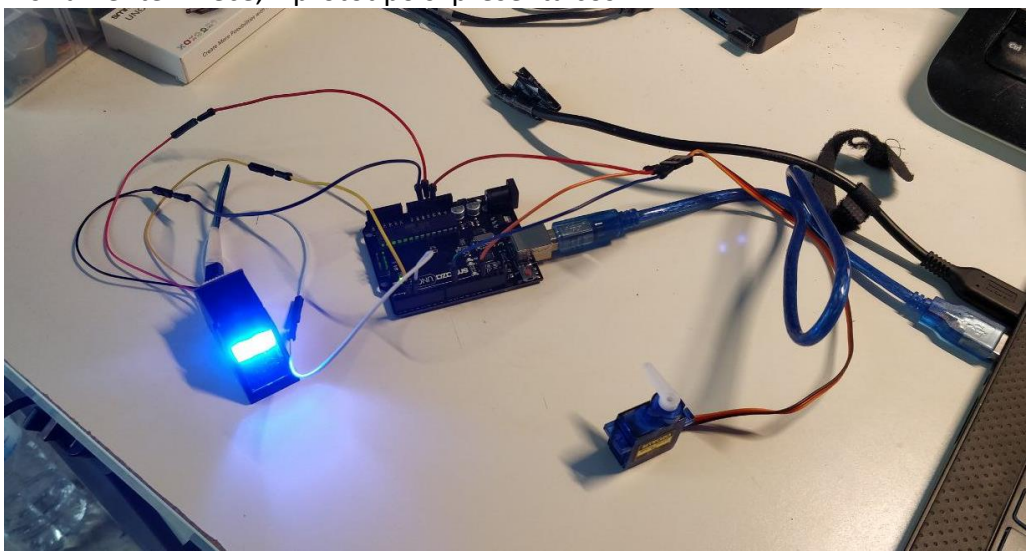
- Un servomotore, utilizzato per simulare l'apertura di una porta, o l'accesso ad un sistema.

- Opzionalmente, un buzzer utilizzato per espandere il prototipo in modo che il sistema emetta un avviso sonoro qualora l'impronta non venga riconosciuta. Utile ad avere una risposta anche sonora durante l'utilizzo del sistema.

La scheda ARDUINO, il sensore e il servomotore sono stati collegati secondo questo schema:



Visivamente invece, il prototipo si presenta così:



LIBRERIE, CODICE E FUNZIONAMENTO DEL SISTEMA

Per l'utilizzo del sensore ottico, ho utilizzato la libreria ADAFRUIT per acquisire le impronte digitali e memorizzarle sul dispositivo.
https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library
Il modulo di scansione delle impronte digitali può conservare fino a 127 ID, ogni ID è associato ad un'impronta digitale autorizzata ad accedere al sistema.

Per il riconoscimento delle impronte invece ho utilizzato uno *sketch* Arduino personalizzato (Serratura_impronta_digitale_martemucci.ino).

In breve, il sistema acquisisce le impronte e autorizza o nega l'accesso.
Più nel dettaglio, tramite un loop, il sistema è sempre in attesa di una nuova impronta, una volta che un'impronta verrà acquisita, la stessa verrà confrontata con quelle memorizzate presenti in memoria.
Nel momento in cui l'impronta viene riconosciuta come autorizzata, la scheda ARDUINO fa aprire il servomotore per un tempo stabilito (in questo caso cinque secondi), per poi richiudersi e tornare nello stato iniziale.

VANTAGGI E SVANTAGGI DEL SISTEMA

I vantaggi e gli svantaggi sono innanzitutto quelli intrinseci dell'impronta digitale usata come tratto biometrico. L'impronta digitale è molto discriminante, non cambia nel tempo ed è ritenuta affidabile. L'uso dell'impronta digitale ha un basso impatto sull'utente ed è abbastanza semplice da implementare. Fra gli svantaggi propri del tratto, alcune persone hanno impronte di bassa qualità. (es. per motivi legati ad età, abitudini, sport, lavori particolari, etc.)
Un problema legato al sensore può essere la sporcizia sullo stesso.
In alcuni casi, tramite calchi, è possibile ricreare delle impronte digitali e ingannare lettori di impronte non particolarmente sofisticati.

Altri vantaggi del sistema, consistono nella loro economicità. Le scheda tipo Arduino UNO, offrono una base economica, intuitiva, personalizzabile ed espandibile. I moduli accessori, necessari per estendere il sistema ed ampliarne le funzionalità, hanno costi contenuti, un'affidabilità accettabile per un ambito di prototipazione e, come accade generalmente con i componenti elettronici, hanno una modularità pressoché totale. Aggiungere troppe espansioni però, può far aumentare i costi del prototipo, oltre a poter rendere necessario l'uso di schede con più memoria, e con più periferiche.

PERFORMANCE EVALUATION

Per valutare le performance del sistema, si è simulato un utilizzo verosimile dello stesso.
Il caso specifico che ho considerato è quello dell'accesso della mia abitazione privata, dove quattro persone sono autorizzate ad accedere.
Si suddivide il test in due fasi.

1. Addestramento del sistema: *enrollment* delle impronte digitali autorizzate.
2. Test di accesso del sistema: identificazione degli utenti autorizzati che provano ad accedere

Per ogni persona autorizzata, ho simulato 30 accessi per calcolare il **FAR**, False Acceptance Rate, facendo utilizzare a tutti l'impronta dell'indice sinistro, non registrata come autorizzata e altri 30 accessi per calcolare il **FRR**, False Rejection Rate, facendo utilizzare a tutti l'impronta dell'indice destro, registrata come autorizzata.
I risultati ottenuti sono stati i seguenti:

	FAR	**FRR**
Vincenzo	0/30	1/30
Vivi	0/30	0/30
Lia	0/30	0/30
Michele	0/30	0/30
TOTALE	0/120 (0%)	1/120 (0.83%)

In media, considerando il totale dei tentativi per impronte autorizzate e non autorizzate, abbiamo ottenuto un solo rifiuto per utente genuino e nessuno acceso per utente impostore, per un errore pari a 1/240 = 0.42%,

Occorre comunque tenere conto che l'accuratezza del calcolo del FAR e del FRR, dipende dal numero di test fatti e da altre condizioni, ad esempio: lo stato di pulizia del sensore ottico, la disposizione del dito sul sensore, il grado di cooperazione dell'utente nonché la qualità dell'impronta dell'utente stesso, etc.

ALTRI USI POSSIBILI

Oltre all'apertura di una serratura, in questo caso simulata con un servomotore, è possibile aggiungere altre componenti, per espandere il prototipo. Ad esempio, attraverso uno schermo LCD 2x16, si può comunicare in output, non solo eventuali messaggi di errore avvenuti, ma anche il nome di chi ha appena effettuato l'accesso.

Su questa scia, è anche possibile espandere il prototipo, prevedendo un modulo GSM che invia tutti i dati di accesso, come ad esempio nome e orario di accesso, ad un numero telefonico o in alternativa, tramite un modulo WIFI, il sistema può inviare questi dati ad un server.

Per esigenze progettuali, il prototipo è stato associato all'apertura di una serratura, ma tramite opportune modifiche e interfacce può avere altre applicazioni, ad esempio:

- Accesso sicuro a personal computer
- Transazioni elettroniche
- Accesso a sistemi di informazioni personali
- Sulla base di questo prototipo, è possibile costruire un semplice sistema multi-biometrico, implementando un secondo sensore che raccolga l'impronta di un altro dito dell'utente registrato.

CONCLUSIONI

Grazie ad un sistema del genere, non solo è possibile garantire, a costi bassi, un accesso esclusivo ad utenti autorizzati, ma si ha anche la possibilità di espandere il sistema ed implementare un vero e proprio «diario» degli accessi, in maniera tale da avere contezza di chi ha avuto accesso al sistema, e quando.
Il sistema in oggetto in definitiva si è comportato secondo le aspettative e cosa più importante di tutte, non ha mai consentito l'accesso ad un utente non autorizzato.

Personalmente ho voluto concentrarmi su questo tratto biometrico poiché lo trovo affascinante: non solo offre una relativa semplicità di utilizzo e caratteristiche ottimali, ma mi ha colpito anche la sua lunga storia, che vede le sue prime tracce datate al 1686, quando il Professore di anatomia Marcello Malpighi, notò nelle impronte digitali, la presenza di creste, spirali e *loop*.