Università degli Studi di Firenze
Facoltà di Ingegneria

Corso di Laurea in
Ingegneria Informatica

Protocollo sicuro per l'elaborazione di dati cifrati mediante una rete neurale

Relatore: Piva Alessandro

Candidato: Caini Michele

Co-relatori:
Bianchi Tiziano
De Rosa Alessia
Orlandi Claudio

A.A. 2006/2007

Introduzione

La necessità crescente di sicurezza unita alla potenza classificativa delle reti neurali ha portato alla nascita di un protocollo che permettesse di sposare le due cose, in modo da ottenere reti neurali sicure grazie alla loro capacità di operare in dominio cifrato. Lo scopo di questo protocollo è quello della classificazione remota sui dati in assenza di una terza parte fidata, che preveda un livello di interazione minimo fra le due parti coinvolte.

Da un lato, le tecniche che mirano a conseguire politiche di sicurezza si fanno di giorno in giorno più raffinate e permettono di esplorare terreni impensabili fino a poco tempo fa. La spinta nello studio di aspetti particolari dei cifrari, come le loro proprietà omomorfiche, permette di inquadrare questi oggetti in un'ottica del tutto nuova che prevede lo sfruttamento di tali caratteristiche per riuscire ad ottenere operazioni in chiaro senza dover passare obbligatoriamente da fasi di decifratura e conseguente cifratura. A partire da questo punto di vista nasce una *nuova matematica*, che permette di operare su valori cifrati per applicare indirettamente funzioni lineari ai valori in chiaro.
Dall'altro lato, le reti neurali stanno prendendo sempre più piede in svariati ambiti e si stanno affermando come strumento potente, flessibile e preciso, utile alla classificazione dei dati e alla rappresentazione di funzioni difficilmente esprimibili o di cui, addirittura, niente ancora si conosce. Lo studio, in questo campo, sta portando alla scoperta di tecniche e algoritmi capaci di generalizzare sui dati, ottenendo così reti neurali in grado di dare risposte sempre più precise.

Il matrimonio fra queste due scienze sfocia in un protocollo che permette di mettere a disposizione degli utenti reti neurali per un utilizzo remoto, fornendo una discreta riservatezza a chi si affida al servizio e vuole proteggere i propri dati come ovviamente anche sicurezza per chi investe nella creazione e nell'addestramento delle reti neurali.
Un terzo elemento importante che ha permesso l'implementazione di un protocollo del genere è sicuramente l'insieme di strumenti messi a disposizione dello sviluppatore, i quali permettono di rendere realizzabili e reali un gran numero di idee: dalla teoria alla pratica, per poter toccare con mano ed esplorare una delle nuove frontiere della crittografia.

Il lavoro di tesi si propone di realizzare uno strumento che permetta di toccare con mano il protocollo in questione, indagando tanto sull'effettiva possibilità di implementazione quanto sulle prestazioni ottenibili in ambienti reali, per dare una risposta all'ovvia domanda se questo possa o meno trasformarsi in una soluzione concreta e rappresentare un possibile futuro in questo ambito.

La discussione riguardante l'argomento si articola in tre capitoli che affrontano e descrivono rispettivamente la parte teorica, le fasi di sviluppo e i test portati avanti sul prodotto finale. Segue una breve descrizione sui contenuti di ogni singolo capitolo:

- **Capitolo 1**: in questo capitolo è descritto il protocollo proposto e sviluppato nel lavoro di tesi; vengono discussi gli aspetti importanti di questo protocollo, gli algoritmi coinvolti e le tecniche per conseguire la sicurezza in seno tanto all'utente quanto a chi fornisce le reti neurali per l'uso remoto e sono trattati gli elementi chiave utilizzati, quali il cifrario, con le loro proprietà e caratteristiche

- **Capitolo 2**: essendo il prodotto finale un software che implementa il protocollo proposto e descritto nel capitolo 1 è necessario dedicarsi all'analisi della struttura del programma discutendone le fasi di progettazione, le scelte effettuate, le problematiche incontrate e le soluzioni introdotte per risolvere tali questioni, discutendo anche i mezzi utilizzati per realizzare il prodotto finale; in realtà, la trattazione non scende nei dettagli del codice spiegandone ogni singola riga o funzione, piuttosto è data una panoramica degli attori principali nel progetto e di come questi implementino soluzioni utili

- **Capitolo 3**: un software è, ovviamente, valutato in base a parametri di complessità, al comportamento che presenta a seguito di variazioni sulle variabili d'ambiente e, perché no, al corretto funzionamento (un programma il cui risultato non è quello atteso, anche se presenta prestazioni invidiabili è di scarso interesse): in questo capitolo è portata avanti un'analisi in base a dati sperimentali nel tentativo di estrapolare una legge che possa risultare utile a prevedere il comportamento del programma in base ad alcuni parametri predefiniti, come il fattore di quantizzazione o il numero di nodi fittizi

Sarà quindi discusso il come, a partire dal cosa, per arrivare al quanto.
Cosa tratta il protocollo proposto, analizzato e descritto in ogni sua sfaccettatura per capirne in linea teorica il funzionamento e poterne comprendere le problematiche, importanti anche dal punto di vista realizzativo.
Come questo è stato implementato, senza tralasciare le metodologie e le tecnologie utilizzate per raggiungere lo scopo, focalizzando sui modi in cui problemi affrontati in linea teorica e relative soluzioni sono stati affrontati e risolti praticamente.

Quanto è realmente utilizzabile il software, indici di prestazione e degenerazione dei valori in base ai parametri di ambiente, un'approssimazione del comportamento per stime a priori, cercando di estrapolare una legge che fornisca indizi sul comportamento del programma in base a variabili esterne.

La discussione si articola quindi in tre settori principali e attraverso questi guida l'analisi dalla teoria alla pratica, fornendo infine risultati concreti nella forma di un software chiamato NNSec.