ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería Eléctrica y Computación

"IMPLEMENTACIÓN DE UN SISTEMA BIOMÉTRICO DE AUTENTICACIÓN"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del Grado de:

INGENIERO EN COMPUTACIÓN ESPECIALIZACIÓN SISTEMAS TECNOLÓGICOS

Presentado por:

WILSON EINSTEIN POZO CARRERA

CRISTIAN MANUEL MEDINA AGUIRRE

Guayaquil – Ecuador

2015

AGRADECIMIENTO

Agradecemos a Dios por su amor y por estar junto a nosotros en todo momento. A nuestros padres por ser los pilares más importante en nuestras vidas. Al ingeniero Carlos Jordán Villamar por su apoyo permanente para la implementación y culminación de este trabajo.

DEDICATORIA

A nuestros padres, familiares,

seres queridos y amigos.

TRIBUNAL DE SUSTENTACIÓN

MSc. Ing. Carlos Jordán

EVALUADOR

MSc. Ing. Marisol Villacrés

EVALUADOR

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este Informe nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

_____

WILSON EINSTEIN POZO CARRERA

_____

CRISTIAN MANUEL MEDINA AGUIRRE

RESUMEN

El presente trabajo consiste en demostrar la utilidad de los sistemas ANFIS para autenticar un usuario utilizando métodos biométricos, apoyándonos del software MATLAB 5.3 y el desarrollo de una interfaz de fácil manejo que permita comparar los patrones de tecleo del usuario que vamos a identificar como un impostor o no. Con esta finalidad se han desarrollado cinco capítulos los mismos que serán descritos a continuación.

El Capítulo 1 presenta el problema que existe al autenticar un persona, aborda los aspectos teóricos de lógica difusa y la biometría y se expone como se las ha usado para resolver el problema que se plantea utilizando sistemas neurodifusos. Debido a la gran extensión de la teoría de la lógica difusa, los tópicos aquí tratados se limitan a los conceptos y definiciones necesarios para entender el funcionamiento de un sistema de inferencias difuso del tipo Sugeno, en el cual se basa la arquitectura ANFIS propuesta en MATLAB. Finalmente se expone a Bio-Key como una solución integral al problema planteado, presentando sus objetivos principales, la estrategia de solución, así como sus alcances y limitaciones

La arquitectura del sistema a implementar se describe en el Capítulo 2, en donde se detallan los módulos requeridos para la captura de patrones, la identificación y la administración del software a implementar, así como sus entradas y salida.

En el Capítulo 3 se presenta la descripción de los pasos seguidos para el entrenamiento de los patrones de tecleo y la generación del FIS utilizando el Editor ANFIS de MATLAB 5.3.

El desarrollo del software es descrito en el Capítulo 4, así como el funcionamiento de comparador del sistema utilizando un controlador normal y el FIS obtenido a partir del Editor ANFIS.

Como quinto capítulo se presentan el estudio realizado a partir de las pruebas y sus resultados para finalizar con las conclusiones y recomendaciones que se ha llegado después del desarrollo del presente trabajo.

Es necesario indicar que no se presenta el código fuente del programa desarrollado debido a su extensión.

ÍNDICE GENERAL

ABREVIATURAS

TSK:	Sistema de inferencia difuso Takagi-Sugeno-Kang
ANFIS:	Adaptive Neuro Fuzzy Inference System: Sistema de inferencia difuso basado en redes de adaptación
J2EE:	Java Platform Enterprise Edition:Plataforma de Java Edición Empresarial
PL/SQL	Procedural Language/StructuredQuery Language: Lenguaje de Programación/ Lenguaje de Consultas estructurado para Oracle.
UML:	Unified Modeling Language: Lenguaje unificado de Modelado
EAO:	Entity Access Object
FAR:	False Acceptance Rate: Tasa de Falsa aceptación
FRR:	False Rejectión Rate: Tasa de Falso Rechazo
GENFIS	Generate Fuzzy Inference System: Generador de Sistema de Inferencia Difuso.
FIEC:	Facultad de Ingeniería Eléctrica y Computación

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad la seguridad informática juega un papel muy importante a nivel empresarial y personal. El robo de información confidencial que se almacenan en dispositivos, equipos, sistemas de información, etc. puede ocasionar perjuicios económicos y dañar la reputación a personas como a grandes corporaciones. Al imaginar esta situación, reflexionamos en lo valiosa que es la información y las medidas de seguridad que se deben tomarse en cuenta para que únicamente las personas autorizadas tengan acceso a ella.

El modo tradicional de acceso a los sistemas informáticos, servicios de red o dispositivos es ingresando un usuario y una contraseña. El propósito de la contraseña es verificar que el usuario es quien dice ser, es decir la contraseña actúa como un mecanismo que autentica al usuario [1]. Sin embargo este tipo de autenticación es frágil cuando existe un usuario que no toma las medidas adecuadas para mantener en secreto su contraseña y aún más si la clave que escogió es fácil de descifrar o adivinar.

El propósito del presente trabajo de investigación es proponer un método innovador de autenticación utilizando biometría de la dinámica de tecleo y sistemas adaptivos de inferencia neuro-difuso (ANFIS), ya que de las

investigaciones realizadas de trabajos previos, esta solución no ha sido implementada en un sistema de autenticación.

La principal ventaja de la solución propuesta es que la dinámica de tecleo no es un método invasivo y se puede implementar a un costo muy bajo ya que no requiere hardware especial para el análisis biométrico.

CAPÍTULO 1.

1. ACERCA DEL PROBLEMA DE AUTENTICAR UNA PERSONA AL ACCESAR A UN SISTEMA INFORMÁTICO

1.1. El Problema de Autenticar una Persona al Accesar a un Sistema Informático.

La forma tradicional de accesar a los sistemas informáticos, ha sido mediante la solicitud del ingreso de un usuario y una contraseña que se asume la conoce únicamente el usuario pertinente, con la intención de verificar que el usuario que ingresa es quien dice ser, es decir la contraseña se encarga de actuar como el método de autenticación del usuario.

Sin embargo, este método de autenticación tiene varios inconvenientes que mencionamos a continuación:

Los usuarios adoptan como contraseñas combinaciones de caracteres demasiado obvios como su nombre, iniciales, fecha de nacimiento, etc., los

cuales pueden ser develados fácilmente. Un usuario podría ver lo que teclea otro usuario al momento de autentificarse con su contraseña, o mediante programas invasivos ejecutados en memoria se podría grabar lo que usuario teclea y así obtener su contraseña. Por lo expuesto anteriormente, vemos que la contraseña no es suficiente para autenticar al usuario de un sistema de forma segura sino que requiere de algún mecanismo adicional que garantice el control de acceso.

La Biometría de la persona ofrece rasgos característicos que al combinarse con el empleo de contraseñas para ingreso de Sistemas bien podrían suplir los inconvenientes mencionados y así permitir el acceso exclusivo de usuarios autorizados.

1.2. Biometría.

La palabra biometría tiene su origen etimológico en el griego “bio” que significa vida y “metría” que significa medida [18], lo cual se podría interpretar como medida de la vida, en la actualidad se define como la disciplina que permite identificar a las personas basándose en características fisiológicas o de comportamiento.

Las características fisiológicas son aquellas que al estudiarlas nos permiten identificar rasgos en la anatomía física del ser humano, mientras que las de comportamiento se encargan del estudio de rasgos conductuales o de comportamiento de un individuo.

1.2.1. Tipos de Biometría.

Existen dos tipos de biometría:

La biometría Estática: Se basa en las características físicas del ser humano [2], como pueden ser huellas digitales, geometría de la mano, análisis del iris, venas del dorso de la mano o reconocimiento facial

La biometría dinámica: Estudia las características de la conducta del ser humano basados en el proceso de identificación de rasgos derivados de una acción realizada [2], entre los cuales tenemos la firma manuscrita, la dinámica del tecleo, la cadencia del paso, el patrón de voz.

1.2.2. Sistemas Biométricos.

Los sistemas biométricos son aquellos que automatizan las tareas de reconocimiento y verificación utilizando técnicas biométricas.

1.2.2.1. Modelo del Proceso de Identificación Personal.

Para identificar una persona, podemos hacer uso de cualquiera de estos tres indicadores que definen el proceso de identificación [3]:

Conocimiento: la persona tiene conocimiento (por ejemplo: un código),

Posesión: la persona posee un objeto (por ejemplo: una tarjeta),

Característica: la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares).

Cada uno de los indicadores anteriores genera una estrategia básica para el proceso de identificación personal. Además pueden ser combinados con el objeto de alcanzar grados de seguridad más elevados y brindar, de esta forma, diferentes niveles de protección.

1.2.2.2. Características de un Identificador Biométrico.

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera sea el indicador, debe cumplir los siguientes requerimientos [4]:

Universalidad: cualquier persona posee esa característica;

Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña;

Permanencia: la característica no cambia en el tiempo;

Cuantificación: la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como indicador biométrico.

1.2.2.3. Arquitectura de un Sistema Biométrico de Identificación Personal.

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona. El segundo maneja la compresión, procesamiento,

almacenamiento y comparación de los datos adquiridos con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema. La arquitectura típica de un sistema biométrico se presenta en la figura 1.1 Esta puede entenderse conceptualmente como dos módulos:

- Módulo de inscripción
- Módulo de identificación

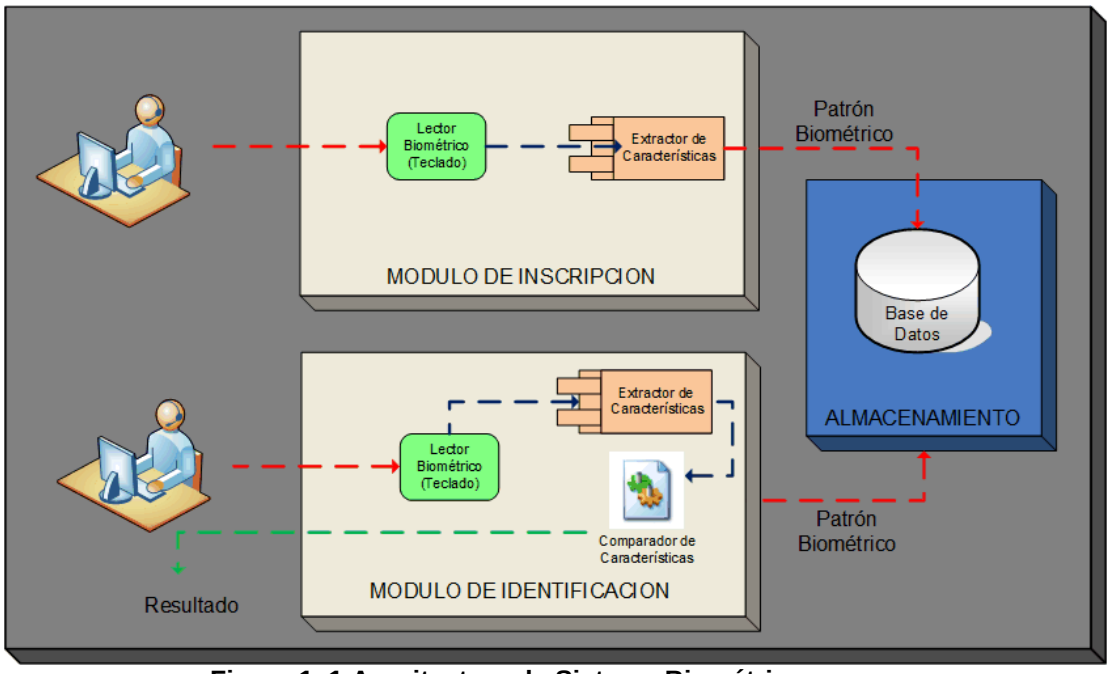

Figura 1. 1 Arquitectura de Sistema Biométrico

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, que será almacenado en una base de datos central u otro medio, recibirá el nombre de patrón biométrico. En otras palabras el patrón biométrico es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico.

El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo en una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato del patrón biométrico. La representación resultante se denomina muestra biométrica y es enviada al comparador de características que confronta a éste con uno o varios patrones biométricos para establecer la identidad.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de fase de inscripción, mientras que los procesos realizados por el mòdulo de identificación reciben la denominación de fase operacional. A continuación se entregan detalles de esta última.

Un sistema biométrico en su fase operacional puede operar en dos modos:

Modo de verificación, o

Modo de identificación

Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con los patrones biométricos del individuo. Por ejemplo, si una persona ingresa su nombre de usuario entonces no será necesario revisar toda la base de datos buscando el patrón biométrico que más se asemeje al de él, sino que bastará con comparar la información de entrada sólo con el patrón biométrico que está asociado al usuario. Esto conduce a una comparación uno-a-uno para determinar si la identidad reclamada por el individuo es verdadera o no. De manera más sencilla el modo de verificación responde a la pregunta: ¿eres tú quién dices ser?.

Un sistema biométrico operando en el modo de identificación descubre a un individuo mediante una búsqueda exhaustiva en la base de base de datos con los patrones biométricos. Esto conduce a una comparación del tipo uno-a-muchos para establecer la identidad del individuo. En términos sencillos el sistema responde la pregunta: ¿quién eres tú?.

Generalmente es más difícil diseñar un sistema de identificación que uno de verificación. En ambos casos es importante la exactitud de la respuesta. Sin embargo, para un sistema de identificación la rapidez también es un factor crítico. Un sistema de identificación necesita explorar toda la base de datos donde se almacenan los patrones biométricos, a diferencia de un sistema verificador.

1.2.2.4. Exactitud en la Identificación.

Para identificar a una persona el Sistema Biométrico debe decidir si acepta o no a la persona que se va a autenticar, esta identificación debe tener un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue “personal autorizado” o “impostor”. Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

a. Una persona autorizada es aceptada,
b. Una persona autorizada es rechazada,
c. Un impostor es rechazado,
d. Un impostor es aceptado.

Las salidas números a y c son correctas, mientras que las números b y d no lo son.

1.2.2.5. Sistemas Biométricos Actuales.

En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características. A continuación enunciamos algunas de las técnicas biométricas:

- Rostro,
- Huellas dactilares,
- Geometría de la mano,
- Venas de las manos,

- Iris,
- Patrones de la retina,
- Voz,
- Firma.
- Dinámica de Tecleo

Cada una de las técnicas anteriores posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir que técnica utilizar para una aplicación específica. En particular deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento. Una huella dactilar, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales. Tambièn las màquinas que miden características físicas tienden a ser màs grandes y costosas que las que detectan comportamientos. Debido a diferencias como las señaladas, no existe un único sistema biométrico que sea capaz de satisfacer todas las necesidades. Una compañía puede incluso decidir el uso de distintas técnicas en distintos ámbitos. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la identificación.

1.3. Dinámica de Pulsación de Teclas

Los estudios de la dinámica de tecleo se remontas a los orígenes de la comunicación de larga distancia o telegráfica, en el año 1824 fue enviado por telégrafo el mensaje "What hath God wrought" U.S. Capitol en Washington, D.C. a el B&O Railroad en Baltimore, Maryland, ya en 1860 el telégrafo fue una revolución. Con la experiencia cada operador desarrolló una forma única de envío del mensaje, la cual permitía identificarlo por su ritmo de digitación.

Más tarde en 1940 cuando se desarrollaba la Segunda Guerra Mundial, los mensajes se trasmitían por código morse, usando la metodología “El puño del Enviador”, con la cual la Inteligencia Militar identificaba a una persona por la forma única de teclear un mensaje (dots-dashes), creando un ritmo que ayudaba a distinguir a los aliados de los enemigos. Basándose en esta metodología, en 1980 la Nacional Science Foundation y la Nacional Bureau Starndards conducen un estudio en los Estados Unidos en el cual establecen que la dinámica de tecleo tiene características únicas que pueden ser identificadas [4].

1.3.1. Reconocimiento Biométrico de Usuarios por Dinámica de Pulsación de Teclas.

La dinámica de tecleo es una característica biométrica que permite identificar a una persona por la velocidad mecanográfica o ritmo y la forma de

comportarse delante del teclado, a partir de estas características se genera un patrón único de digitación el cual se basa en latencia, tiempo de presión de teclas, correlación, etc.

Los principales métodos para la autenticación de personas a través de su dinámica de tecleo utilizan herramientas de lógica difusa, redes neuronales, técnicas estadísticas o combinan el empleo de alguna de las herramientas descritas [6]. Por ejemplo en la tarea de clasificación se han utilizado algoritmos de Bayes, redes neuronales; las cuales dan excelentes resultados pero necesitan ser entrenadas, últimamente se han realizado estudios utilizando un clasificador difuso [7].

En la actualidad los sistemas de autenticación biométrica, utilizan tecnologías modernas y eficaces para identificar un usuario en un sistema informático, pero los sistemas que se ofrecen en el mercado tienen un costo elevado debido a que su implementación requiere infraestructura de Hardware y Software, muchas de las implementaciones con dispositivos ópticos necesitan demasiado cuidado en el uso y los costos de mantenimiento son elevados (scanner de mano, huellas digitales), otros en cambio presentan resistividad de parte de los usuarios por el malestar visual que provocan (reconocimiento de iris y retina).

Debido a las desventajas mencionadas en el párrafo anterior y al escaso desarrollo en la última década de herramientas informáticas biométricas utilizando dinámica de tecleo se ideó BioKey, el cual es un producto que ofrece una alternativa de solución para autenticar usuarios. Bio-Key es una

solución atractiva ya que su implementación es de bajo costo debido a que no requiere dispositivos adicionales de Hardware, solo necesita el software y el teclado para poner en marcha una solución utilizando esta técnica biométrica, la misma que es implementada con un método basado en la inteligencia artificial ofreciendo una solución que se aproxima más a la realidad.

1.3.2. Introducción a Sistemas Expertos – Lógica Difusa.

La lógica difusa es una lógica alternativa a la lógica clásica que pretende introducir un grado de vaguedad en las cosas que evalúa. En la actualidad el ser humano utiliza esta lógica para representar el conocimiento que es ambiguo e impreciso.

La Lógica difusa se inició en 1965 con Lotfi A. Zadeh, profesor de la universidad de California en Berkeley. Se originó como herramienta para solucionar problemas en sistemas industriales complejos, posteriormente fue utilizada en electrónica de entretenimiento y hogar, sistemas de diagnóstico y otros sistemas expertos[7].

La lógica difusa es útil en procesos complejos, cuando no existe un modelo de solución simple o un modelo matemático preciso, cuando se necesita usar el conocimiento de un experto que utiliza razonamiento inexacto.

Actualmente la lógica difusa es utiliza en un sin número de aplicaciones de nuestra vida cotidiana, tales como control de tráfico, control de compuertas hidroeléctricas, centrales térmica, control en máquinas lavadoras,

ascensores, metros, reconocimiento de patrones, este último es el que utilizaremos en el presente trabajo.

1.3.2.1. Conjuntos Difusos

Debido a que existen conceptos que no tienen límite claro, surge la necesidad de trabajar con conjuntos difusos. Un conjunto difuso se encuentra asociado por un valor lingüístico que está definido por una palabra lingüística o adjetivo. La teoría de conjuntos difusos contempla la pertenencia parcial de un elemento a un conjunto, es decir, cada elemento presenta un grado de pertenencia a un conjunto difuso que puede tomar cualquier valor entre 0 y 1. Este grado de pertenencia se define mediante la función característica asociada al conjunto difuso, para cada valor que pueda tomar un elemento o variable de entrada x, la función característica μA(x) proporciona el grado de pertenencia de este valor de x al conjunto difuso A. Un conjunto difuso en el universo de discurso puede definirse como lo muestra la ecuación 1.1

$$A= \{(x, \mu_A(x))| \ x \in U\} \qquad 1.1$$

Donde μA (x) es la función de pertenencia de la variable x, y U es el universo en discurso. Cuando más cerca es la pertenencia del conjunto A al valor de 1, mayor será la pertenencia de la variable x al conjunto A, esto se puede ver en la figura 1.2

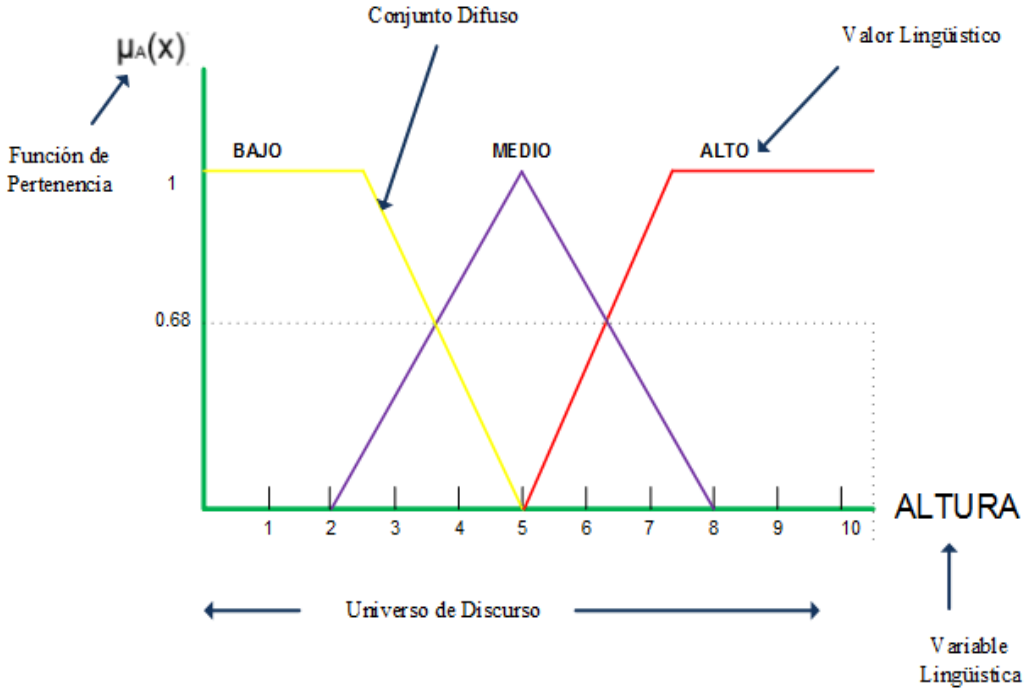

Figura 1. 2 Ejemplo de Conjunto Difuso

1.3.2.2. Funciones de Pertenencia

Aun cuando cualquier función puede ser válida para definir un conjunto difuso, existen ciertas funciones que son comúnmente utilizadas por su simplicidad matemática para representar conjuntos difusos, entre estas funciones se encuentran las del tipo triangular, mostrado en la figura 1.3, trapezoidal mostrado en la figura 1.4, gaussiana, etc.

$$\mu_A(x) = \begin{cases} 0 & \text{para } x \le a \\ \frac{x-a}{m-a} & \text{para } a < x \le m \\ \frac{b-x}{b-m} & \text{para } m < x \le b \\ 0 & \text{para } x > b \end{cases}$$

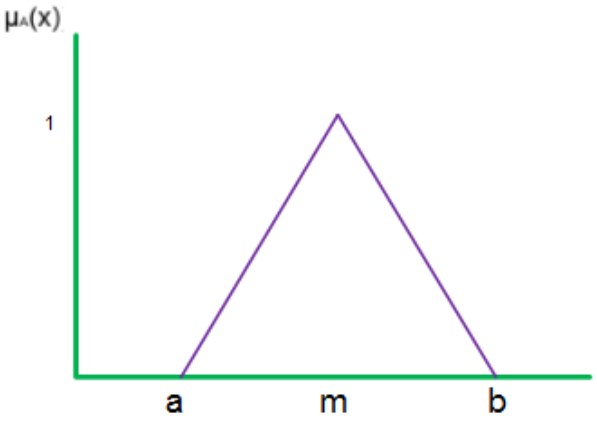

Figura 1. 3 Ejemplo de Función Triangular

$$\mu_A(x) = \begin{cases} 0 & \text{para } x \le a \\ \frac{x-a}{b-a} & \text{para } a < x \le b \\ 1 & \text{para } b < x \le c \\ \frac{d-x}{b-c} & \text{para } c < x \le d \\ 0 & \text{para } x > d \end{cases}$$

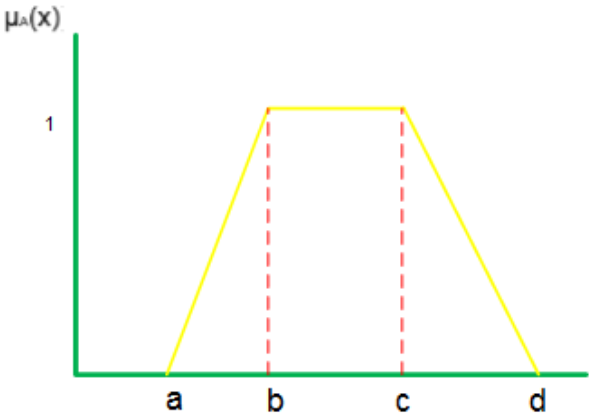

Figura 1. 4 Ejemplo de Función Trapezoidal

1.3.2.3. Sistemas de Inferencias Difuso

Este sistema ha recibido diferentes nombres como: Sistema basado en reglas difusas, sistema experto difuso, modelo difuso, controlador lógico difuso o, simplemente, sistema difuso.

Su estructura básica consiste de cinco componentes (ver la figura 1.5), las cuales se indican a continuación:

• Una base de reglas, que contiene un cierto número de reglas difusas si ...entonces.

• Una base de datos, la cual define las funciones de membresía de los conjuntos difusos usados en las reglas difusas.

• Una unidad de toma de decisiones, la cual realiza la operación de inferencia sobre las reglas.

• Una interfaz de fusifícación, la cual trasforma la entrada clara a un grado de equivalencia con un valor lingüístico.

• Una interfaz de defusificación, la cual transforma e! resultado difuso de la inferencia a una salida clara.

Generalmente la base de reglas y la base de datos se conocen conjuntamente como base de conocimientos

El razonamiento difuso es la operación de inferir sobre las reglas difusas si ...entonces. Los pasos del razonamiento difuso realizados por un sistema de inferencia difuso son:

1. Compara las variables de entrada con las funciones de membresía en la parte del antecedente para obtener un valor de membresía (un valor de

compatibilidad) de cada etiqueta lingüística (este paso a menudo es llamado fusificación).

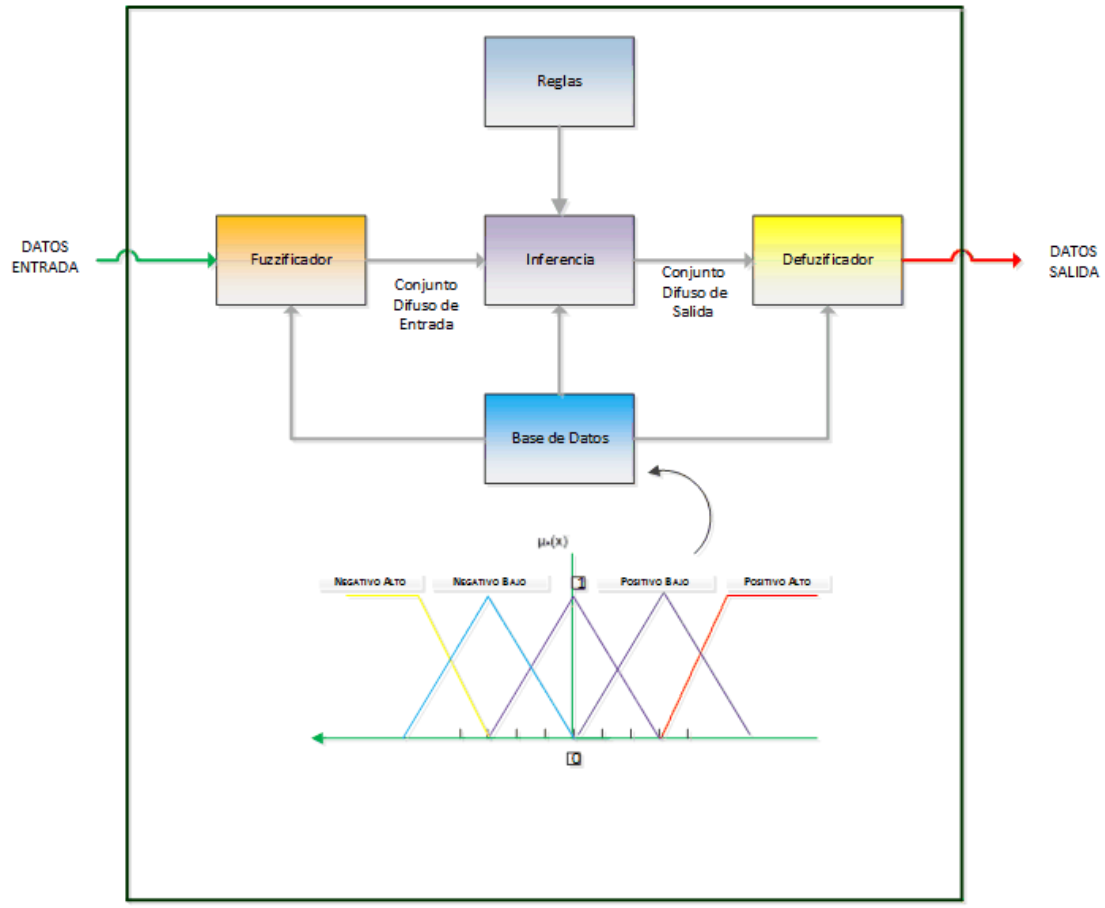

Figura 1. 5 Sistema de Inferencia Difuso

2. Combina (a través de un operador especifico como la norma - T) los valores de membresía de la parte del antecedente para obtener el soporte de cada regla .

3. Genera una salida del consecuente (difuso o clara) en cada regla dependiendo del soporte.

4. Agregación de todas las salidas de los consecuentes para obtener una salida numérica. Este paso es llamado defusificación.

Existen diferentes tipos de sistemas de inferencia difusos, los cuales se han utilizado en diversas aplicaciones. Las diferencias básicas pueden estar en los consecuentes de sus reglas difusas, así como en los métodos de defusificacion que emplean. Los nombres que se les han dado normalmente se toman de las personas que primero los propusieron; así, por ejemplo, se tiene el sistema de inferencias difuso tipo Mamdani, el de tipo Takagi-Sugeno-Kang (TSK).

1.3.3. Sistema de Inferencia Difusa Basado en Redes Adaptativas (ANFIS)

La arquitectura que se propone para el desarrollo del presente trabajo, es un tipo de red adaptiva, la cual, funcionalmente, es equivalente a un sistema de inferencias difuso. Esta arquitectura puede representar tanto modelos difusos tipo Sugeno (Sugeno de orden 1 y 0).

Básicamente, ANFIS modela un sistema de inferencias difuso en el cual sus parámetros se ajustan mediante un algoritmo de retro propagación basándose en un conjunto de datos de entrada / salida (datos de entrenamiento), lo cual le permite al sistema aprender.

El enfoque de este trabajo es el estudio y manejo de los sistemas ANFIS que posee MATLAB 5.3 las cuales pueden operar con un sistema tipo Sugeno, de orden cero o de primer orden.

Debido a la mayor rapidez en el entrenamiento y a las mejores características que presentan los sistemas de primer orden sobre los de orden cero, son éstos con los que se desarrolla el presente trabajo. La siguiente descripción se centrará en ello, teniendo en cuenta que fácilmente se puede hacer una generalización hacia los otros tipos de sistemas, como el de orden cero.

Para explicar el funcionamiento de la arquitectura, se considera un sistema de inferencias con dos entradas (x, y) y una salida (z). Para un modelo difuso tipo Sugeno de primer orden, un conjunto con dos reglas difusas si... entonces, se define como:

Regla 1: Si x es Ai y y es 81, entonces zi = pi x + qi y + n,

Regla 2: Si x es /b y yes 82, entonces Z2= p2X + q2y + r2.

La figura 1.6 ilustra el mecanismo de razonamiento para un Sistema de Inferencia Difuso tipo Sugeno;

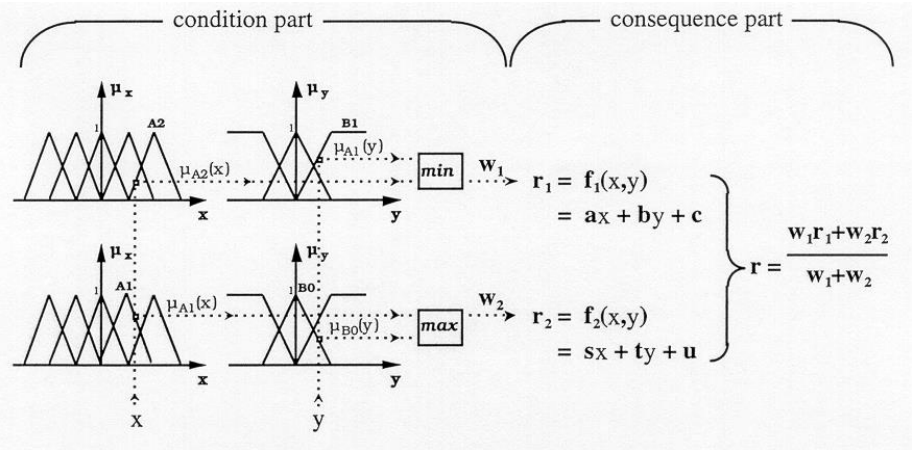

Figura 1. 6 Mecanismo de Inferencia Difuso Sugeno

La arquitectura ANFIS correspondiente se muestra en la figura 1.7, en la cual los nodos en una misma capa realizan funciones similares.

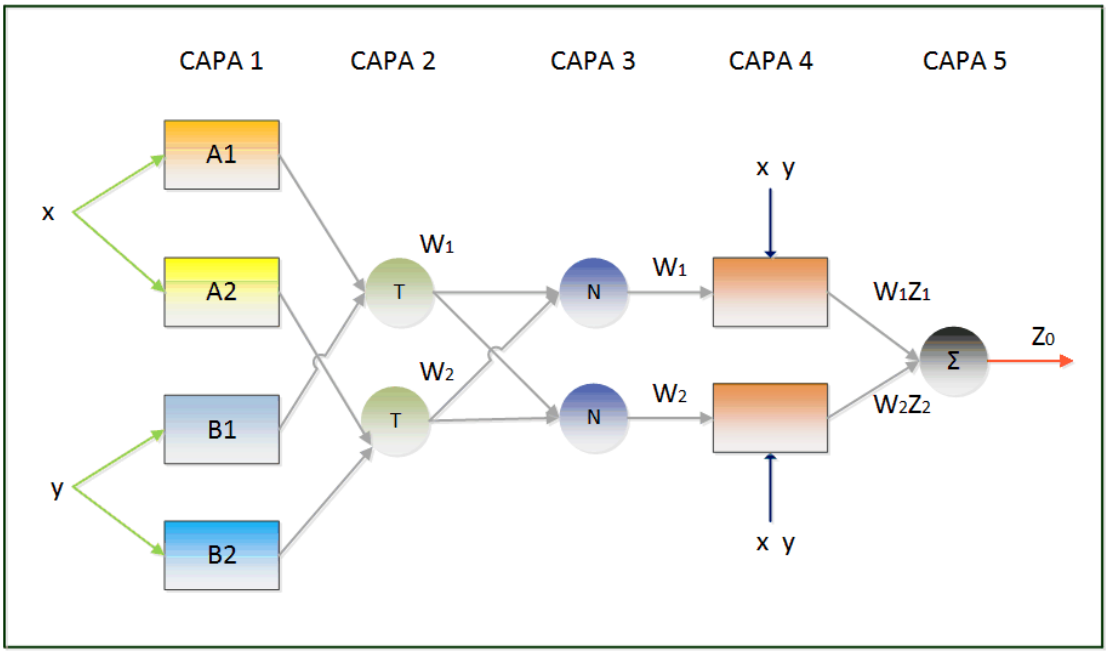

Figura 1. 7 Arquitectura ANFIS para Inferencia Takagi-Sugeno

1.4. Objetivos de BioKey.

El objetivo esencial consiste en ofrecer un componente informático para autenticar usuarios de manera segura, eficiente y a un bajo costo, adicionalmente se creará un sistema computacional para el monitoreo del proceso de autenticación.

Para alcanzar este objetivo, el producto desarrollado autentica una persona cuando ingresa al sistema informático. Por otra parte, para que el sistema pueda autenticar a un usuario, necesita de los datos característicos

biométricas del mismo, por lo cual es necesario proveer al usuario de una interfaz que le permita ingresar de una manera rápida y sencilla esta información.

Según lo expuesto en los párrafos anteriores se puede puntualizar los objetivos generales de BioKey:

- Autenticar a un usuario de manera segura.
- Proveer una herramienta para verificar como se realiza el proceso de autenticación.
- Desarrollar un Sistema de Administrativo para el monitoreo del proceso de autenticación
- Generar reportes para auditar los ingresos aceptados y rechazados.

1.5. Alcances y limitaciones de BioKey

Como presentamos en las secciones anteriores Bio-Key es un Sistema Biométrico de tipo dinámico que sirve autenticar usuarios. Las características de comportamiento dinámico en una persona cambian en ciertas circunstancias, lo que podría afectar la confiabilidad del sistema propuesto, como por ejemplo una persona podría estar contestando el teléfono mientras ingresa su información de autenticación, la persona podría tener una o sus dos manos lastimadas, el estado emocional de la persona podría influir cuando se ingresas la información. Debido a esto los sistemas biométricos de digitación se utilizan en conjunción con un mecanismo convencional de identificación usuario/contraseña.

CAPÍTULO 2.

2. DESCRIPCIÓN DEL SISTEMA

2.1. Metodología TECLEO-ANFIS de Reconocimiento de Usuarios por Dinámica de Pulsación de Teclas.

La Metodología ANFIS-BIOKEY realiza el Reconocimiento de Usuarios a través de su Dinámica de Pulsación de Teclas. El proceso de autenticación propuesto, está compuesto por tres etapas principales:

- Obtención de la muestra biométrica a través de mediciones de tiempos de dinámica del tecleo.
- Entrenamiento de red ANFIS para reconocimiento biométrico de tecleo.
- Autenticación del usuario.

La metodología descrita surge de la experiencia de mediciones de los tiempos de Dinámica de Pulsación.

2.1.1. Módulos del Sistema.

El sistema Bio-Key está conformado por tres módulos listados a continuación:

- Módulo de inscripción
- Módulo de identificación.
- Módulo de Administración

Estos tres módulos se pueden visualizar en la figura 2.1.

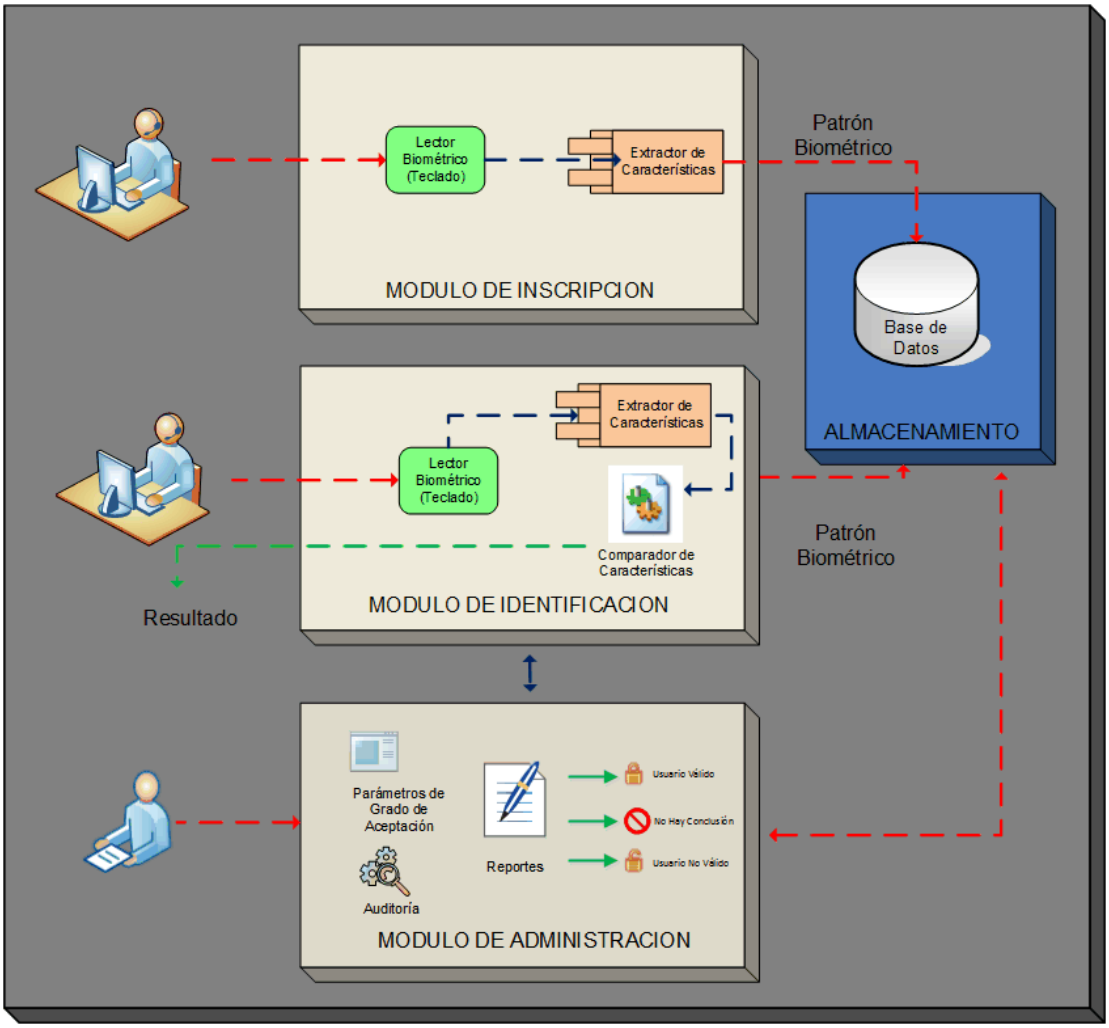

Figura 2. 1 Diagrama Modular de Bio-Key

2.1.1.1. Módulo de Inscripción.

En este módulo se inscribe al usuario, solicitándole el ingreso de Número identificación, Usuario, contraseña y correo electrónico. Una vez establecido un usuario/contraseña válidos, se solicita realizar un número de 20 pruebas de ingreso de clave para conformar muestras de los tiempos de digitación.

Las muestras serán utilizadas para el entrenamiento de la red ANFIS para que luego del aprendizaje se pueda utilizar como método de autenticación del usuario. En estudios realizados por otros autores en actividades de reconocimiento de tecleo se toman hasta 100 muestras [9], [10], [11] y se afirma que para obtener buenos resultados es necesario una cantidad de muestras mayor a treinta.

2.1.1.2. Módulo de Identificación.

En BioKey el módulo de identificación se utiliza para decidir si la persona que está ingresando al sistema informático es quien dice ser, para esto se genera la muestra biométrica con los tiempos de digitación de la contraseña del usuario, la generación de esta muestra se realiza de forma similar a la del patrón biométrico con la diferencia que solo se necesitará que la persona ingrese una sola vez su usuario y contraseña. Cuando Bio-Key tenga la muestra para autenticar, buscará el patrón biométrico del usuario y realizará la comparación de la muestra con el patrón biométrico, logrando así determinar si el usuario es quien dice ser o es un impostor.

2.1.1.3. Módulo de Administración.

Para efectos de auditoría se ha creado un módulo que tiene como finalidad obtener reportes de usuarios aceptados y rechazados, también se obtiene el grado de confiabilidad en cada uno los usuarios aceptados. De igual manera

contiene un módulo en el cual se ingresan los parámetros necesarios para poner en marcha a Bio-Key y analizar la autenticación en tiempo real.

2.1.2. Características funcionales y operacionales del Sistema

Siendo Bio-Key un sistema biométrico de autenticación, este se encarga de la verificación de un usuario, aceptarlo o rechazarlo. Cuando el usuario ingresa al sistema informático se capturan como entradas los tiempos característicos de dinámica de tecleo de la contraseña, estos tiempos son colectados en el módulo de inscripción y suministrados a la red ANFIS-BIOKEY la cual se entrena con tiempos característicos de dinámica de tecleo para identificación del usuario. Las variables de salida del sistema indicaran si el usuario que se autentica es un usuario válido o no. Las entradas y salidas de Bio-Key se pueden apreciar en forma gráfica en la Figura 2.2.

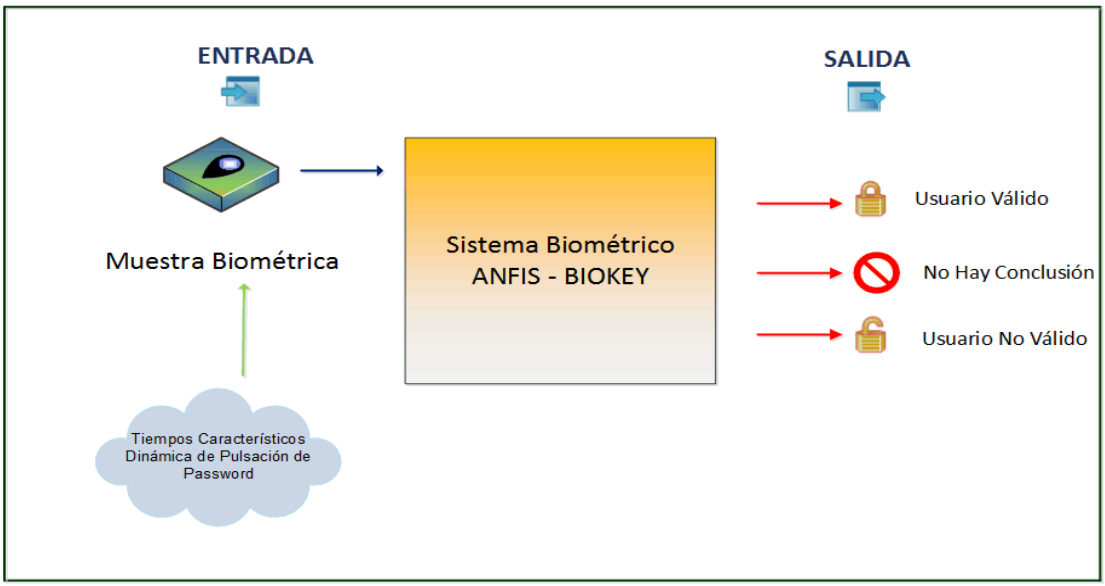

Figura 2. 2 Diagrama de Entradas y Salidas Bio-Key

2.2. Entradas del sistema

2.2.1. Extracción de las características de dinámica de pulsación de teclas.

Para extraer las características de dinámica de tecleo, convertimos en formato digital la forma en la cual una persona pulsa las teclas en un teclado, estas características son extraídas en tiempo real utilizando los datos adquiridos en el momento que los usuarios digitan su contraseña. La forma en la cual se extraen estas características es utilizando los tiempos de duración y latencia que existen entre la pulsación de teclas.

Tiempo de duración.- es el tiempo en el cual el usuario presiona y libera una tecla.

Tiempo de Latencia.- es el tiempo en el cual un usuario libera una tecla y presiona la siguiente.

2.3. Salidas del Sistema

2.3.1. Autenticación del Usuario.

Para realizar la autenticación del usuario se verifica si la muestra biométrica de tiempos característicos de dinámica de tecleo de la contraseña es reconocida por la red ANFIS-BIOKEY. El patrón biométrico almacenado en la base de datos es comparado con la muestra a autenticar. El acceso al

sistema se otorga cuando el patrón biométrico y la muestra biométrica reportan semejanza, caso contrario se niega el acceso.

CAPÍTULO 3.

3. DISEÑO DE BIOKEY

3.1. Visión Panorámica del Diseño

En la construcción de BIOKEY debemos considerar que las entidades y/o clases interaccionan entre ellas y no trabajar de forma aislada, ellas comparten métodos y atributos, lo cual evitan reescribir código y permite reutilizar los objetos existentes.

La jerarquía establecida entre clases es una característica propia de la Programación Orientada a Objetos que la diferencia de la Programación Procedimental, porque permite tanto extender como reutilizar código existente sin necesidad de reescribirlo.

BIOKEY, se presenta como un sistema de control. El usuario introduce su usuario y contraseña, esta última se controlará i/o validará a través de la dinámica de tecleo. Dicho tecleo se comparará con un patrón del usuario

para determinar si realmente es nuestro usuario o un impostor. Hay que tener en consideración que cuando hablamos de biometría siempre consideramos valores con umbrales de incertidumbre. Debido a esta incertidumbre el sistema permitirá realizar la configuración del umbral a partir del cual consideraremos que un usuario es impostor. Cuando mayor sea el umbral, mayor será la seguridad y cuando menor sea ese umbral, menor la seguridad.

3.2. Arquitectura del Sistema

El diseño Arquitectónico de BIOKEY está basado en un modelo web multicapa, conformado por capa de Presentación, Negocio y gestión de datos las cuales se muetran en el gráfico de la figura 3.1. Se seleccionó el patrón de diseño multicapa ya que este ofrece ventajas como encapsulación de la lógica del negocio, procesamiento distribuido, centralización del control y fácil mantenimiento.

Figura 3. 1 Diagrama de Arquitectura Multicapa

La Capa de Presentación es aquella donde se encuentra la interfaz web de entrenamiento y la de acceso, en ambas se solicita al usuario el ingreso del usuario y contraseña, se extrae el patrón de características biométrico y en el segundo caso se autentica al usuario; está capa se encuentra desarrollada en Java 2EE (1.6)/Web.

La Capa de Negocio encargada de recibir las peticiones del usuario, procesarlas y responder a las solicitudes de autenticación. Esta capa se comunica con la capa de presentación para recibir solicitudes y presentar resultados, y con la capa de datos para solicitar el almacenamiento o recuperación de datos. En BIO-KEY esta capa contiene el Subsistema que extrae las características del usuario, del que genera el patrón del usuario y del clasificador ANFIS, estos subsistemas están encapsulados en un componente Java denominado BioKey.jar generado, el cual se integra con el ToolBox ANFIS de MathLab.

La Capa de Datos es donde residen los datos de configuración y los patrones de características de los usuarios. Esta es la encargada de proporcionar la información a la capa de negocio para realizar las comparaciones e identificar a los usuarios. Esta capa está conformada por un gestor de Bases de Datos, y recibe de la capa de negocio, solicitudes para almacenar y recuperar información. El gestor de base de datos usado es Oracle 10g el cual utiliza lenguaje procedural PL/SQL.

A continuación en la Figura 3.2 se presenta el Diseño multicapa de BioKey.

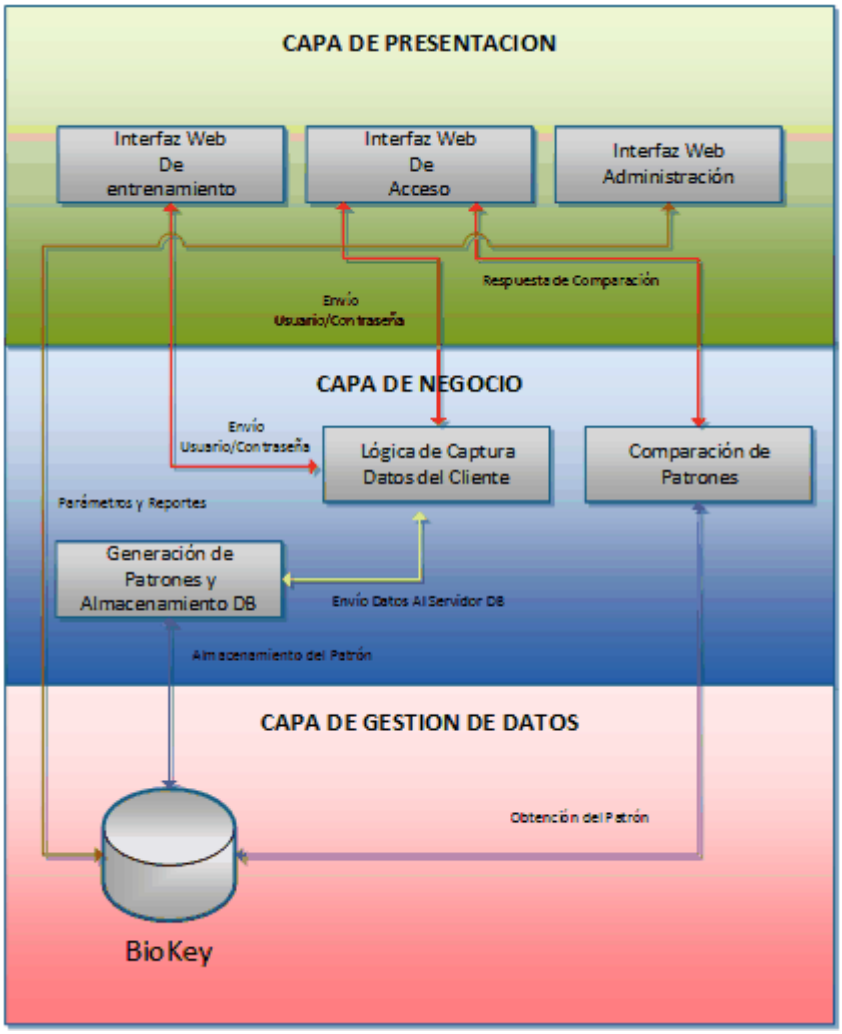

Figura 3. 2 Diagrama Multicapa de Bio-Key

3.2.1 Diseño Detallado

Bio-Key fue diseñado utilizando lenguajes orientado a objetos, es por ello que el modelado del diseño detallado se realizó utilizando notación UML, la cual se ha convertido en un estándar de facto en cuanto a notación orientada a objetos, ya que esta permite tener una visión completa y coherente del sistema que se va a desarrollar; los diagramas UML utilizados para el modelado son: Diagramas de casos de uso, Diagramas de secuencia y Diagramas de clase.

Los diagramas de casos de usos muestran la relación entre los actores y los casos de usos del sistema, representan la funcionalidad que ofrece el sistema en lo que se refiere a su interacción externa [15]. Los diferentes actores utilizados en los casos de usos son: usuario de inscripción, usuario a autenticar y usuario administrador. En la Figuras 3.3, 3.4 y 3.5 se presentan de forma gráfica los casos de uso utilizados en el sistema Bio-Key.

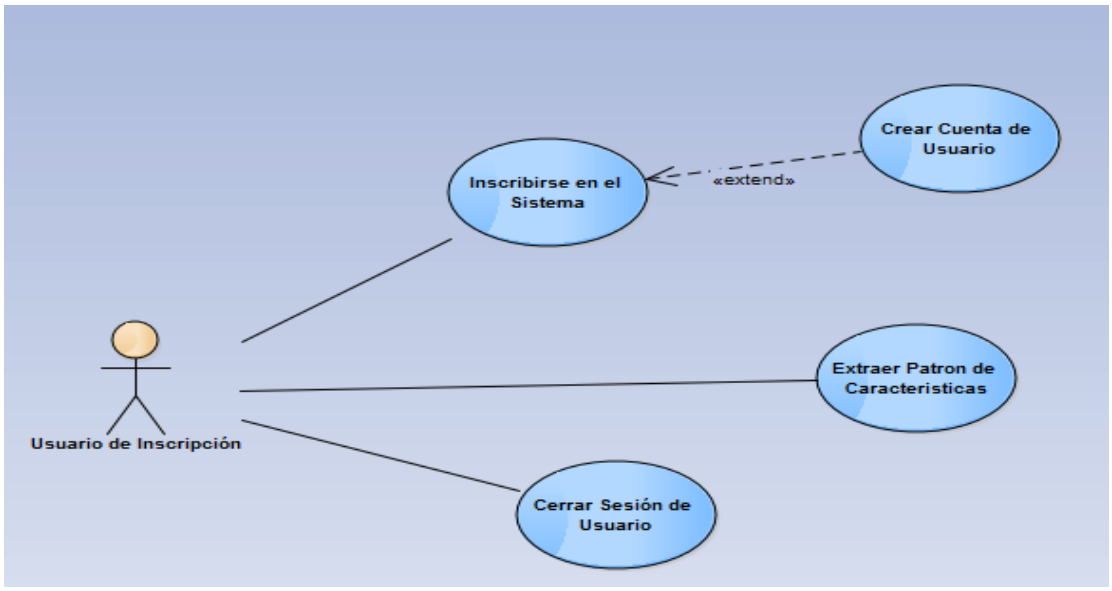

Figura 3. 3 Diagrama de Caso de Uso Inscripción de Usuario

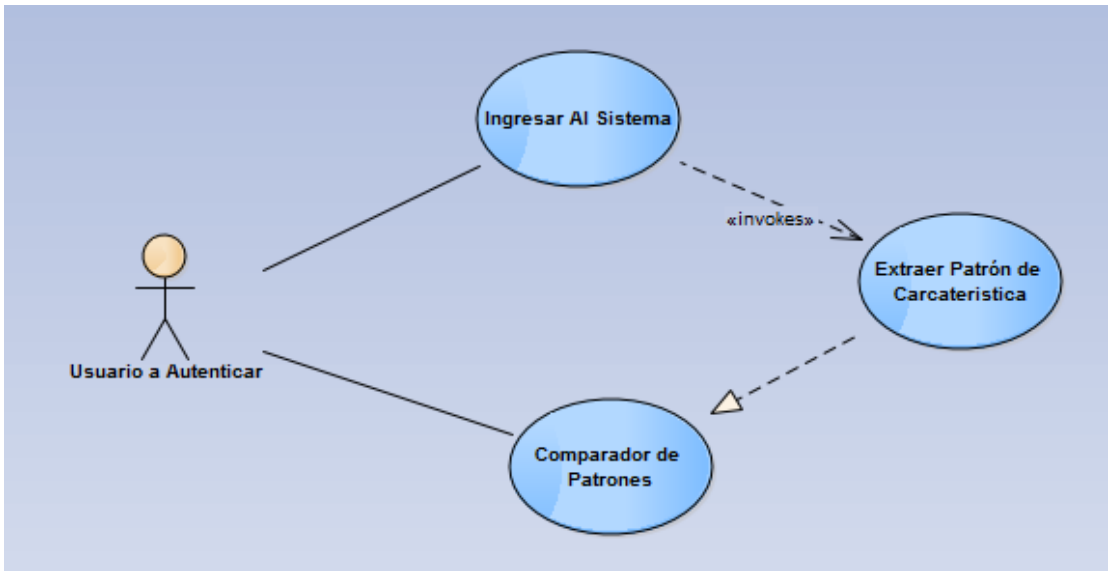

Figura 3. 4 Diagrama de Caso de Uso Autenticar Usuario

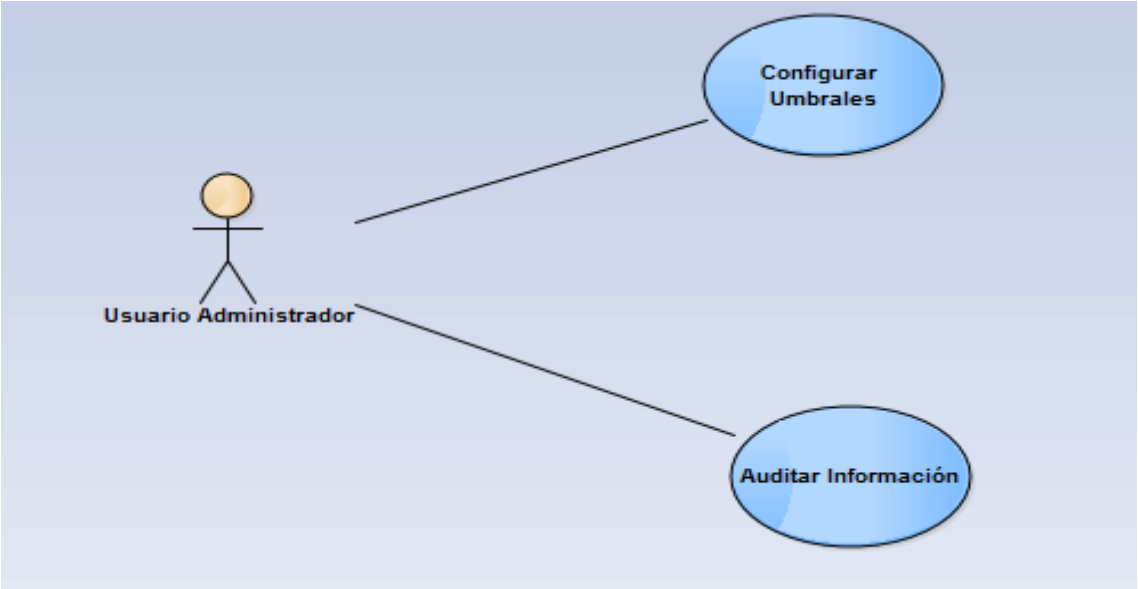

Figura 3. 5 Diagrama de Caso de Uso Administrar Información

A continuación se presentan los diagramas de clases utilizadas en Bio-Key de tal manera que el lector tenga un modelo conceptual de software que se va a implementar. Estos diagramas se muestran en las figuras 3.6, 3.7, 3.8 y 3.9.

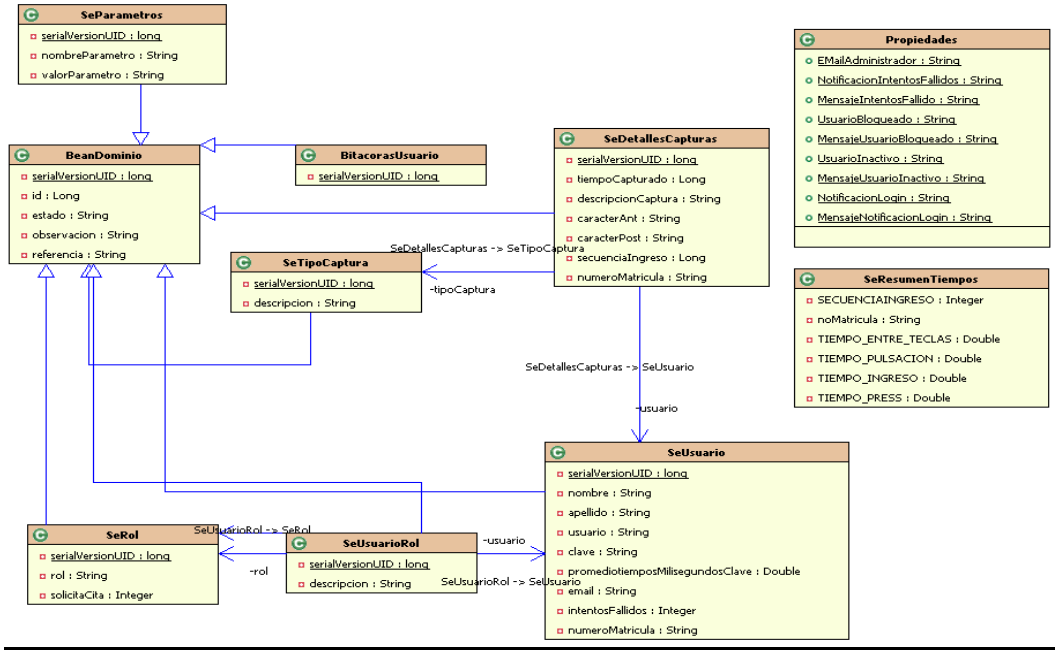

Figura 3. 6 Diagrama UML de Modelo de Clases

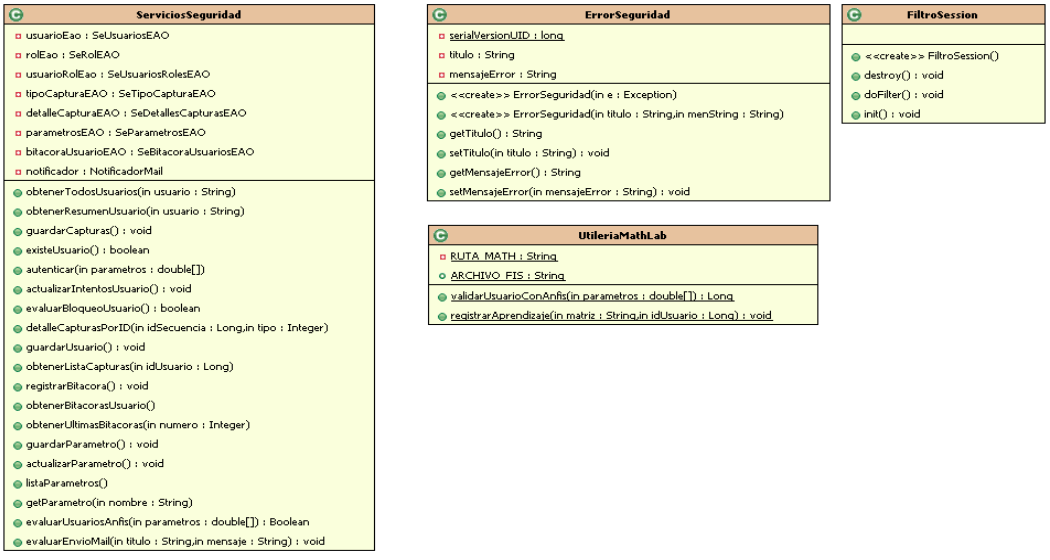

Figura 3. 7 Diagrama UML de Modelo de Utilerías

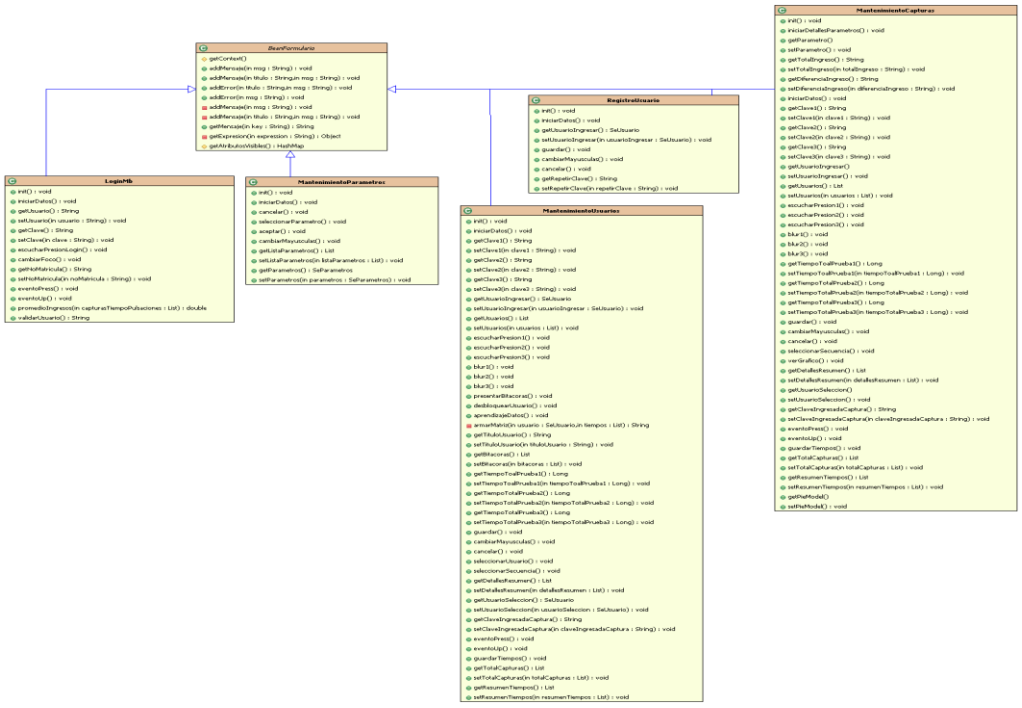

Figura 3. 8 Diagrama UML Modelo de Vistas

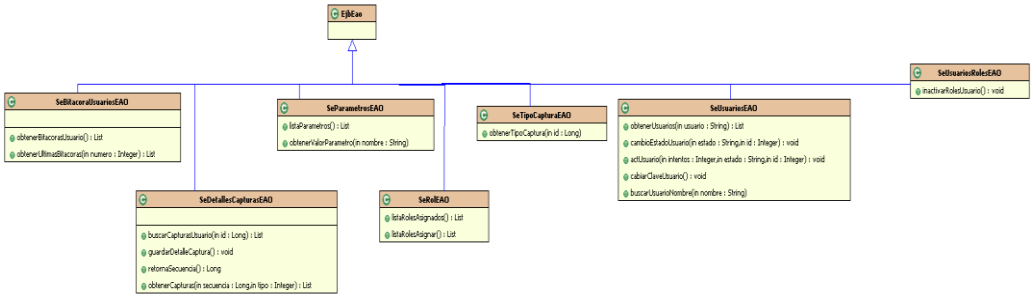

Figura 3. 9 Diagrama UML Modelo EAO

Para implementar el modelo de datos Bio-Key se utiliza una base de datos relacional y el modelado se ha realizado utilizando un diagrama Entidad relación, el cual permite identificar los objetos de base de datos y sus relaciones. En la figura # 3.10 presentamos el modelo entidad relación de Bio-Key.

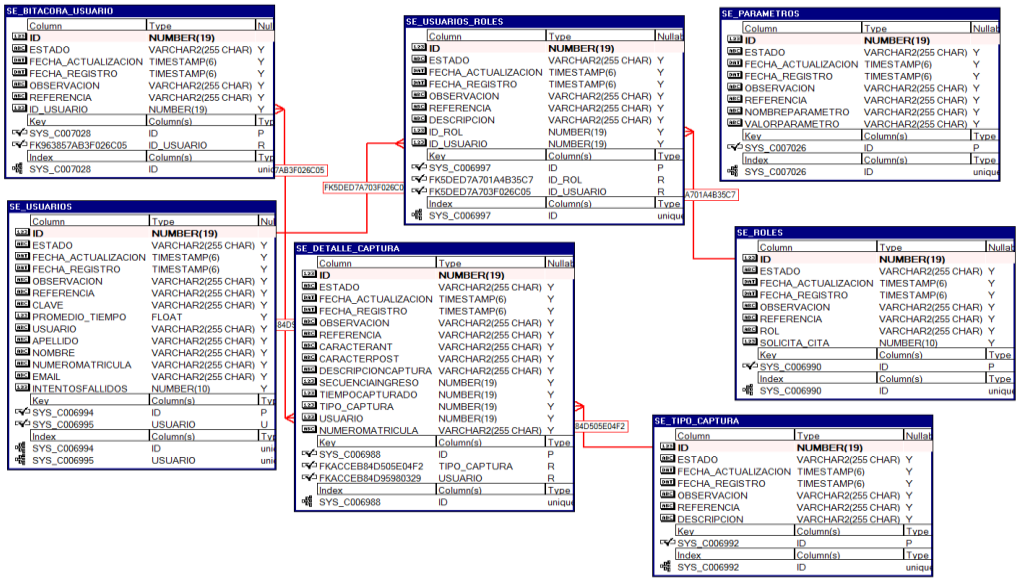

Figura 3. 10 Diagrama Modelo Entidad Relación de Bio-Key

3.3. DISEÑO DE PRUEBAS

3.3.1. Escenarios de Evaluación

Los escenarios de evaluación elaborados para validar el desempeño del sistema Bio-Key, consisten en permitir acceso en un Sistema Prototipo WEB

a múltiples usuarios para medir los tiempos de dinámica de tecleo que utilizan al momento de digitar una contraseña.

Las pruebas a realizar involucran básicamente dos formas de acceso al sistema Bio-Key y dos únicos resultados obtenidos al momento de validar el acceso al sistema, tal como se describe en la Tabla # 1:

BIO-KEY		
Actor	Escenario Evaluación	Resultado Autenticación
Usuario Válido	Ingresar al sistema con su clave privada.	Otorga acceso
		Deniega Acceso
Usuario Impostor	Ingresar al sistema con la clave obtenida de un usuario de manera fraudulenta.	Otorga Acceso
		Deniega Acceso

Tabla 1 : Resultados de la Autenticación

Las evaluaciones se realizaron a usuarios validos como a usuarios ilegítimos o impostores en un total de 10 intentos por cada actor.

3.3.2. Métricas para evaluación del Sistema.

Como se indicó en la sección 3.1 vista panorámica del diseño, Bio-Key identifica si un usuario es aceptado o rechazado basado en umbrales de incertidumbre con el cual se define el grado de confianza para identificar un usuario autorizado o impostor. El grado de aceptación nos permite utilizar

dos tasas de errores para evaluar el sistema, la tasa de falsa aceptación y la tasa de falso rechazo, las cuales serán descritas en las dos siguientes secciones.

3.3.2.1. Usuario Legítimo e Impostor.

En Bio-Key un usuario es considerado legítimo cuando se identifica que el porcentaje de similitud entre la habilidad de tecleo de la contraseña y el patrón de tecleo aprendido en ANFIS para el mismo usuario excede al 70%.

Un usuario es impostor cuando el sistema Bio-Key identifica que el porcentaje de similitud entre la habilidad de tecleo de la contraseña y el patrón de tecleo aprendido en ANFIS para el mismo usuario no excede al 70%.

3.3.2.2. Falsa Aceptación y Falso rechazo.

La Falsa Aceptación (FAR: False Acceptance Rate) ocurre cuando el sistema autentica de forma correcta a un usuario ilegitimo o impostor y el Falso rechazo (FRR: False Rejection Rate) se define como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor [16].

La FAR y la FRR son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos. Si, por ejemplo, para el

ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa, como muestra la figura # 3.11. El grado de seguridad deseado se define mediante el umbral de aceptación u, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

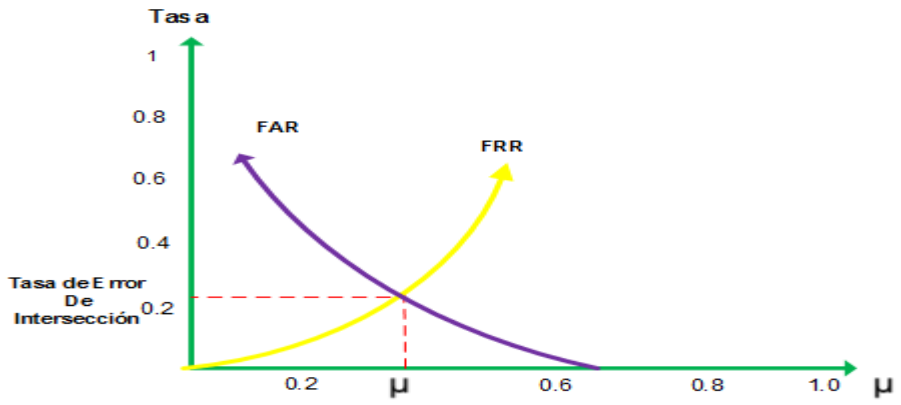

Figura 3. 11 Modelado de tasas FRR y FAR para Sistema Biométrico

La FRR es una función estrictamente creciente y la FAR una estrictamente decreciente [16]. La FAR y la FRR al ser modeladas como función del umbral de aceptación tienen por dominio al intervalo real [0,1], que es además su recorrido, puesto que representan frecuencias relativas. La figura # 20 muestra una gráfica típica de la FRR y la FAR como funciones de u. En esta figura puede apreciarse un umbral de aceptación particular, denotado por u*, donde la FRR y la FAR toman el mismo valor. Este valor recibe el nombre de tasa de error de intersección (cross-over error rate) y puede ser utilizado como medida única para caracterizar el grado de seguridad de un sistema biométrico. En la práctica, sin embargo, es usual expresar los requerimientos de desempeño del sistema, tanto para verificación como para identificación, mediante la FAR. Usualmente se elige un umbral de aceptación por debajo de u* con el objeto de reducir la FAR, en desmedro del aumento de la FRR.

CAPÍTULO 4.

4. IMPLEMENTACIÓN DEL SISTEMA

4.1. Desarrollo del Sistema

Para resolver el problema planteado en el capítulo 1, Bio-Key compara patrones biométricos que se forman a partir de la inscripción del usuario al sistema y del momento en el cual el usuario ingresa, en el cual se valida si es un usuario valido o impostor. Los principales puntos relacionados con la metodología de la extracción del patrón biométrico y la comparación de estos para la autenticación se describen en las siguientes secciones.

4.1.1. Generación de Muestra Biométrica de Tecleo

El método que se plantea para la obtención de la muestra biométrica de la dinámica de tecleo de un usuario, se basa en la medición de los tiempos característicos de dinámica de tecleo generados al momento de ingresar el

conjunto de caracteres digitados correspondientes a la contraseña de usuario para acceder al sistema.

En la implementación del método, tres características fueron extraídas de la contraseña, estas son: el tiempo entre las pulsaciones de dos teclas consecutivas (Pulsar-Pulsar), el tiempo entre soltar la tecla anterior y pulsar la siguiente tecla (Soltar-Pulsar) y el tiempo entre pulsar y soltar la misma tecla (Pulsar-Soltar). A continuación presentamos el modelo matemático utilizado para representar las características extraídas:

Sea $k = \{ k_1, k_2, k_3, \ldots\ldots\ldots k_n \}$ el conjunto de teclas que fueron pulsadas para representar la clave de un usuario. Definimos como $t_{i.pulsar}$ el instante de tiempo en que la tecla k_i es pulsada y como $t_{i.soltar}$ el instante de tiempo en que la tecla k_i es suelta, donde i = 1,2,3,…..,n.

A) Tiempo pulsar-pulsar

La característica que llamaremos de "tiempo pulsar-pulsar" se refiere al intervalo de tiempo que es medido entre las pulsaciones de dos teclas consecutiva. Se definen los elementos del vector de la característica temporal pulsar-pulsar para un par de teclas consecutivas (k_i, k_{i+1}) como:

$pp_i = t_{i+1,\,pulsar} - t_{i.\,pulsar}$, donde i=1,2,……..,n-1

B) Tiempo soltar-pulsar

La característica que llamaremos de tiempo "soltar-pulsar" se refiere al intervalo de tiempo que es medido entre soltar una tecla y pulsar la tecla

consecutiva. Se definen los elementos del vector de la característica temporal soltar-pulsar para un par de teclas consecutivas (k_i, k_{i+1}) como:

$sp_i = t_{i+1,pulsar} - t_{i.soltar}$, donde i=1,2,…….,n-1

C) Tiempo pulsar-soltar

El intervalo de tiempo entre pulsar y soltar una misma tecla es conocido como duración de la tecla (keystroke duration). Se definen los elementos del vector de la característica temporal pulsar-soltar para una tecla como:

$ps_i = t_{i,soltar} - t_{i.pulsar}$, donde i=1,2,…….,n-1

En la figura # 4.1 se puede apreciar las características asociadas a los tiempos y pulsaciones de las teclas de la palabra YOVY.

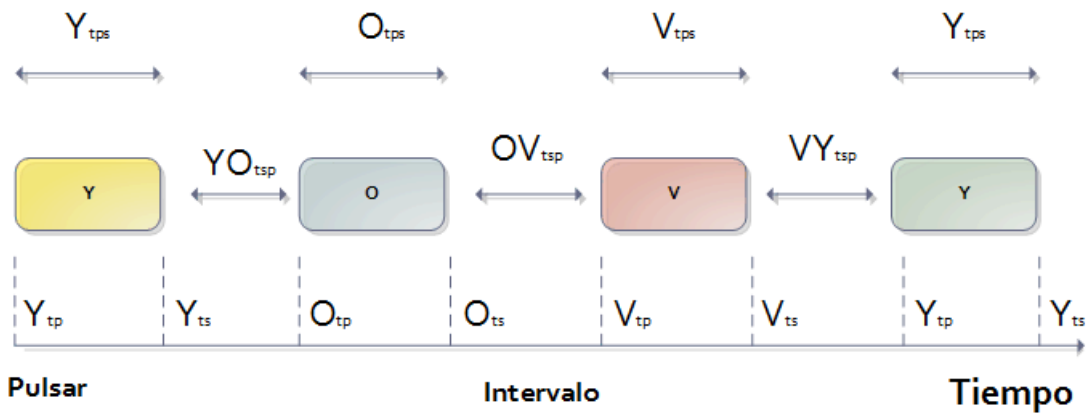

Figura 4. 1 Diagrama de Características de la Dinámica de Tecleo

El registro de los tiempos descritos se realizó mediante los eventos KeyUp cuando el usuario libera una tecla y KeyDown cuando el usuario pulsa una tecla, estos eventos se encuentran disponibles en el objeto KeyListener de

java y se ejecutan cuando el usuario realiza pulsaciones de teclas en el teclado.

En la Figura # 4.2 se visualizan los registros de tiempos de tecleo ingresados por estudiantes de la facultad de ingeniería eléctrica y computación en Bio-key.

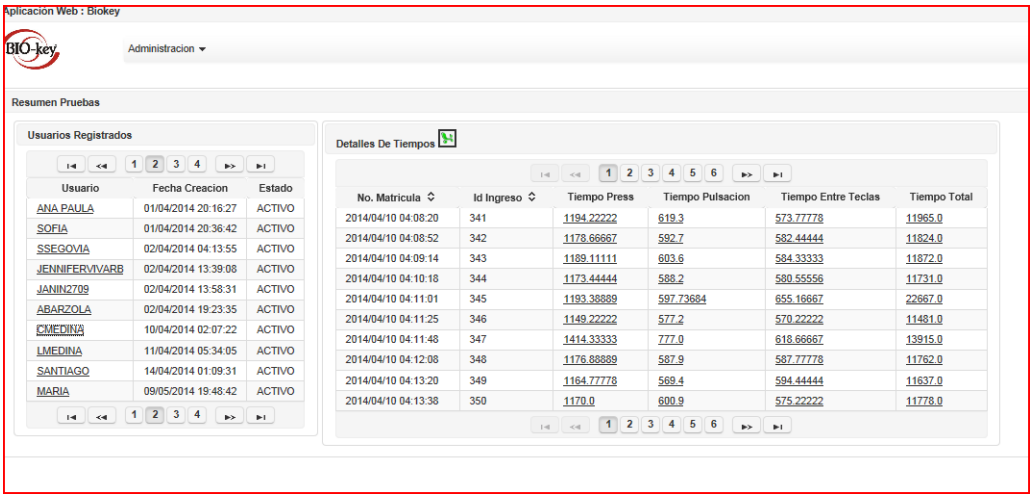

Figura 4. 2 Captura de Pantalla de Tiempos de Tecleo

Como se mencionó en la sección 2.2, la generación del patrón biométrico se genera cuando se inscribe el usuario al sistema y cuando se realiza la prueba de acceso, las Figuras 4.3 y 4.4 muestran los eventos que se utilizan en estos dos instantes.

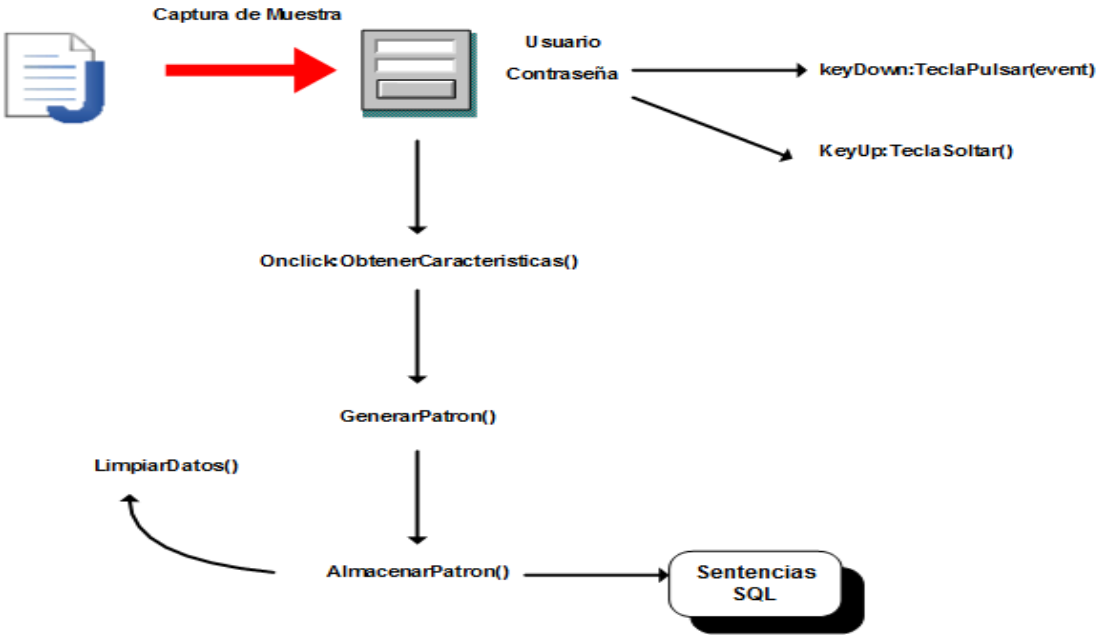

Figura 4. 3 Diagrama Entrenamiento de Bio-Key

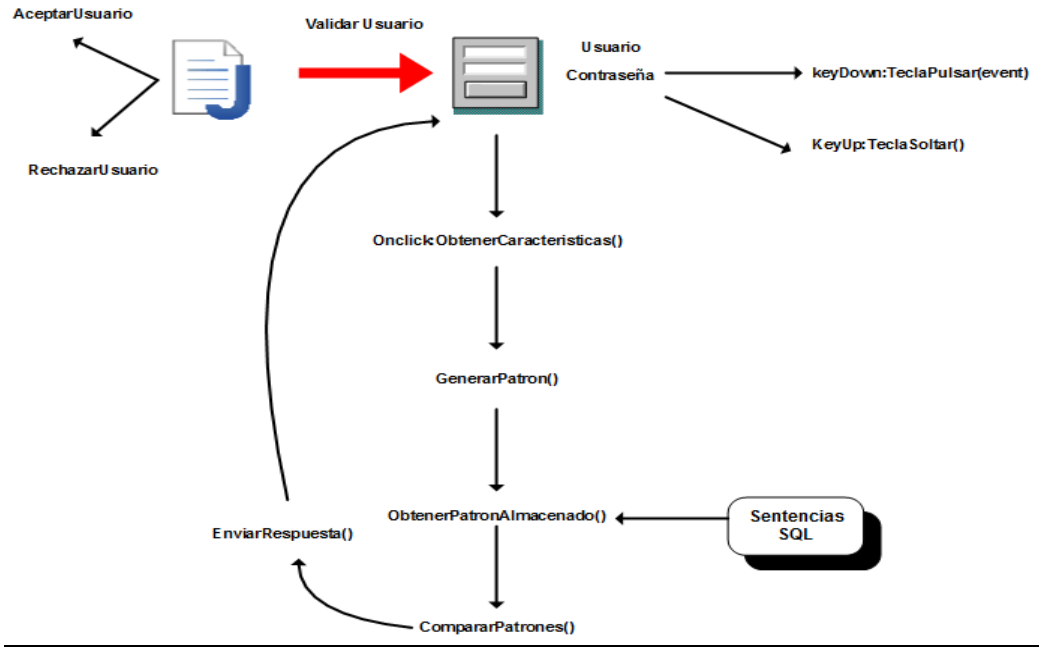

Figura 4. 4 Diagrama Validación de Usuario en Bio-Key

4.1.2. Generación del Patrón Biométrico de Tecleo

Para la generación del patrón biométrico se deben obtener al menos 50 muestras biométricas, la cual es una cantidad suficiente y permite seleccionar un grupo determinado de ellas, las cuales servirán para extraer una plantilla con los tiempos promedios de PULSAR-PULSAR, SOLTAR-PULSAR y PULSAR-SOLTAR, a esta plantilla le asociamos un código identificador de usuario, ambos forman la matriz de datos de aprendizaje de la red ANFIS Bio-Key formada por cuatro vectores característicos, tres de entrada y uno de salida.

Las funciones de pertenencia fueron modeladas de forma inicial mediante la utilería GENFIS de MathLab.

La ejecución del aprendizaje se realiza utilizando el TOOLBOX de MathLab AnfisEdit, el proceso recibe por entradas un conjunto de muestras de tiempos característicos Figura # 4.5.

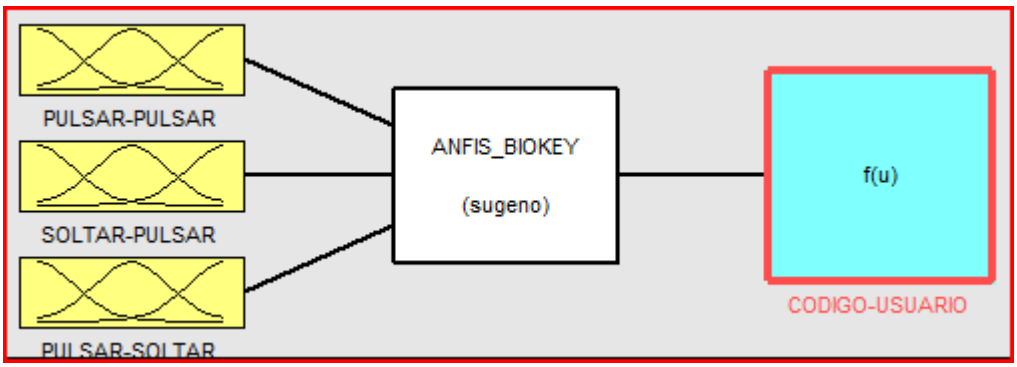

Figura 4. 5 FIS ANFIS_BIOKEY

En la figura # 4.6 se muestra el modelo estructural de Anfis generado con 3 funciones de membresía tipo triangulo para cada uno de los tiempos característicos.

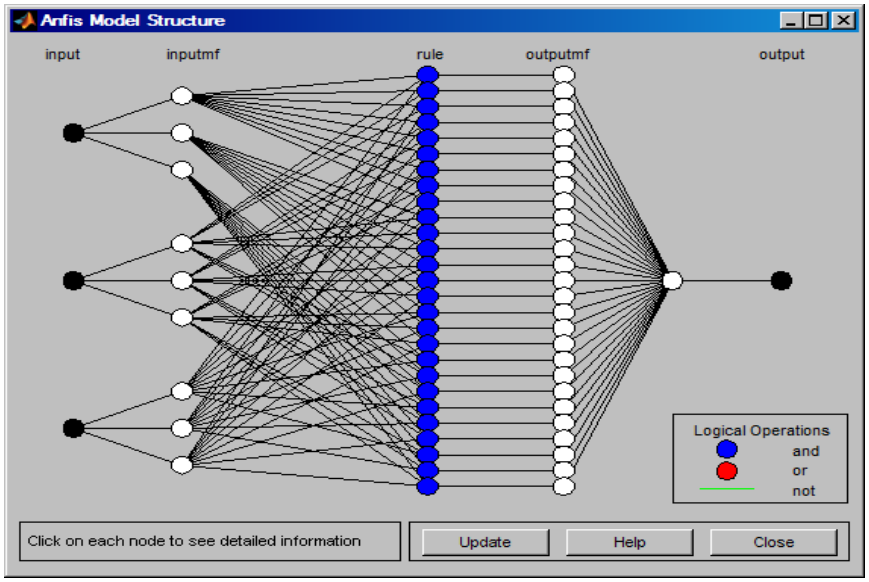

Figura 4. 6 Modelo de Estructura ANFIS_BIOKEY

Luego del entrenamiento se conforman reglas del tipo IF_THEN las cuales se ilustran en la gráfica de superficie mostrada a continuación: figuras 4.7 y 4.8

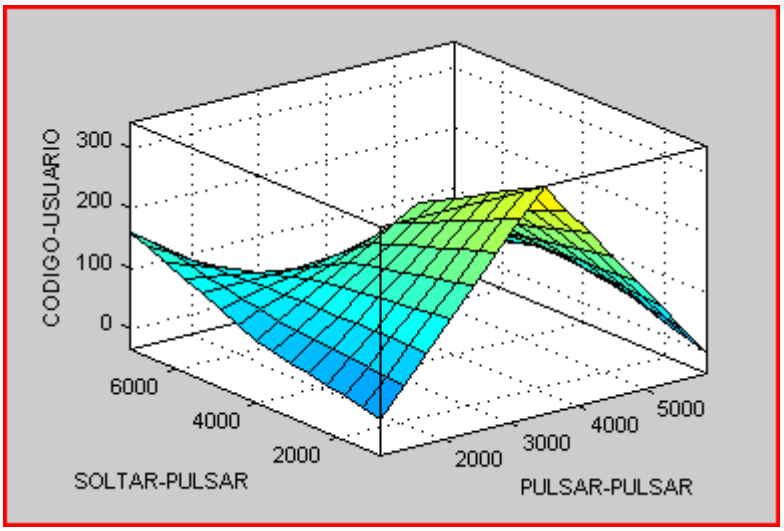

Figura 4. 7 Diagrama de Superficie de Reglas

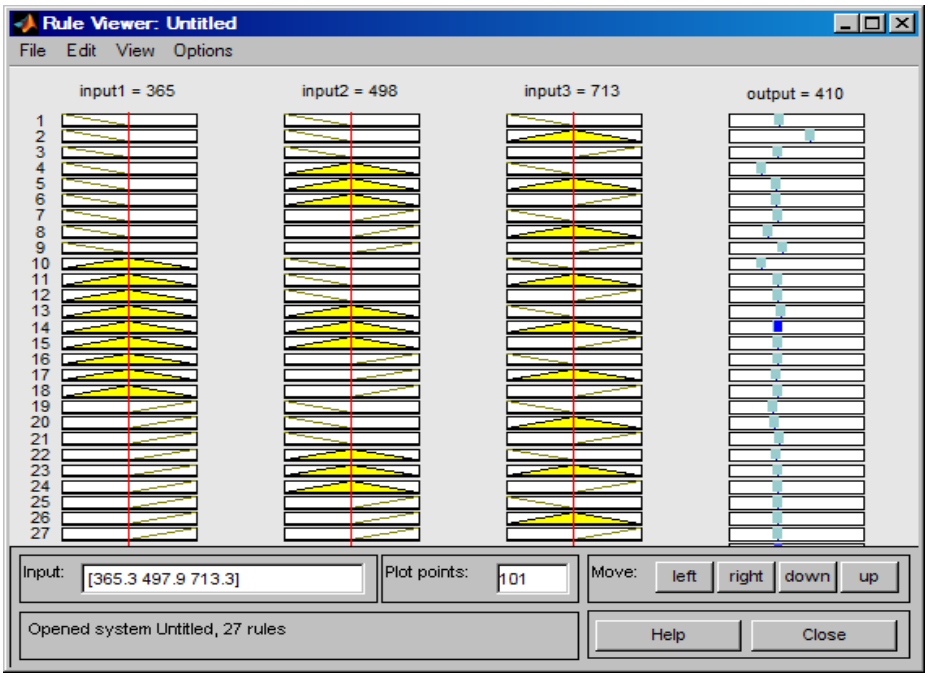

Figura 4. 8 Visor de Reglas

4.1.3. Almacenamiento del patrón biométrico en la Base de Datos.

Una vez que se genera la muestra biométrica o el patrón biométrico de tecleo, esta se almacena en una base de datos relacional, la idea de

almacenar esta información es poder generar reportes y auditar la información ingresada por los usuarios aceptados y rechazados.

4.1.4. Administración de Usuarios, Parámetros, Umbrales y Reportes

La interfaz de administración de usuarios permite administrar la seguridad de accesos en la aplicación para todos los usuarios registrados en el Sistema, permite generar: Bitácora de ingresos, Matriz Test de Ingresos y Generar Base de Conocimiento ANFIS del Usuario. La pantalla de Administración de usuarios se presenta en la Figura # 4.9.

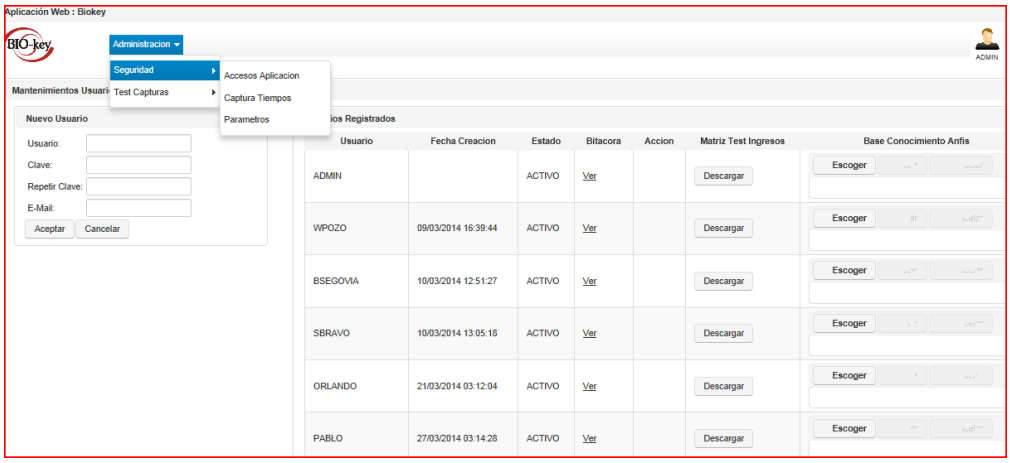

Figura 4. 9 Captura de Pantallas - Administración de Usuarios Aprendizaje

Adicionalmente permite modificar los parámetros que se muestran a continuación:

NUMERO INTENTOS: Cantidad mínima de Intentos exigidos para un usuario para que Bio-Key pueda habilitar el modo aprendizaje.

NUM INTENTOS MAIL: Cantidad de mínima de intentos requeridos para que Bio-Key desconozca al usuario, generar un mail de alerta.

NUM INTENTOS BLOK: Cantidad de intentos que permite Bio-Key al usuario desconocer antes de bloquearlo en el sistema.

DATOS: Cantidad de capturas de tiempos característicos exigidas al usuario para conformar una muestra representativa de datos de aprendizaje.

DOBLE AUTENTICACION: Habilita o deshabilita la autenticación ANFIS-BIOKEY según el valor que tome, el valor “S” Habilita esta opción, mientras que en parámetro configurado en “N” la inactiva.

En la figura # 4.10 se pueden apreciar los parámetros de configuración de Bio-Key.

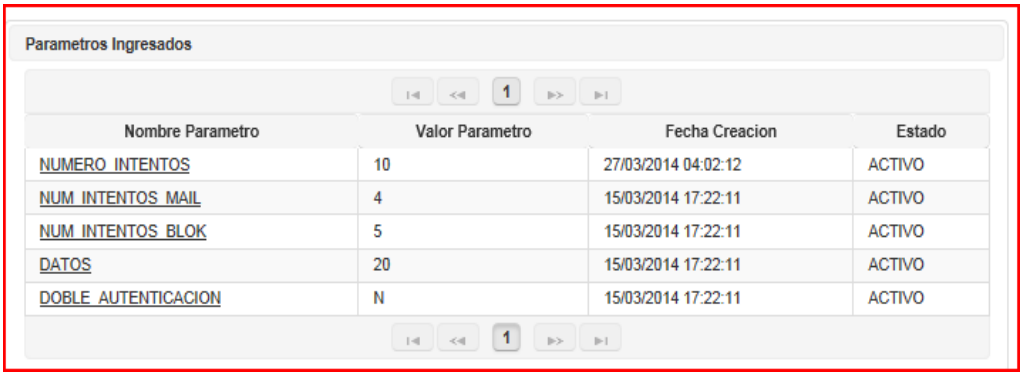

Figura 4. 10 Captura Pantalla - Administración de Parámetros Aprendizaje

Bio-key cuenta con un módulo de reportes para poder auditar los datos ingresados por los usuarios aceptados y rechazados. La idea principal de los reportes es poder realizar un análisis de las tasas de falso rechazo y falsa aceptación para fijar el umbral de aceptación en valores que se adapten a los

niveles de seguridad deseados. La pantalla de reportes de Bio-key se presenta en la figura # 4.11.

Figura 4. 11 Captura Pantalla - Consulta Visual de Acceso Usuarios

CAPÍTULO 5.

5. PRUEBAS Y ANÁLISIS DE DESEMPEÑO

5.1. Estudio

Para las pruebas del Sistema Prototipo se recolectaron muestras de estudiantes de la carrera de ingeniería en Computación de la FIEC, amigos y familiares. Lo que se intentó con este grupo heterogéneo, es probar que la aplicación biométrica logra reconocer a cualquier persona.

Los objetivos de la prueba fueron probar la autenticación del usuario y establecer los porcentajes de falsas aceptaciones (FAR) y falsos rechazos (FRR).

En la primera fase se les solicitó a los usuarios que dieran de alta a su perfil en el sistema, cada uno de ellas realizó el ingreso de un usuario y contraseña, la cual podían elegir libremente, pero se les hacía la recomendación de que usaran una palabra o frase con la que estuvieran familiarizados en su escritura y que fuera de al menos de diez caracteres de

longitud. El umbral de aceptación (UA) del sistema se fijó en 80%, Se decidió tomar este valor en base a los resultados reportados en [17] y a algunas pruebas y observaciones preliminares hechas por nosotros. Para la extracción de las características de tecleo de las personas, se les solicitó teclear 50 veces el usuario y contraseña, con esta información se obtuvo el patrón biométrico de tecleo de la persona.

La recolección de muestras y la medición de los tiempos de tecleo, se realizó a través del acceso al Software Prototipo Bio-Key, publicado en el portal Web de la Facultad de Ingeniería Eléctrica y Computación (FIEC), la URL utilizada para el acceso a la página de la aplicación es: www.fiec.espol.edu.ec\bio-key. Luego de obtener el patrón biométrico de la persona, se le solicitó al usuario autenticarse en un sistema prototipo de control de acceso. La figura # 5.1 muestra la pantalla de control de acceso para autenticar usuarios en Bio-Key.

Figura 5. 1 Captura de Pantalla - Ingreso Sistema Bio-Key

5.2. Resultados

La tabla 2 muestra los resultados de la autenticación de 5 usuarios legítimos e impostores. De un total de 500 intentos de autenticación que hubo por parte de usuarios legítimos, el sistema rechazó de manera equivocada un total de 15 intentos. De este análisis se obtuvo las tasas medias de FRR igual 3% y de 1.6 % para FAR, aceptables para un sistema biométrico de Dinámica de Tecleo. .

ID USUARIO	INTENTOS VALIDOS	FRR (%)	FAR (%)
WPOZO	100	0	2
CMEDINA	95	5	1
PAOLA	95	5	3
DANIEL	100	0	1
GLORIA	95	5	1
Media	**97**	**3**	**1.6**

Tabla 2 : Desempeño del Sistema de Autenticación Biométrico

En síntesis, se obtuvo un error de falsa aceptación no superior al 1.6 %, lo que constituye una fortaleza de este método. El aspecto crítico del sistema de autenticación es no aceptar a un usuario impostor, ya que el hecho de

rechazar al usuario correcto tiene como consecuencia únicamente que el usuario tenga que autenticarse nuevamente.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Este trabajo tuvo por objetivo lograr una nueva aportación a las áreas de seguridad de la información, al desarrollar un sistema capaz de reconocer dinámicas de tecleo y que pudiera trabajar en conjunto con los tradicionales sistemas de autenticación basados en nombre de usuario y contraseña, de esta manera fortalecer la seguridad proporcionada por éstos últimos.

Basándonos en los resultados experimentales podemos concluir que:

1.-La dinámica de tecleo es un método seguro para la autenticación de usuarios, pero posee un grado de imprecisión, si este método se lo combina con otros se obtiene un método infalible para solucionar el problema presentado en el capítulo 1.

2.-Nuestra contribución en este trabajo es la utilización de tres características de la dinámica de tecleo y la implementación utilizando ANFIS y lógica difusa.

3.-La principal ventaja que se encontró en el actual sistema biométrico es que provee una segunda capa de seguridad, fortaleciendo los sistemas basados en nombre de usuario y contraseña; otra ventaja es, que actúa de manera transparente para el usuario durante la etapa de autenticación.

4.-La desventaja que se presenta, radica en la etapa de registro de usuario, ya que para algunos de ellos puede llegar a ser tedioso el escribir en repetidas ocasiones su contraseña.

5.-La dinámica de tecleo es un método biométrico de autenticación seguro y que aún no ha sido explotada como otras técnicas biométricas, a pesar de que su implementación requiere un bajo costo y no es invasiva como otros métodos biométricos.

Recomendaciones

Respecto al trabajo a futuro hay varios puntos importantes sobre los cuales enfocarse:

1.-Al sistema se le puede agregar un método de adaptación, es decir, que le permita al software reconocer y aprender las variaciones y evolución que va sufriendo la dinámica de tecleo del usuario a lo largo del tiempo, lo que permitiría mejorar el desempeño.

2.-El software se podría mejorar para que sea tolerante a los errores de escritura tanto en el proceso de registro como en el de autenticación.

3.-Un último aspecto sobre el cual hay que trabajar es el portar el sistema a teléfonos celulares convencionales, los cuales no cuentan con pantallas táctiles para el ingreso de dato

BIBLIOGRAFÍA

[1] Vega Pérez “Auditoria de Sistemas Informáticos” Universidad Católica del Salta “Auditoria de Sistemas” (2005).

http://apuntes.secureinf.com/auditoria-de-sistemas-informáticos.htmln

[2] Pró L. González J. y otros., (2009) “Tecnologías Biométricas aplicadas a la seguridad en las organizaciones”, Universidad Nacional Mayor de San Marcos, Perú.

[3] S. M. Matyas Jr, and J. Stapleton, “ A Biomatric Standard for information Management and Security” Computers & Security, vol 19 pp428-441, May,2000.

[4] L. Hong and A. Jain, “Integrating Faces and Fingerprints for Personal Identification”, IEEE Transaccions on Pattern Analisys and machine Intelligence, vol. 20, no. 12, pp. 1295-1307,1998.

[5] Tom Olzak, “Keystroke Dinamic: Low Impact Biometric Verification”, pp. 1-10 September 2006.

[6] Jarmo Ilonen. Keystroke Dynamics. Technical report, Lappeenranta University of Technology, 2004.

[7] L.C.F. Araújo, M.G.Lizárraga, L.H.R. Sucupira Jr., J.B.T. Yabu-uti y L.L. Ling “Autenticación Personal por Dinámica de Tecleo Basada en Lógica Difusa”, Universidad Estatal de Campinas, Sao Paulo, Brasil 2000.

[8] “Control Difuso” [en Línea]. Universidad Simón Bolívar, Septiembre 2007 [ref. 5 de septiembre del 2007]. Disponible en Web

http://prof.usb.ve/montbrun/ps2320/fuzzy/fuzzy.html

[15] Xavier Ferré Grau, María Isabel Sánchez Segura. “Desarrollo Orientado a Objetos con UML”, Facultad de informática – UPM, pp. 9 September 2006.

[16] D. Morales, “Reconocimiento Digital de Huellas Dactilares en base a Vectores de Carac2, Tesis de Ingeniero Civil Electricista, Universidad de Chile, 1999.

[17] Jose Guadalupe Aguilar Hern´andez and Luis Adrian Lizama P´erez. Autenticaci´on de usuarios a trav´es de Biometr´ıa de Tecleo. Mexican Conference on Informatics Security 2006, 2006.

[18] Online Etymology Dictionary. Authentication. http://www.etymonline.com.