Una propuesta de arquitectura biométrica de control de acceso basada en ontologías

Javier Guerra Casanova[1], Alberto de Santos Sierra[1], Carmen Sánchez Ávila[1] y Vicente Jara Vera[2]

[1] Grupo de Biometría y Tratamiento Numérico de la Información.
Centro de Domótica Integral (CeDInt)
<jguerra@cedint.upm.es>
<alberto@cedint.upm.es>
<csa@mat.upm.es>
[2] Dpto. de Matemática Aplicada a las Tecnologías de la Información.
ETSI de Telecomunicación. Universidad Politécnica de Madrid.
Ciudad Universitaria s/n, 28040 Madrid
<vjara@mat.upm.es>

Resumen Hoy en día existen multitud de investigaciones sobre técnicas biométricas para autenticar a personas y cuantificar su estado físico y psíquico (cansancio, ansiedad, estrés...) En este artículo se propone integrar estas técnicas en una arquitectura de control de acceso basada en el modelo OrBAC ("Organization-based Access Control"). Con esta propuesta, el administrador de seguridad de una organización va a ser capaz de definir las políticas de seguridad de alto nivel que van a dar acceso a un usuario al sistema, así como las políticas de autenticación y comprobación de características que un usuario ha de verificar para que el sistema pueda confirmar que es quién dice ser y que está capacitado para realizar la acción para la que solicita acceso. Para la definición de los elementos de una organización a bajo y alto nivel, para la especificación de las técnicas biométricas disponibles en una organización y para la gestión de las políticas de seguridad, autenticación y comprobaciones biométricas se ha desarrollado una ontología, que al razonar sobre ella, traducirá las políticas de alto nivel a órdenes concretas a realizar por el usuario que trata de acceder al sistema. Esta arquitectura propuesta puede ser utilizada por cualquier organización que quiera imponer unas políticas de seguridad de acceso muy alto, por tanto, puede ser de gran utilidad para entornos militares, hospitales, centrales nucleares o aeropuertos.

Palabras clave: Biometría, Arquitectura de Control de Acceso, OrBAC, Razonamiento Ontológico, Autenticación, Comprobación Biométrica.

1. Introducción

Este artículo trata de definir una arquitectura completa de control de acceso según la identidad y las capacidades de las personas para realizar una acción en concreto.

Esta arquitectura puede ser muy útil para ambientes de alta seguridad, donde no solo hay que asegurar que la persona que accede sea realmente ella, sino que también es importante que para realizar una acción la persona esté en plenas facultades físicas y psicológicas.

Hoy en día existen muchas líneas de investigación para autenticar a una persona mediante sus características biométricas, [1], [2], así como para la medición de ciertos parámetros que indican el estado físico y psicológico de una persona antes de realizar una acción, [3], [4]. Esta arquitectura va a tratar de integrar todas estas técnicas, para que puedan utilizarse unas u otras según se requieran.

Gracias a este sistema, pueden aplicarse autenticaciones multimodales o comprobaciones de diversas características físicas o psicológicas de las personas para la realización de acciones de alta seguridad, [5], [6], [7].

Este sistema permite elevar el nivel de seguridad de acceso a un sistema no solo controlando el acceso, sino comprobando biométricamente la identidad de la persona que accede y la capacidad física y psíquica que tiene para realizar ciertas acciones en el sistema.

Esta arquitectura puede ser de gran utilidad en entornos de alta seguridad como aeropuertos, hospitales, bancos y servicios secretos o militares, donde se requiere un control de acceso muy rígido a determinados lugares y estar en plenas facultades a la hora de realizar ciertas operaciones, como manejar un avión, operar en el quirófano, realizar una gran transferencia bancaria o acceder a documentos secretos.

El artículo se compondrá de las siguientes secciones: En primer lugar se explicará la arquitectura general propuesta, introduciendo cada una de las fases que va a tener la misma. A continuación se comentará la tecnología de acceso OrBAC, [8], que se utilizará como base del modelo que se ha definido. En las secciones siguientes se expondrán cada una de las fases propuestas en la arquitectura, detallando la ontología necesaria para controlar el razonamiento en cada una de ellas. Por último el artículo concluirá con unas conclusiones de las ventajas del modelo propuesto.

2. Arquitectura propuesta

La arquitectura que se propone para el control de acceso se basa en tres fases:

1. Identificación : El usuario se identificará en el sistema e indicará qué quiere hacer. El sistema comprobará que el usuario existe en su base de datos y comprobará que tiene el permiso necesario para realizar la acción que solicita.
2. Autenticación: Si el usuario tiene el permiso necesario para ejecutar la acción que solicita, el sistema le exigirá que autentique su identidad mediante

ciertas técnicas biométricas que la organización ha de disponer. Según el perfil del usuario, la acción que quiera realizar y las políticas de seguridad correspondientes definidas por el administrador del sistema el usuario deberá autenticarse en diferentes aparatos de manera multimodal. Para ejecutar acciones que se quieran dotar de mayor de seguridad será necesario autenticarse a través de más técnicas biométricas.

3. Comprobación de capacidades: Una vez autenticado, el sistema podrá exigir realizar las comprobaciones biométricas necesarias que aseguren que el usuario está en condiciones de realizar la acción que pretende. Según las políticas de decisión del sistema, se decidirá si el usuario tiene acceso o es rechazado por el mismo.

Según esta arquitectura, el rechazo de un usuario puede realizarse tras cualquier etapa, en todos estos supuestos:

- Si no hay una identificación almacenada en el sistema del usuario que trata de acceder al mismo.
- Si las políticas de seguridad del sistema no permiten que el usuario realice la acción que solicita.
- Si el sistema reconoce mediante técnicas biométricas que el usuario que trata de acceder no es quien ha dicho que es.
- Si el usuario no se encuentra en condiciones de realizar el acceso al sistema.

Para el control de los accesos y rechazos al sistema se proponen unas políticas de seguridad en dos niveles basadas en la arquitectura OrBAC, donde el administrador de seguridad podrá definir unas políticas de seguridad de alto nivel, que derivarán en políticas de seguridad de nivel concreto, [9].

Para controlar cada una de las fases y las políticas de seguridad del sistema se han definido varias ontologías, que se explicarán en la sección propia de cada fase del modelo.

3. Control de acceso basado en la filosofía OrBAC

El control de acceso a una organización se basa en la arquitectura OrBAC, que define dos niveles de comportamiento.

En el nivel concreto, un sujeto realiza una acción sobre un objeto. Para un nivel superior, se definen las entidades Rol; como un conjunto de sujetos con las mismas características de seguridad, Actividad; como una agrupación de acciones del mismo nivel de seguridad y Vista; como un grupo de objetos protegidos por las mismas condiciones de seguridad.

El administrador de seguridad en OrBAC define unas políticas de seguridad de alto nivel en el que va a prohibir/permitir/obligar a todos los sujetos que pertenecen a un rol realizar las acciones agrupadas en una actividad sobre todos los objetos incluidos en una vista.

Además, OrBAC define el concepto de Contexto, [10], para definir distintas condiciones que pueden alterar las políticas de seguridad de una organización, por ejemplo, condiciones temporales (horario nocturno, navidad), condiciones de localización (oficinas de Montevideo) u otras. Las políticas de seguridad de alto nivel, incluyen los contextos de aplicación, y solo se activarán si en el momento de intentar acceder, la organización se encuentra en ese contexto.

Según la arquitectura OrBAC, las políticas de alto nivel definidas, se traducen automáticamente en políticas de seguridad de nivel concreto que son las que indican si un usuario en particular tiene permiso para realizar la acción que solicita sobre el objeto correspondiente.

A partir de la arquitectura OrBAC, este trabajo propone incluir las comprobaciones biométricas de autenticidad y de disposición a realizar la actividad dentro del modelo mediante ontologías, tal y como se explicará en las secciones siguientes.

4. Fase de identificación

Cuando un usuario trata de acceder al sistema, lo primero que ha de hacer es identificarse, mediante un código, una tarjeta o similar. En este primer paso el sistema comprobará que el sujeto pertenece al sistema y que además, el usuario tiene permiso para realizar la acción. Para ello se basará en la definición de una organización según el modelo OrBAC junto a las políticas de acceso definidas por el administrador del sistema que van a decidir si el Sujeto que llega al Sistema tiene permiso para realizar la Acción que solicita en el Contexto en el que se encuentra. Puede observarse como funciona el razonamiento en el esquema de la figura 1:

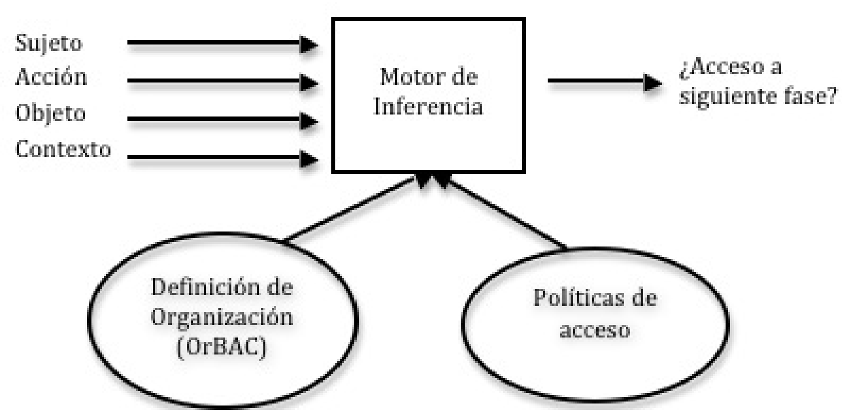

Figura 1. Razonamiento en la fase de identificación

Para controlar esta fase, se ha definido una ontología que implementa todas las clases necesarias. Se agrupan en dos grandes grupos:

- Para representar los elementos de una organización: Se han definido como clases de la ontología todos los elementos posibles de una arquitectura Or-BAC.
  - Sujeto
  - Rol
  - Acción
  - Actividad
  - Objeto
  - Vista
  - Contexto
- Para definir las políticas de acceso a la organización:
  - PoliticaAltoNivel
  - Permiso

El administrador del sistema define instancias de la clase PoliticaAltoNivel que indican qué Roles tienen permiso para realizar qué Actividades sobre qué Vistas.

Al llegar un usuario al sistema e identificarse, el motor de inferencia razona sobre la ontología para decidir si el sujeto que ha llegado tiene permiso para realizar la acción solicitada sobre el objeto indicado, en el contexto que se encuentra la aplicación. Para ello, es necesario que el propio razonador haga una conversión de políticas de seguridad de alto nivel a Permisos de bajo nivel, que indiquen qué Sujetos pueden ejecutar qué Acciones sobre qué Objetos.

En el caso de que el usuario tenga el permiso para realizar la acción, se pasa a la siguiente fase de la arquitectura propuesta: la fase de autenticación biométrica multimodal.

5. Autenticación biométrica multimodal

En esta fase, se propone que el sistema realice una autenticación biométrica del usuario. Una vez que se ha determinado que el usuario que dice ser tiene permiso para ejecutar la acción que solicita, puede ser necesario para ciertas operaciones realizar una autenticación biométrica para comprobar que la persona que accede es quien dice ser.

El administrador del sistema va a definir políticas de autenticación que exijan que un usuario pase con éxito una/varias/ninguna autenticaciones biométricas a través de varias técnicas en función del Rol al que pertenezca, el tipo de acción que quiera ejecutar sobre el tipo de objeto determinado y el contexto del sistema.

En esta fase, la inferencia sigue el esquema de la Figura 2:

Para la implementación de esta fase se han añadido en la ontología de la sección anterior varias clases agrupadas de la siguiente manera:

- Clases para definir los distintos tipos de autenticación biométrica. Para ello se propone adaptar a ontologías la propuesta de Wayman de sistematización de métodos biométricos, [11], incluyendo las siguientes clases:

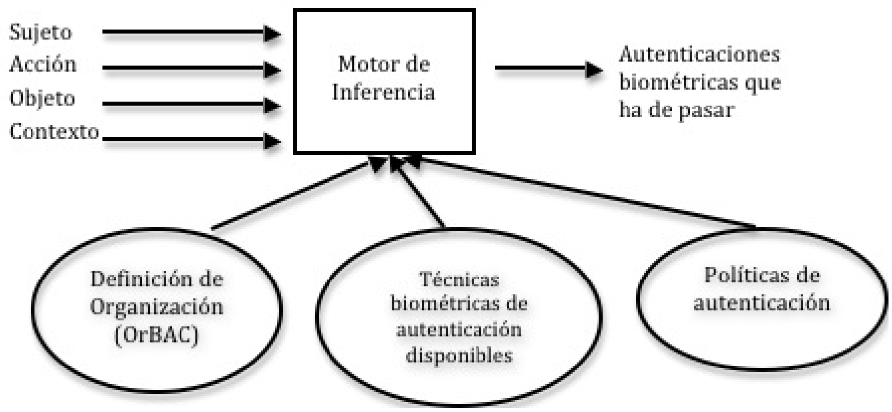

Figura 2. Razonamiento en la fase de autenticación

- Pattern: La característica biométrica que se va a utilizar para autenticar al usuario (Cara, [12], Huella, [13], Iris, [14], Geometría de la mano, [15] . . .)
- Structure: Lo que se va a medir de la característica biométrica. Por ejemplo, en firma: velocidad y aceleración, presión..
- Extraction: Método para extraer los patrones biométricos del usuario: Análisis matemáticos morfológicos, análisis de wavelets, Vectores propios..
- QualityControl: Métodos para comprobar que las muestras obtenidas del usuario son de calidad o no: Modelos de Markov, Vectores propios, procesamientos de imágenes.
- Recognition: Métodos de comparación de patrones: Correlaciones, Modelos de markov, Redes neuronales. . .

Además, habría que incluir la clase Autenticacion, que va a incluir las características de cada una de las técnicas biométricas que va a soportar la organización. Estarán definidas las propiedades autenticacion_pattern, autenticacion_structure, autenticacion_extraction, autenticacion_qualityControl y autenticacion_recognition que relacionan las instancias Autenticacion con cada una de las clases correspondientes. También, es imprescindible añadir una propiedad autentication_id que relacione la técnica biométrica con el dispositivo físico que posee la organización para realizar la comprobación biométrica que se ha definido.

- Clases para definir las políticas de autenticación de la organización: El administrador de seguridad de la organización va a poder ofrecer distintos niveles de seguridad, decidiendo los tipos de autenticaciones biométricas que ha de pasar el usuario según el perfil que tenga, el tipo de acción que desee ejecutar, la clase del objeto sobre el que va a realizar la acción y el contexto en que se encuentre el sistema.

- PolíticaAutenticacion: Cada instancia de esta clase será un política de autenticación de alto nivel que incluirá la autenticación biométrica que han de pasar todos los sujetos de un Rol para poder ejecutar las acciones de una Actividad sobre los objetos de una Vista en cierto Contexto.
- SolicitudAutenticacion: Esta clase es la equivalente a la clase Permiso para esta fase. En ella se incluyen las solicitudes de autenticación concretas que ha de pasar un Sujeto para poder realizar una Acción sobre un objeto. Las instancias de esta clase serán inferidas por el sistema.

El razonamiento en esta fase es similar a la anterior, ya que el razonador ha de traducir las políticas de autenticación representadas en alto nivel (Rol, Actividad, Vista) a solicitudes de autenticación de nivel concreto (Sujeto, Acción, Objeto) según las distintas entradas del sistema, la descripción de la organización y las políticas de alto nivel establecidas.

Tras esta fase, al usuario se le exigirá pasar las autenticaciones biométricas para demostrar su identidad, según los resultados de la inferencia. El sistema ha de tener un módulo que sea capaz de traducir las autenticaciones exigidas a ordenes concretas sobre equipos concretos donde ha de pasar dichas autenticaciones (lectores de huella, cámaras…). En caso de que el usuario no pase alguna de las autenticaciones en las distintas técnicas biométricas, el sistema le rechazará.

6. Comprobación biométrica de capacidades físicas y psíquicas

Llegados a este punto, el sistema ha identificado al usuario, sabe que tiene permiso para realizar la acción que solicita y ha verificado que el usuario es quien dice ser. Esta última fase va a decidir qué pruebas biométricas ha de pasar el usuario autenticado para comprobar que tiene las capacidades físicas y psíquicas necesarias para realizar la acción requerida. (grado de estrés, cansancio, miedo, ansiedad…) En la actualidad existen muchas líneas de investigación trabajando en la detección de estas características, [3], [4], y más que aparecerán en años sucesivos; con esta arquitectura, se pueden integrar todas ellas en un sistema real.

En esta fase, la inferencia tiene un esquema similar que en las fases anteriores, tal y como se observa en el esquema de la Figura 3:

Para este razonamiento, es necesario añadir en la ontología que se está describiendo las clases necesarias para la definición de las comprobaciones biométricas que tiene instaladas la organización y para definir las políticas de seguridad que van a seguir:

- Clases para la representación de comprobaciones biométricas. De igual manera que en la sección anterior, se propone utilizar la propuesta de Wayman para la definición de métodos biométricos, en este caso, aplicados a técnicas de comprobaciones físicas o psíquicas.

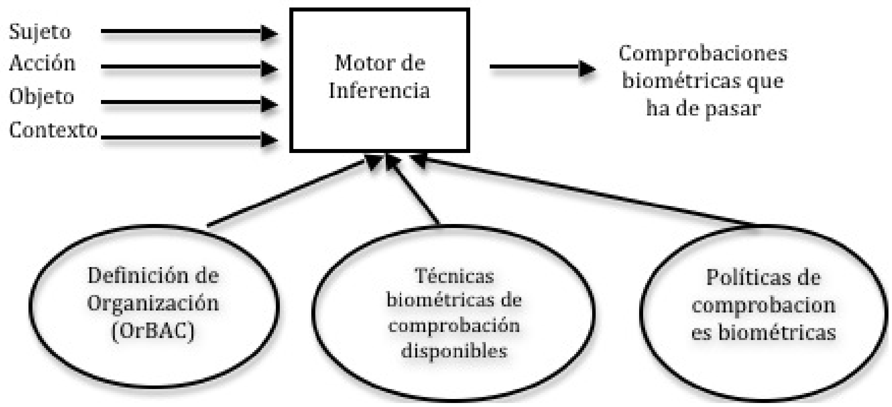

Figura 3. Razonamiento en la fase de comprobación de capacidades

- ComprobaciónBiométrica: Esta clase contiene las propiedades comprobacion_pattern, comprobacion_structure, comprobacion_extraction, comprobacion_qualityControl y comprobacion_recognition para relacionar cada una de las propiedades de la propuesta de Wayman de definición de métodos biométricos con las técnicas biométricas implementadas en la organización para la comprobación de estados físicos y psíquicos. En esta clase, es necesario incluir también la propiedad comprobación_id para relacionar la técnica biométrica con el dispositivo físico concreto de la organización que va a llevar a cabo la medida biométrica y la comprobación de la característica biométrica correspondiente.

- Clases para definir las políticas de la organización de comprobaciones de aptitudes de acceso: El administrador de seguridad de la organización va a poder definir las pruebas que ha de pasar cada usuario para estar seguros de la capacidad del mismo para poder realizar una acción.
  - PoliticaComprobacion: Las instancias de esta clase son políticas de alto nivel definidas por el administrador de seguridad que especifican las comprobaciones biométricas físicas y psíquicas que han de realizar todos los sujetos de un Rol para poder realizar las acciones incluidas en una Actividad sobre todos los objetos que pertenecen a una vista en un Contexto.
  - SolicitudComprobacion: Esta clase se corresponde a la clase Permiso en esta fase. Se incluyen las solicitudes de comprobaciones de características concretas que ha de pasar el sujeto que accede al sistema. Estas instancias serán inferidas por el motor de razonamiento según las Políticas de comprobación definidas. En esta clase se incluye la propiedad solicitudComprobacion_umbral, que marca el porcentaje máximo que puede tener una persona de una características física o psíquica para tener acceso al sistema (Por ejemplo, un 75 % de estrés).

En esta fase el razonamiento consiste en traducir las políticas de comprobación de alto nivel (Rol, Actividad, Vista) a las solicitudes de comprobación de bajo nivel del Sujeto, Acción y Objeto entradas del sistema.

Como resultado de esta fase, al usuario se le exigirá realizar unas comprobaciones específicas para demostrar que se encuentra en el estado físico y psíquico imprescindible para realizar la acción que quiere sobre el objeto deseado. Nuevamente, el sistema ha de tener un módulo para traducir las solicitudes de comprobaciones exigidas a órdenes concretas sobre equipos concretos donde se van a llevar a cabo las comprobaciones biométricas. Si el usuario sobrepasa el valor umbral de una de las características biométricas, el sistema no le permitirá el acceso.

7. Conclusiones

En este artículo se ha presentado una propuesta de arquitectura para el control de acceso integrando un esquema típico basado en OrBAC con las posibles tecnologías biométricas de autenticación y comprobación de estados físicos y psíquicos para poder tener acceso a la ejecución de una acción.

Gracias a este modelo, una organización puede aumentar sus niveles de seguridad manteniendo sus políticas de seguridad y ampliándolas a políticas de autenticación y comprobación de estado.

Al ser una arquitectura general, se puede integrar fácilmente cualquier tipo de tecnología biométrica que exista o vaya apareciendo; siendo esta arquitectura fácilmente escalable y actualizable según se vayan instalando nuevos dispositivos para realizar las autenticaciones y comprobaciones biométricas necesarios.

Este modelo permite autenticar o comprobar las características de un mismo usuario mediante distintas técnicas, dando un enfoque de multimodalidad biométrica al sistema.

Para controlar las distintas fases de la arquitectura se ha utilizado una ontología, para que mediante un motor de razonamiento se infieran automáticamente las solicitudes concretas de autenticación y comprobación biométrica que un usuario ha de pasar en base a las políticas de seguridad definidas en la organización.

Esta arquitectura puede tener una gran aplicación en entornos de alta seguridad, donde para realizar una acción o acceder a un lugar es necesario tener permiso, tener la seguridad de que el que accede es quien dice ser y que esté en plenas facultades físicas y psíquicas. Puede aplicarse en entornos militares, de control de acceso en aeropuertos, hospitales, centrales nucleares..

Referencias

1. A. K. Jain, A. Ross and S. Pankanti, “Biometrics: A Tool for Information Security”, IEEE Transactions on Information Forensics and Security Vol. 1, No. 2, pp. 125-143, June 2006.

2. S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric Recognition: Security and Privacy Concerns”, IEEE Security & Privacy Magazine, Vol. 1, No. 2, pp. 33-42, March-April 2003.
3. Barreto, A., Zhai, J., Adjouadi, M., “Non-intrusive Physiological Monitoring for Automated Stress Detection in Human-Computer Interaction”, LNCS 4796, pp 29-38, Springer-Verlag Berlin Heidelberg 2007
4. Healey, J. A., Picard, R. W., “Detecting Stress During Real-World Driving Tasks Using Physiological Sensors”, IEEE Transaction on Intellignet Transportation Systems, Vol. 6, No. 2, Junio 2005.
5. A. Ross and A. K. Jain, “Multimodal Biometrics: An Overview”, Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.
6. A. K. Jain and A. Ross, “Multibiometric Systems”, Communications of the ACM, Special Issue on Multimodal Interfaces , Vol. 47, No. 1, pp. 34-40, January 2004.
7. A. Ross, A. K. Jain, and Jian Zhong Qian, “Information Fusion in Biometrics”, Proc. 3rd International Conference on Audio- and Video-Based Person Authentication (AVBPA),, pp. 354-359, Sweden, June 6-8, 2001.
8. A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel and G. Trouessin. “Organization Based Access Control”. IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Lake Come, Italy, June 4-6, 2003.
9. F. Cuppens, N. Cuppens-Boulahia, T. Sans and A. Miège. “A formal approach to specify and deploy a network security policy”.Second Workshop on Formal Aspects in Security and Trust (FAST). Toulouse, France. August, 2004.
10. F. Cuppens and A. Miège. “Modelling contexts in the Or-BAC model”. 19th Annual Computer Security Applications Conference, Las Vegas, December 2003.
11. J. Wayman, A. K. Jain, D. Maltoni, and D. Maio, “Biometric Systems: Technology, Design and Performance Evaluation”,Springer Verlag, 2005.
12. R.-L. Hsu, “Face Detection and Modeling for Recognition”, Ph.D. Thesis, 2002.
13. S. C. Dass and A. K. Jain, “Fingerprint-Based Recognition”, Technometrics, vol. 49, no. 3, pp. 262-276, 2007.
14. Wildes, R.P., “Iris recognition: an emerging biometric technology,”Proceedings of the IEEE , vol.85, no.9, pp.1348-1363, Sep 1997
15. Arun Ross.“A Prototype Hand Geometry-based Verification System”, M.S. Project Report, 1999.