

山口 俊光[†] 納富 一宏[†] 石井 博章[†] 斎藤 恵一[‡] 藤本 哲男^{‡‡}[†]神奈川工科大学情報工学科[‡]東亜大学経営学部経営学科^{‡‡}芝浦工業大学工学部機械工学科

1 はじめに

未知の症例の病態を類推・検討する際、過去の臨床症例を検索し閲覧しながら行うことができれば大変便利である。しかしながら、臨床症例のような医療情報には個人情報が含まれる場合があるので、IDとパスワードのみによる従来の認証方式では安全性が十分とは言えない。

このパスワードのみで行なう認証の弱点を補うため提案がなされている。我々は以前、自己組織化マップを用いてパスワードを入力する際のタイミングから認証を行う手法を提案した [1]。

そこで、本稿では先の提案で課題として残された、認証の結果の安定性を高めるという点について述べる。

2 システムの構成

Fig.1 に示すようにインターネットを介したサーバ/クライアントモデルで構成されている。クライアントは Java Applet として、サーバは Java Servlet としてそれぞれ実装されている。認証に必要な ID、パスワード、パスワードを入力する際の打鍵タイミングをクライアント側で取得し、それをサーバに送信する。サーバ側では送られてきた情報で認証を行う。現在の実装ではクライアントに対し認証が成功か失敗かを返し、クライアントがそれをユーザに提示するようになっている。

今回実験用に構築したシステムのプログラムの規模は、サーバサイド、クライアントサイドあわせて 1600 行程度である。

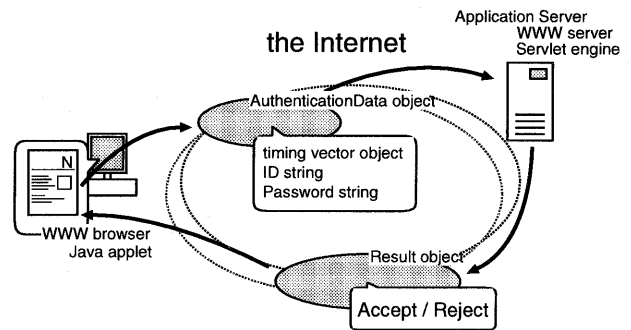


Fig. 1: System Structure

3 自己組織化マップを用いた個人認証

3.1 自己組織化マップの生成

自己組織化マップを生成するための学習用にユーザ登録の際にキータイプの間隔を計測をおこなう。間隔の測定は 1 ミリ秒単位で行われる。今回は生成のために 1 人につき 4 回分のパスワード入力タイミングを収集した。収集したタイミングを入力として、2000 回の学習を行い認証に用いるマップを生成する。

3.2 複数マップによる認証

以前、提案したシステムでは、1 枚の自己組織化マップを用いて認証を行っていた。この単一マップ認証では、SOM の学習結果の変動が大きく、本人拒否率 (FRR) が極端に高くなる場合が認められた。そこで、今回は学習結果の不安定さを補うため、複数のマップを用いて認証する方法を検討した。

システムにログインするときも生成時と同様に打鍵タイミングを測定する。入力された文字列が正しいかどうかを確認し、パスワードを入力した際の打鍵タイミングを入力ベクトルとして、マップ上にマッピングする (Fig.2)。

この際に Fig.3 に示すように、3 枚のマップに同時マッピングする。マップ作成時に用いた入力的位置と新たな入力的位置のユークリッド距離を各マップについてもとめ、一定の閾値以下のマップが 2 枚以上あればログインを許可し、そうでなければパスワードが正確に入力されていてもログインを拒否する。

Development of DBMS for Clinical Cases : Improvement of Personal Authentication with Keystroke Timing Pattern on Self-Organizing Maps

Toshimitsu YAMAGUCHI[†] Kazuhiro NOTOMI[†] Hiroaki ISHII[†] Keiichi SAITO[‡] Tetsuo FUJIMOTO^{‡‡}

[†]Department of Information and Computer Science, Kanagawa Institute of Technology

[‡]Department of Business Management, Faculty of Business Management, University of East Asia

^{‡‡}Department of Mechanical Engineering, Shibaura Institute of Technology

e-mail: mit@ish.ic.kanagawa-it.ac.jp

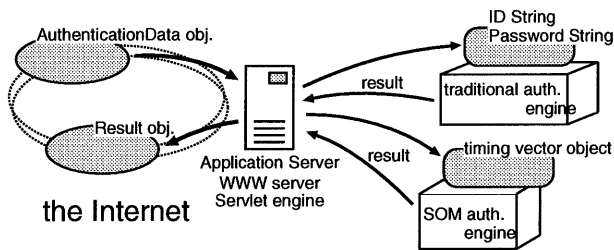


Fig. 2: SOM based Personal Authentication System

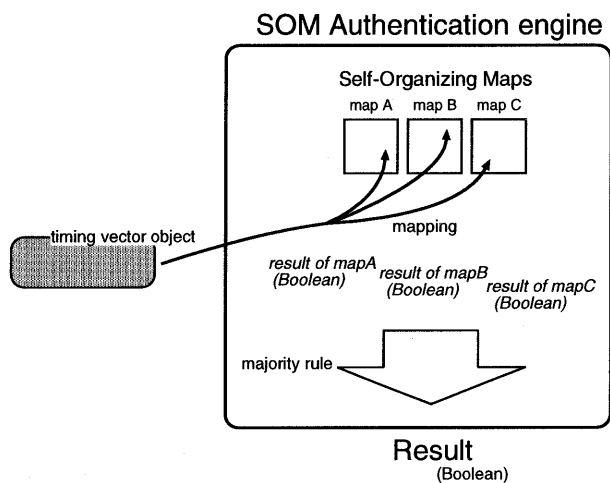


Fig. 3: 3 maps SOM Authentication Engine

4 評価

4.1 評価方法

同じパスワードの打鍵タイミングをマップ作成用に4回、試行用に30回計測した。実験は、「5分間タイプ練習」、「3分間休憩」、「計測」の順で行った。3枚のマップを作成し、各マップに試行用の入力をマッピングする。マップ作成用入力4点からのユークリッド距離をそれぞれの測定し平均値を求める。その平均が0から80まで1きざみの閾値より小さければ「受容」とし、閾値以上であれば「拒否」として閾値ごとのFRR(False Reject Rate:本人拒否率)およびFAR(False Accept Rate:他人受容率)を計算した。FAR, FRRの定義式を以下に示す。

$$FAR = \frac{\text{他人受容回数}}{\text{試行回数}} \quad (1)$$

$$FRR = \frac{\text{本人拒否回数}}{\text{試行回数}} \quad (2)$$

4.2 評価結果

実験結果を Fig.4 に示す。値は30試行分のFAR, FRRの平均を10人分求め、それを平均したものである。

る。FRRが10%以下になる閾値とFARが60%以下になる閾値を Table.1 に示す。

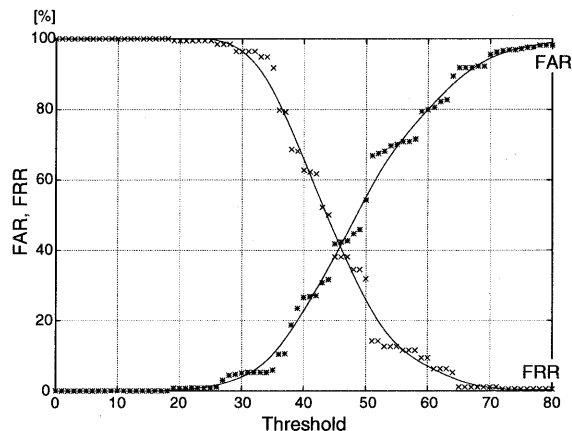


Fig. 4: FAR and FRR (Average)

Table. 1: 3 map Result

Threshold	59	50
FAR[%]	79.46	54.30
FRR[%]	9.39	31.87

パスワードが盗まれてしまった場合、通常のパスワードのみの認証方式ではFRRは0%に近いが、FARは100%になってしまう。本システムを用いることによりFARを50%強に抑えた閾値50の場合でもFRRは30%程度にとどめることができた。

また、ユーザごとの認証結果のばらつきを抑え、安定したFAR, FRRを得ることができるようになった。

5 まとめ

複数の自己組織化マップを用いた個人認証について述べた。今後はFAR, FRRの低下をはかり、信頼性の向上を目指す。

参考文献

- [1] 山口, 納富, 他: WWWによる臨床症例検索システムの開発 — 自己組織化マップを用いた打鍵タイミングによる個人認証, 情報処理学会第61回全国大会講演論文集, 4R-4 (2000).
- [2] Simson Garfinkel, G. S.: UNIX & インターネットセキュリティ, O'REILLY (1998), 山口 英 監訳, 谷口 功 訳.
- [3] 徳高平蔵, 他: 自己組織化マップの応用, 海文堂 (1999).