Seguridad en el acceso a Bases de Datos utilizando Agentes Móviles

David Franco Borré[*] Yasmín Moya Villa[†] Moises Quintana Alvarez[‡]

Resumen

En este articulo se analizan aspectos concernientes a los agentes móviles y los problemas de seguridad que estos conllevan presentando un modelo o esquema para acceder a una bases de datos distribuida que permita en un alto grado mejorar los tiempos de respuestas en la red y crear un modelo de seguridad que colabore en el proceso de autenticación de los usuarios a la base de datos. El modelo propuesto lo hemos denominado **ABADAM** (Acceso a BAses de Datos utilizando Agentes Móviles), ABADAM se implementó utilizando: el lenguaje de programación JAVA, el API AGLETS y MS SQL Server.

Palabras claves: *Agentes Móviles, Base de Datos Disribuida, Java, Aglets, MS SQL Server.*

Abstract

In this paper analyze aspects concerning the mobile agents and the problems of security that these entail presenting a model or scheme to accede to distributed databases that allow in a high degree to improve the response times in the network and to create a security model that collaborates in the process of authentication of the users to the data base. The proposed model we have denominated it ABADAM (Access to Databases using Mobile Agents), ABADAM was implemented using: the programming language JAVA, API AGLETS and MS SQL Server.

Keywords*: Mobile Agents, Distributed Databases, Java, Aglets, MS SQL Server.*

1 Introducción

En los últimos años se ha discutido como los agentes móviles se han convertido en una nueva herramienta de programación en ambientes distribuidos e Internet. El crecimiento acelerado de las redes ha conducido a un mayor desarrollo de sistemas de información distribuidos donde se puede acceder a bases de datos distribuidas. La necesidad de tener los programas cerca de los datos para aumentar el rendimiento de las aplicaciones dio origen a tecnologías como CORBA y DCOM. Con la aparición de los agentes móviles y lenguajes multiplataformas como Java, los ambientes distribuidos han demostrado mejorar el desempeño de las aplicaciones permitiendo una interacción local en el procesamiento de la información reemplazando tener una conexión constante en la red. A pesar del desempeño que se ha logrado con el uso de agentes móviles para acceder a bases de datos distribuidas, el crecimiento de esta tecnología se ha visto retardada por problemas de seguridad.

La originalidad de este trabajo consiste en diseñar e implementar un sistema de agentes móviles que colaboren en el proceso de autenticación para acceder a una base de datos distribuida, aunque

[*] Universidad Tecnológica de Bolívar, Cartagena (Colombia), dafrabo@yahoo.com
[†] Universidad Tecnológica de Bolívar, Cartagena (Colombia), yasminmoyavilla@yahoo.com
[‡] Universidad Tecnológica de Bolívar, Cartagena (Colombia), mquintan@unitecnologica.edu.co

este proyecto trabaja con un sistema de agentes móviles para acceder a bases de datos distribuidas pero, por su diseño flexible, se puede aplicar a cualquier arquitectura de bases de datos que soporte instrucciones SQL y se pueda conectar mediante un driver ODBC, este articulo es soportado por el proyecto de grado que lleva el mismo nombre para optar por el título de Magíster en Ciencias de la Computación y pretende ser un aporte más de las aplicaciones de los agentes móviles.

2 Agentes Móviles

Un Agente Móvil es un objeto especial que tiene un estado de datos (otros objetos no agentes, estructuras y bases de datos), un estado de código (las clases del agente y otras referencias a objetos) y un estado de ejecución (el control de procesos que se ejecutan en el agente).

La característica principal de un agente móvil es que accede a un conjunto de métodos que le permiten moverse de un servidor a otro. Un agente móvil tiene: un programa que define las actividades que ejecutará y un grado de inteligencia que, además de ayudarlo a interactuar con los usuarios, lo ayuda a la resolución de tareas adversas de su entorno.

Las características básicas de un agente móvil son: autonomía, movilidad, concurrencia, direccionabilidad, continuidad, reactividad, sociabilidad y adaptabilidad.

Un agente para que sea catalogado como agente móvil debe ser capaz de ejecutarse en diferentes computadoras, es decir, que pueda suspender su ejecución en un servidor y reanudarla en otro servidor una vez que se haya desplazado a este.

Según Lange y Oshima [2]: “Un agente móvil es una entidad que tiene cinco atributos: estado, implementación, interfaz, identificador y un ente principal (persona u organización)” (Figura 1). Cuando el agente se mueve en la red toma estos atributos y viaja con ellos. El estado lo necesita el agente para reanudar el cómputo después de viajar. La implementación se necesita para la ejecución del agente independiente de su ubicación. La interfaz se necesita para comunicación del agente. El identificador se necesita para reconocer y ubicar al agente mientras viaja. Y el ente principal determina la responsabilidad moral y legal.

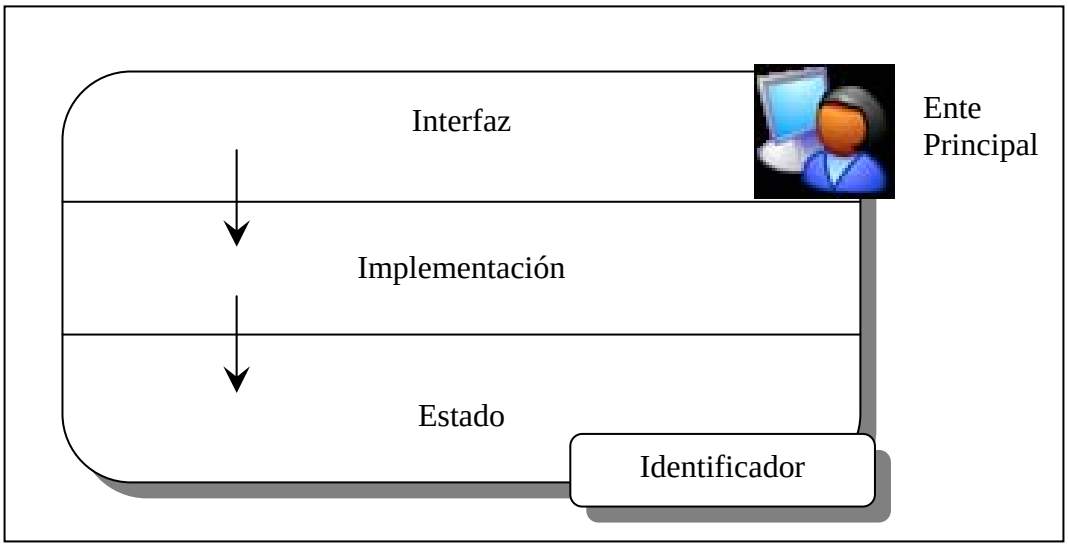

Figura 1. Propiedades de los Agentes

Una de las principales motivaciones para el uso de los agentes móviles es su aplicabilidad en sistemas distribuidos. Danny Lang [3] presenta siete ventajas que se obtienen al utilizar agentes móviles:

1. Reducen el tráfico de red.
2. Superan el estado latente de las redes.
3. Encapsulan protocolos.
4. Se ejecutan de forma asíncrona y autónoma.
5. Se adaptan dinámicamente.
6. Son heterogéneos por naturaleza.
7. Son robustos y tolerables a fallas.

Entre las aplicaciones de los agentes móviles, Venners Hill [4] cita las siguientes:

- Recolección de datos de distintos sitios.
- Búsqueda de filtrado.
- Monitorización.
- Comercio electrónico.
- Procesamiento paralelo.
- Distribución masiva de información.
- Interacción y negociación.
- Cálculos en multiprocesos.
- Redes parcialmente desconectadas.
- Entretenimiento y entrega de correo inteligentemente.

Una de las principales plataformas para el desarrollo de agentes móviles es JAVA dado que maneja de manera eficiente la seguridad y portabilidad por su característica de lenguaje interpretado (su salida no es un ejecutable, sino un código binario ejecutado por una máquina virtual que emula el interprete de Java). Vale la pena mencionar algunos sistemas que permiten la implementación de agentes móviles: Aglets, Java-to-go, ARA, Voyager, Mole, Agent TCL, Odyssey, TACOMA, entre otros.

3 Seguridad de los agentes móviles

Las aplicaciones basadas en agentes móviles no deben implementarse hasta que se tomen medidas mínimas de seguridad en la red, como tener un firewall y brindar protección a los servidores contra código malicioso que viene en un agente móvil, todo esto se puede prevenir con controles y protecciones adecuadas para el acceso en ambientes de ejecución.

El tema de la seguridad de agentes móviles ha sido un factor fundamental para que no sea aceptado en su totalidad en Internet, pero hay plataformas para la creación de agentes móviles que permiten alcanzar un nivel de seguridad aceptable, una de ellas son los Aglets que son capaces de restringir el acceso de los agentes generalizándolos en dos grupos: confiables y no confiables.

Los agentes móviles son programas que viajan con su código y datos desde un computador a otro a través de Internet o cualquier red, lo que conlleva a que surjan varios problemas de seguridad porque tanto los agentes móviles como los servidores con que interactúan son vulnerables a ataques y brechas de seguridad. Algunos problemas de seguridad que se pueden presentar son: Autenticación, Autorización y Confidencialidad.

La movilidad de los agentes y la interacción con otras máquinas de la red, puede hacer que surjan algunos requerimientos de seguridad en el acceso a bases de datos distribuidas que podrían ser clasificados de dos tipos. El primero de ellos se refiere a los problemas de seguridad inherentes a los sistemas de agentes móviles y en el segundo se refiere a los aspectos que se requieren para garantizar la seguridad en el ámbito de la Base de Datos Distribuida. A continuación se expone con mayor detalle cada uno de estos problemas.

3.1 Amenazas de Seguridad Inherentes al Sistema de Agentes Móviles

La seguridad ha sido tradicionalmente un inconveniente en los sistemas informáticos, pero el sistema de agentes móviles por sus características presenta un nuevo tipo de inconvenientes de seguridad. Los dos problemas principales son: El problema del agente malicioso y el problema del servidor malicioso.

3.1.1 El Problema del Agente Malicioso.

Cuando los agentes móviles llegan al servidor, necesitan algunos permisos de usuario para poder ejecutar su código. Normalmente el control de acceso a los equipos de una red se hace por medio de contraseñas, en donde cada usuario se autentica al inicio con su *login* y *password*; pero este esquema funciona para sistemas estáticos y no para agentes móviles, puesto que el agente debe llevar una contraseña para cada sitio de su itinerario, lo que aumenta su tamaño y así mismo incrementa los requerimientos de seguridad para poder proteger esas contraseñas.

Entre los agentes pueden existir agentes maliciosos que realizan acciones no deseadas o destructivas, como el acceso no autorizado, alteración de la información, sobrecargar o causar incluso daños a la integridad del servidor. En la figura 2 se presenta un agente malicioso que llega al servidor para realizar labores que atentan contra la integridad del servidor, como es la utilización no autorizada de los recursos para obtener información privada.

El problema del agente malicioso puede generar tres tipos de amenazas a los servidores:

- **El acceso no autorizado a los recursos.** Cuando un agente móvil llega a un servidor, ejecuta su código usando los recursos de este. Por esta razón, los recursos del servidor están expuestos a ataques de agentes maliciosos, por lo tanto si no existen mecanismos de controles adecuados, agentes no deseados podrían acceder los datos privados del sistema. En el caso de las Bases de Datos Distribuidas, si un agente malicioso accede a los datos puede modificarlos y causar inconsistencias en la base de datos.

- **Sobrecarga de los recursos del servidor.** Se deben plantear mecanismos de protección adecuados para prevenir el consumo excesivo de los recursos del servidor por parte de agentes no deseados, debido que al sobrecargarlo el tiempo de respuesta se incrementa o inclusive hacer que no haya respuesta a los agentes que buscan acceder a la base de datos.

- **Creación de agentes residentes en el Servidor.** Un ataque del cual puede ser víctima un servidor por parte de un agente malicioso, es la creación de un agente que resida en el servidor. Con un agente de este tipo podría suceder cualquiera de los dos ataques mencionados anteriormente, ó que se clonen tantos agentes que podrían también sobrecargar al servidor hasta bloquearlo.

La solución que se le da normalmente al problema del agente malicioso se lleva a cabo por medio de restricción de privilegios a los agentes, pero esto podría ocasionar que los usuarios que traten de acceder a la base de datos mediante un agente no pueda hacerlo, por tal razón es necesario buscar mecanismos alternos de protección que brinden seguridad y permitan la realización de las tareas de los agentes.

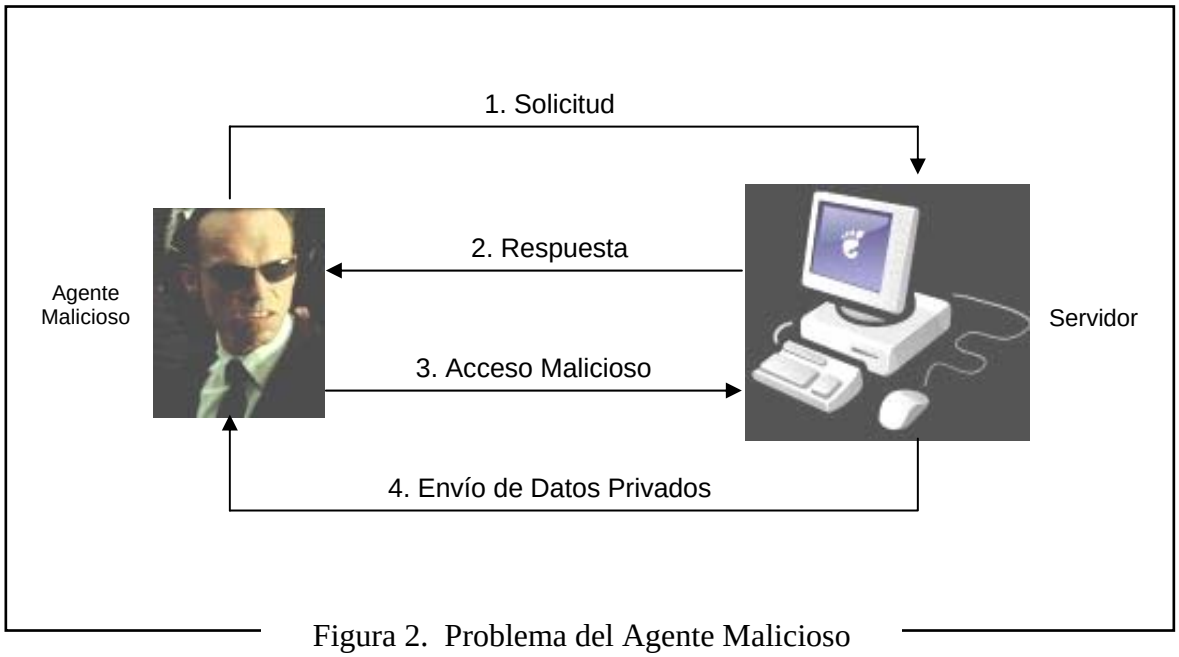

Figura 2. Problema del Agente Malicioso

3.1.2 El problema del Servidor Malicioso

Un servidor malicioso es aquel que podría espiar ó alterar el código y/o los datos de un agente, proporcionar llamadas falsas al sistema, retornar al agente datos no deseados, entre otros. En la figura 3 se ilustra un ataque de un servidor malicioso a un agente móvil.

Cuando el agente móvil llega al servidor, ya no depende de la máquina que lo envió, por lo tanto, el servidor receptor debe instanciar la clase que dio origen al agente, leer el estado de datos que se encuentra serializado y ejecutarlo, por lo que el código y datos del agente móvil quedan totalmente expuestos.

Los ataques de servidores contra agentes móviles se podrían clasificar de diversos tipos:

- **Clonación del Agente.** Uno de los ataques al agente móvil consiste en que un servidor lo captura y construye una réplica de él, de esa manera, se hace pasar por el agente original para los propósitos que ese programa residente en el servidor. En el caso de acceso a bases de datos se podría clonar un agente para robar información o alterar los datos.

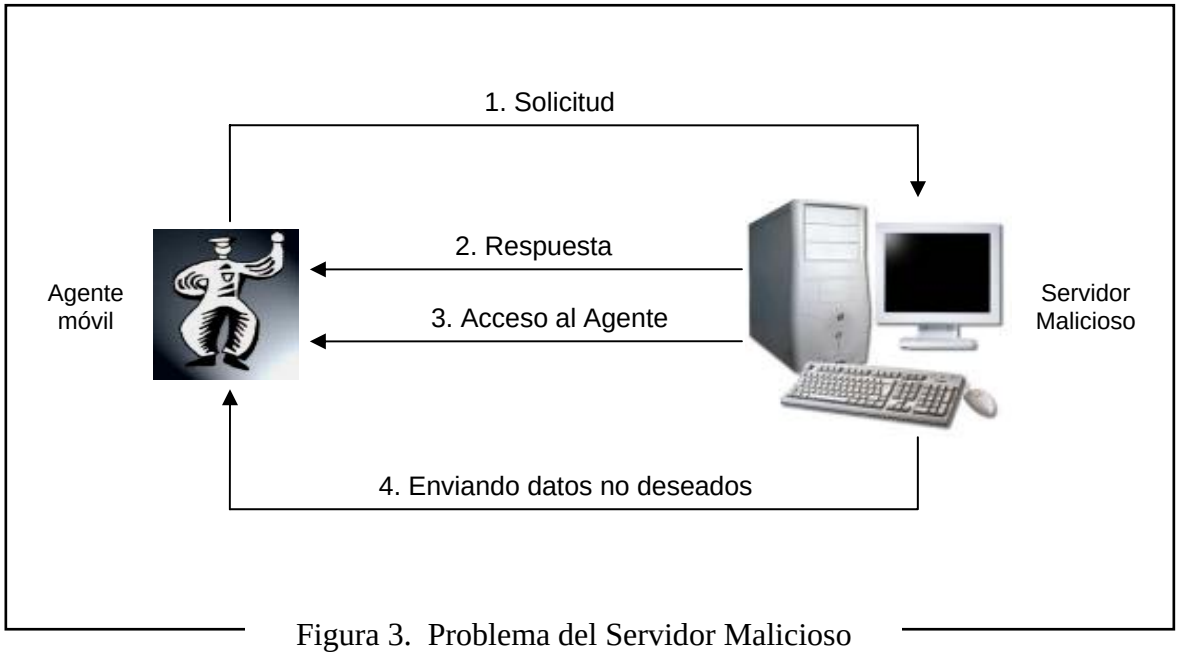

Figura 3. Problema del Servidor Malicioso

Los ataques de servidores contra agentes móviles se podrían clasificar de diversos tipos:

- **Clonación del Agente.** Uno de los ataques al agente móvil consiste en que un servidor lo captura y construye una réplica de él, de esa manera, se hace pasar por el agente original para los propósitos que ese programa residente en el servidor. En el caso de acceso a bases de datos se podría clonar un agente para robar información o alterar los datos.

- **Negación de servicio.** Los ataques de negación del servicio se pueden dar cuando el servidor impide que el agente continúe su itinerario o permitir al agente continuar, pero no al sitio que tiene determinado en el itinerario, sino a aquel que el servidor elija. En el caso de acceso a bases de datos un servidor podría hacer esperar al agente indefinidamente o desviarlo a una máquina no deseada.

- **El ataque del hombre en el medio.** Un agente móvil puede ser alterado e interceptado mientras se desplaza de una máquina a otra. Una manera de hacerlo es mediante el uso de un programa capaz de monitorear los agentes móviles pudiendo observar los mensajes intercambiados por ellos para extraer o modificar los datos. Con un ataque de este tipo se podrían capturar datos como passwords o información confidencial.

- **Modificación de los datos que lleva el agente.** Cuando un agente móvil se ejecuta en un servidor, este puede observar el contenido del agente, por tal motivo, si no se establecen los mecanismos de protección adecuados, un servidor malicioso puede alterar los datos que trae consigo el agente.

3.2 Problemas del acceso a bases de datos distribuidas con agentes móviles

Con el desarrollo que ha tenido Internet y las comunicaciones se incrementado exponencialmente el uso de bases datos distribuidas apareciendo los agentes móviles como una alternativa para mejorar el desempeño en este tipo de aplicaciones distribuidas. El modelo de agentes móviles va teniendo un mayor auge cada vez, tanto que existen en el mercado herramientas para crear agentes móviles, se cuenta con estándares, plataformas y productos que facilitan su desarrollo (como se expuso en el capitulo dos), pero debido a problemas de seguridad el acceso a bases de datos distribuidas mediante agentes móviles no ha tenido el auge esperado. Por tanto se hace necesario buscar soluciones para lograr un nivel de seguridad adecuado para proteger el acceso a las bases de datos y la forma de alcanzarlo es logrando mejorar aspectos de seguridad como son: la autenticación, autorización, confidencialidad e integridad.

3.2.1 Autenticación.

Mediante la autenticación un usuario asegura decir que es quién dice ser. Para lograr esta autenticación en el acceso a la base de datos distribuida el propio motor de la base de datos lo autentica por lo general con un login y password, que en algunos casos podrían ser utilizados métodos como: Identificación Biométrica, Documentos de Identificación y Firmas Digitales. El problema radica que login y passwords podrían viajar con los agentes y ser interceptados por agentes o programas maliciosos para violar el acceso a la base de datos.

3.2.2 Autorización.

Con la autorización se asegura que el usuario que va acceder a la información posea los permisos de seguridad o privilegios necesarios, para que la información en la red permaneciera privada. En una base de datos después que se autentica el usuario, este usuario posee unos permisos asignados por el administrador de la base de datos de acuerdo a los derechos o necesidades del usuario. Por lo tanto este problema ya no dependería de los agentes móviles sino del administrador de la base de datos que debe asignar los privilegios adecuados a los usuarios.

3.2.3 Confidencialidad

La confidencialidad asegura que ningún usuario sin los privilegios adecuados tenga acceso a la información. De igual manera que en la autorización se depende mucho del administrador de la base de datos, pero cuando los datos viajen con el agente se podría considerar un mecanismo de encriptación para proteger la confidencialidad de la información que viaja en la red.

3.2.4 Integridad

La integridad asegura que los datos sean consistentes y no hayan sido alterados. Los motores de bases de datos tienen sus propios mecanismos para proteger la integridad de los datos, labor que depende del administrador de la base de datos. Por lo tanto el sistema de agentes móviles también debe proporcionar mecanismos criptográficos para que los datos que transportan en la red no sean alterados.

4 Aglets

Uno de los principales marcos de trabajo para agentes Móviles, desarrolladas en Java, son los Aglets, creados por el equipo del laboratorio de desarrollo de IBM en Tokio. Un Aglet tiene una serie de estados que definen su funcionamiento. Los principales eventos en la vida de un Aglet son: Creación o Clonación; Liberación de recursos; Movilidad; y Persistencia (permite la desactivación y activación del Aglet).

El servidor crea un contexto para los Aglets. Allí serán insertados todos los Aglets que llegan al servidor, además tiene un monitor de red que permite monitorear la red buscando por otros Aglets, y un administrador de seguridad que protege al sitio (Figura 4).

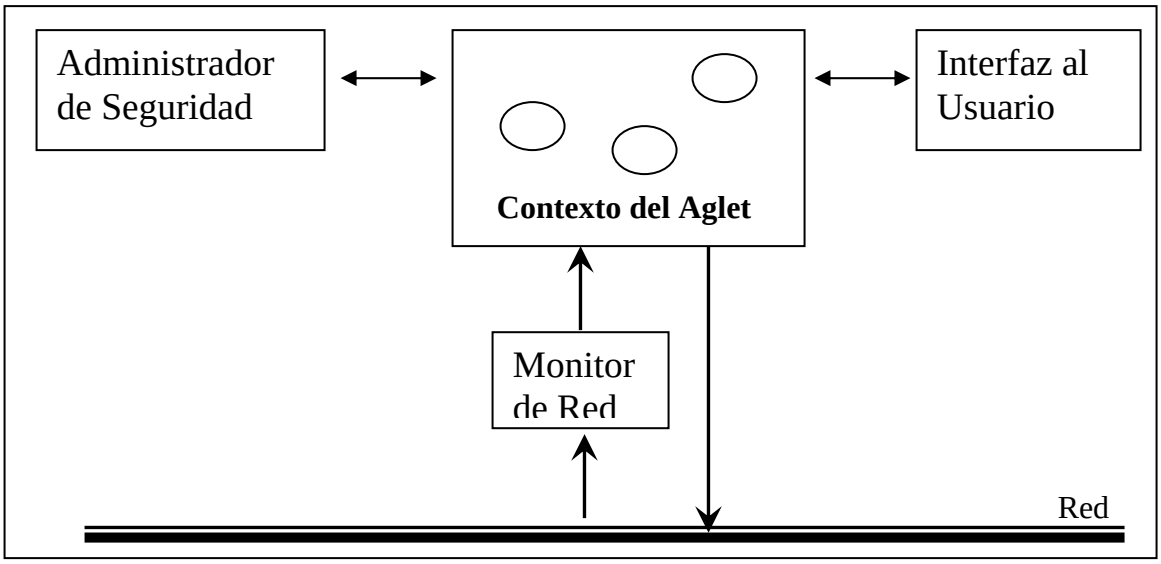

Figura 4. Contexto de los Aglets, Interfaz al usuario y Monitor de red.

La estructura definida en los Aglets permite que estos actúen autónomamente colaborando con otros Aglets. La colaboración es una necesidad en los agentes porque en general ninguno está aislado ni puede realizar tareas complejas solo. La movilidad y el paso de mensajes son características importantes para la colaboración.

Los Aglets no pueden migrar con su estado: memoria, pila de ejecución y registros, ya que están implementados en Java donde un programa no tiene acceso directo para manipular su estado (definido en el modelo de seguridad de la máquina virtual Java - JVM). Por lo tanto, cuando el Aglet va a ser transferido, debe almacenar todo lo necesario para luego retomar su estado cuando es reactivado, esto es llamado movilidad débil.

Al utilizar los Aglets, se tiene un modelo de fácil comprensión para la programación de agentes móviles sin tener que hacer modificaciones en la máquina virtual de Java o código nativo. También se tiene el soporte de una comunicación dinámica que permite a los agentes comunicarse con otros agentes tanto conocidos como desconocidos. Además, se proveen mecanismos de

seguridad que son de fácil comprensión y lo suficientemente simples para permitir que los usuarios finales puedan especificar una serie de restricciones de acceso a los agentes móviles.

5 Base de Datos de Prueba: SQL Server 2000

Se escogió SQL Server 2000 para gestionar la base de datos por brindar las condiciones para realizar la fragmentación y réplicas, se instaló sobre el sistema operativo Windows 2000 Server para realizar las transacciones de prueba con ABADAM.

6 Modelo Propuesto

Después de haberse analizado los aspectos concernientes a los agentes móviles y los problemas de seguridad que estos conllevan se presentará en esta sección un modelo de seguridad para el sistema de agentes móviles que acceden a una base de datos distribuida, además de brindar un proceso que colabore en la autenticación de los usuarios que quieren acceder al servidor de base de datos. El sistema propuesto está conformado por un sistema de agentes móviles, un modelo de seguridad y la base de datos (Figura 5).

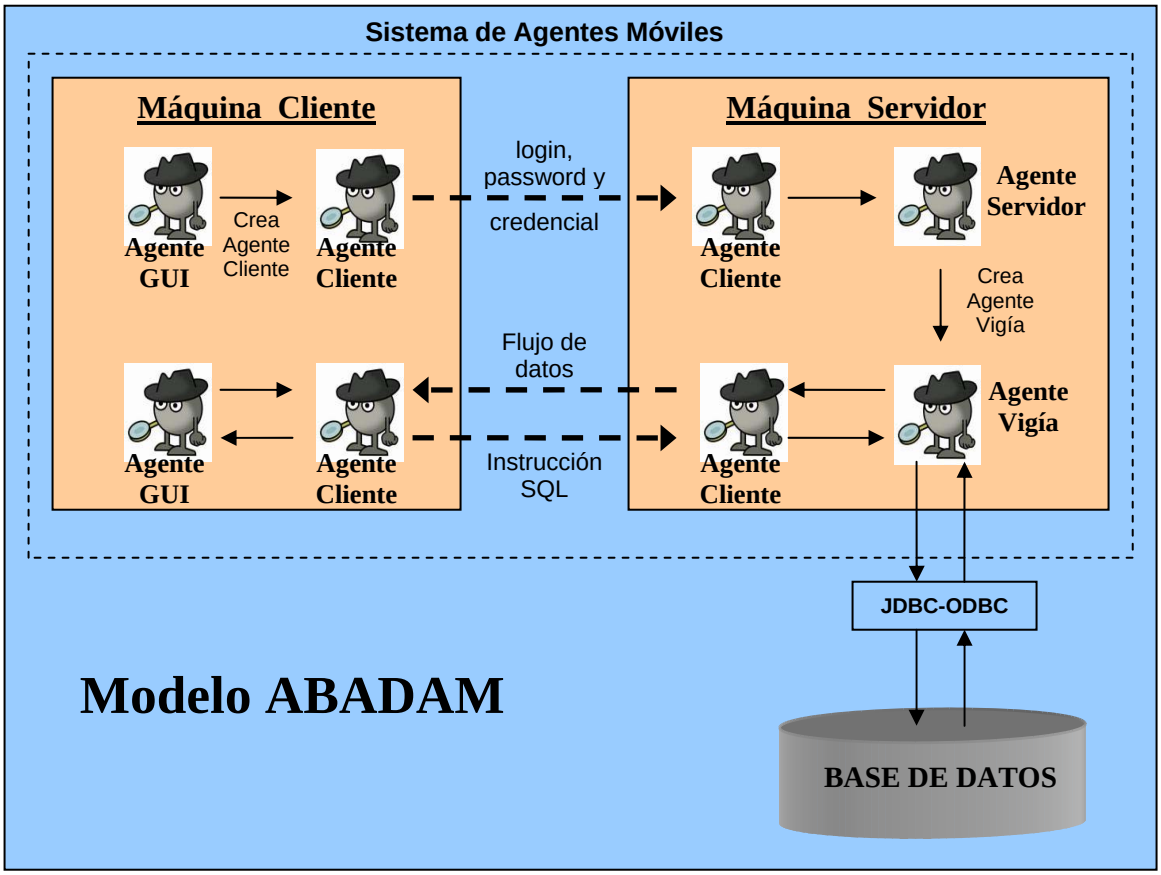

Figura 5. Modelo Propuesto ABADAM

6.1 Sistema de agentes móviles

El sistema de agentes móviles propuesto en este proyecto está clasificado de la siguiente forma:

- **Agente GUI**. La interfaz gráfica del usuario de ABADAM es invocada por el agente GUI que consiste en un agente estacionario y permite al usuario digitar su usuario, contraseña y dirección IP del servidor. Estos datos son entregados al agente móvil cliente para que se conecte a la base de datos, si el agente cliente regresa con éxito de la conexión se le solicitará que proceda a la captura de la instrucción SQL para realizar la operación deseada en la base de datos y desplegar los resultados de la transacción.

- **Agente Servidor**. El agente servidor es un agente estacionario ubicado en la máquina donde se encuentra la base de datos, este agente tiene la función de crear un agente vigía por cada agente cliente válido que llegue al servidor a establecer una sesión con la base de datos.

- **Agentes clientes**. El agente cliente es un agente móvil que creado por la interfaz del usuario y se comunica con el agente servidor, el cual le asigna un agente vigía con quien tratará el cliente mientras dure la sesión.

- **Agentes vigías**. El agente vigía es un agente estacionario creado por el agente servidor por cada agente cliente valido que llegue al servidor. Este agente vigía tiene la función de comunicarse con el agente cliente mientras dure la sesión del usuario para se de el intercambio de mensajes entre el cliente y el servidor.

Por cada usuario conectado a la base de datos del servidor, existirá un agente móvil cliente y por consiguiente existirá un agente vigía por cada agente cliente. De la misma manera si un usuario cierra su sesión o interfaz se destruirá el agente cliente y vigía correspondiente a ese usuario.

6.2 Modelo de Seguridad

El modelo de seguridad propuesto en ABADAM brinda un alto nivel de seguridad para proteger al servidor de base de datos de agentes maliciosos dando solución al problema del agente malicioso expuesto en la sección 3.1.1 debido a que solo tendrán acceso aquellos agentes válidos o confiables. El agente servidor será capaz de detectar agentes no válidos y los considerará como agentes maliciosos, los cuales eliminará en el mismo instante que lleguen al servidor.

Además ABADAM brinda un componente adicional de seguridad convirtiéndose también en un proceso colaborador en la autenticación de los usuarios, ya que si algún usuario mal intencionado o hacker, creara un agente móvil cliente y porte un login y password valido no podrá realizar la autenticación al no portar la credencial que lo acredite como un agente cliente confiable y será destruido inmediatamente.

El Sistema de agentes propuesto en este proyecto evita que agentes no deseados o malintencionados lleguen al servidor, con lo cual elimina cualquier posibilidad de que el servidor colapse por sobrecarga de agentes no válidos.

Los aspectos descritos resaltan claramente el nivel de seguridad brindado por el Sistema de Agentes de este proyecto, además de mejorar el rendimiento de la red al no mantener canales

constantes entre cliente y servidor, aspecto que no es fácilmente manejado en la forma tradicional de comunicación cliente servidor.

6.3 Base de Datos

La base de datos con la que se probó el sistema de agentes de este proyecto se describió en la sección 5. El agente vigía es el que se conecta a la base de datos mediante el ODBC creado en el servidor de base de datos.

A pesar que en este proyecto se trabajó con el motor de MS-SQL Server, el sistema de agentes está diseñado para adaptarse a cualquier motor de base de datos, basta con configurar el ODBC apropiado.

7 Conclusiones

En ABADAM los usuarios que desean conectarse a la Base de Datos lo hacen mediante el sistema de agentes móviles que brinda un alto nivel de seguridad contra ataques de otros agentes porque aunque un agente malicioso obtuviese un login y password validos para conectarse a la base datos, no lo lograría al no tener la credencial que lo amerite como agente de ABADAM.

El alto nivel de seguridad se extiende también al no permitir el alojamiento de agentes no deseados o maliciosos en el servidor porque serán destruidos en el mismo instante que lleguen al servidor, esto también evita que el sevidor sea colapsado por la llegada de agentes no deseados.

El modelo propuesto además de brindar un alto nivel de seguridad ofrece un mecanismo colaborativo en el proceso de autenticación del usuario porque al no permitir que usuarios se conecten directamente a la base de datos desde una fuente confiable, el motor de la base de datos estaría más descargado. Esto no sucede en algunos sistemas tradicionales en los cuales muchos usuarios no autorizados tratan de establecer contacto con el servidor de la base de datos produciendole a este consumo de recursos innecesarios.

ABADAM se convierte en una herramienta útil porque permite al usuario conectarse a cualquier base de datos mediante un driver ODBC, sea distribuida o no, y ejecutar cualquier instrucción SQL sobre la Base de Datos que se desee conectar.

Las aplicaciones donde se puede implementar este modelo no solo se limitan al aspecto de seguridad, sino que además, ABADAM al no tener ocupado el canal de cominicaciones permanentemente mientras se está conectado a la base de datos ofrece un mayor rendimiento en la red institucional, sobre todo en redes donde hay demasiado tráfico, como es el caso de instituciones que además de soportar el tráfico de datos de las aplicaciones empresariales también tienen que soportar el tráfico exagerado que producen los usuarios conectados a Internet navegando y descargando archivos.

Referencias

[1] FRITZ, Hohl. An approach to solve the problem of malicious hosts in mobile agent systems. Institute of parallel and distributed systems, University of Stuttgart. Alemania. 1997.

[2] LANGE, Danny y OSHIMA, Mitsuru.Programming and Deploying Java Mobile Agents with Aglets. Addison Wesley. 1998. p.17.

[3] LANGE, Danny. Mobile Agents: Enviroments, Technologies, and applications. Proceedings of the Practical Applications of intelligent Agents and Multi-Agent Technology Conference, PAAM98. 1998.

[4] BILL, Venners. Solve real problems with aglets, type of mobile agent. JavaWorld – Under the hood Magazine. Mayo 1997. Pág. 2-4.

[5] MAN, Mo y WEI V. A Taxonomy for Attacks on Mobile Agent. IEEEXplore. EUROCON'2001 Trends in Communications, International Conference. Volumen 2. p. 385-388. 2001.

[6] BORSELIUS, Niklas. Mobile agent security. Electronics & Communication Engineering Journal. Volumen 14. p. 211-218. 2002.

[7] LANGE, Danny y OSHIMA, Mitsuru. Programming and Deploying Java Mobile Agents with Aglets. Addison-Wesley. 1998.