UCUENCA

UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

COMPUTACIÓN

Trabajo Final - Diseño de Sistema Multiagente de Correo Electrónico

Autor:

Bryan Steven Mendoza Barahona

David Patricio Romero Alemán

Asignatura: Sistemas Multiagentes

Docente: Ing. Otto Parra

Fecha de entrega: 13/07/2025

Diseño de Sistema Multiagente para Correo Electrónico

1. Contextualizar el problema

El correo electrónico es uno de los medios de comunicación más utilizado. A diario se envían y reciben millones de mensajes que contienen desde simples notificaciones hasta información confidencial. A pesar de su popularidad y utilidad, el correo electrónico presenta múltiples desafíos relacionados con la seguridad, fiabilidad, detección de amenazas, eficiencia en la entrega y gestión autónoma de operaciones.

Además, los sistemas tradicionales de correo dependen en gran medida de arquitecturas monolíticas o centralizadas, que presentan limitaciones frente a entornos distribuidos, adaptativos y dinámicos. Amenazas como phishing, spam, suplantación de identidad, acceso no autorizado, o fallas en la entrega siguen afectando a millones de usuarios diariamente, lo que evidencia la necesidad de soluciones más inteligentes, autónomas y resilientes.

En este contexto, este sistema multiagentes (MAS) ofrece una alternativa poderosa y flexible para abordar estos retos, el cual incorpora diversos agentes que colaboran para alcanzar metas comunes. Cada agente se encarga de una tarea crítica: autenticación, cifrado, detección de amenazas, enrutamiento, recepción o notificación. Logrando mejorar la eficiencia, la capacidad de adaptación y la tolerancia a fallos del sistema.

2. Identificación de Agentes

Número	Agente	Descripción
1	Agente de Autenticación	Se encarga de verificar la identidad de los usuarios durante el inicio de sesión, gestionar credenciales (como contraseñas o autenticación de dos factores). También detecta intentos de acceso sospechosos.
2	Agente de Envío de Correos	Gestiona la preparación y validación de los mensajes de correo antes de su envío. Verifica que los campos obligatorios estén completos, válidos, formato adecuado y cumplan con las políticas de seguridad. Posteriormente envía el correo al servidor SMTP del dominio del remitente.
3	Agente Criptográfico	Protege la confidencialidad e integridad de los mensajes aplicando técnicas de cifrado, usando TLS. Para ello usará algoritmos como AES, ECDHE y SHA-256.

4	Agente de Enrutamiento	Dirige los correos electrónicos a través de la red, seleccionando la ruta más eficiente y confiable desde el servidor emisor hacia el servidor del destinatario. Consulta registros DNS para identificar el servidor de correo correcto.
5	Agente de Detección de Amenazas	Analiza los correos entrantes y salientes en busca de spam, phishing, malware u otras actividades maliciosas. Utiliza filtros basados en reglas, listas negras y aprendizaje automático para identificar patrones sospechosos y tomar acciones.
6	Agente de Recepción de Correos	Gestiona la sincronización de los correos al buzón del destinatario entre el servidor y los clientes de correo mediante IMAP, asegurando que el buzón del destinatario se mantenga actualizado y consistente.
7	Agente de Notificación	Informa a los usuarios sobre la llegada de nuevos correos, fallos en la entrega o alertas de seguridad. Personaliza las notificaciones según las preferencias del usuario.

Tabla 1: Descripción de los agentes

3. Definición del modelo PEAS para cada agente

- **Agente de Autenticación**
  - **Performance**: Cantidad de falsos positivos que acceden a la cuenta, tiempo de respuesta.
  - **Environment**: Login de la página web/móvil o aplicación, base de datos de datos.
  - **Actuators**: Avisos de contraseña incorrecta, tokens de sesión, bloqueo de IPs tras múltiples intentos fallidos.
  - **Sensors**: Datos del usuario (contraseña y dirección de correo), dirección IP.

- **Agente de Envío de Correos**
  - **Performance:** Mensajes enviados correctamente, número de errores de procesamiento por formato del mensaje, tiempo de envío.
  - **Environment:** Interfaz de redacción de los correos, servidor SMTP.
  - **Actuators:** Avisos de rechazo o datos incorrectos (archivo muy grande, dirección del destinatario inexistente, dominio inexistente, asunto vacío)
  - **Sensors:** Campos de asunto del correo, destinatario, archivos adjuntos, cuerpo.

- **Agente Criptográfico**
    - **Performance:** Tasa de fallos del cifrado/firmado. Nivel de confidencialidad e integridad del mensaje.
    - **Environment:** Correos electrónicos.
    - **Actuators:** Algoritmos de seguridad para cifrado (AES), intercambio de claves (ECDHE) y firmado hash (SHA-256).
    - **Sensors:** Estado del mensaje, existencia de claves de cifrado.

- **Agente de Enrutamiento.**
    - **Performance:** Latencia, tasa de entregas exitosas al servidor destino.
    - **Environment:** Internet (red de servidores).
    - **Actuators:** Consultas al DNS, establecer conexión con el servidor destino.
    - **Sensors:** Dominio del destinatario, respuesta del DNS, estado de los servidores.

- **Agente de Detección de Amenazas**
    - **Performance:** Tasa de detección de amenazas (spam, malware), tasa de falsos positivos.
    - **Environment:** Correos entrantes, listas negras, historial de correos maliciosos.
    - **Actuators:** Bloquear remitente, marcar mensaje como sospechoso, alertar al usuario.
    - **Sensors:** Contenido del correo, dirección IP y dominio del remitente, patrones anómalos.

- **Agente de Recepción de Correos.**
    - **Performance:** Sincronización correcta y completa, tiempo de sincronización.
    - **Environment:** Servidor IMAP, buzón del destinatario.
    - **Actuators:** Descargar correos del servidor, actualizar estado de cada correo (leído, sin leer, archivado)
    - **Sensors:** Nuevos correos, preferencias del usuario, estado del servidor IMAP.

- **Agente de Notificación**
    - **Performance:** Notificaciones relevantes, nivel de atención del usuario.
    - **Environment:** Bandeja de entrada, interfaz del usuario (web/móvil)
    - **Actuators:** Alertas y mensajes emergentes.
    - **Sensors:** Nuevos correos, fallos de entrega y preferencias del usuario.

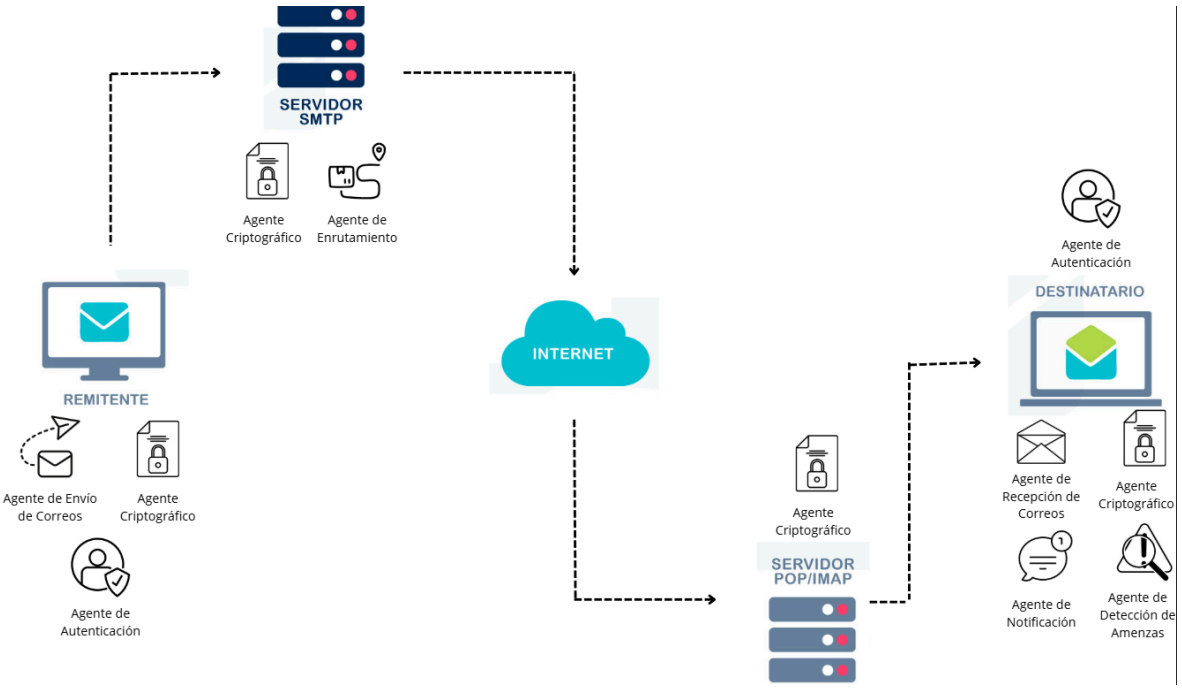

Figura 1: Diagrama de agentes del sistema de correo electrónico

4. FC-MAS

Para este MAS, se usa el framework de componentes para Sistemas Multiagentes (FC-MAS) para diseñar la estructura general del sistema de correo electrónico y comprender de mejor manera la integración de los componentes. FC-MAS se basa en 5 capas principales, las cuales están descritas a continuación y acopladas para el sistema actual. Adicionalmente, se muestra el esquema de cada capa usando FC-MAS en la Figura 2.

a. Capa de red física

Esta capa establece la estructura lógica de comunicación entre los agentes del sistema de correo electrónico, donde cada uno actúa como un nodo autónomo con roles definidos (autenticación, envío, cifrado, enrutamiento, etc.). La interconexión entre ellos se realiza mediante enlaces lógicos sobre redes IP, utilizando protocolos estándar como SMTP (para el envío), IMAP/POP3 (para la recepción) y TLS (para seguridad).

La topología empleada es distribuida y estructurada, evitando un nodo central y permitiendo que los agentes interactúen directamente según los requerimientos del flujo de trabajo. Logrando escalabilidad, descentralización y resistencia a fallos.

Todos los agentes operan en una red donde intercambian correos, comandos de control y datos de seguridad. Las conexiones son punto a punto, activándose bajo demanda según eventos o solicitudes durante el ciclo de vida del mensaje.

b. Capa de Sincronización

Esta capa se encarga de coordinar el trabajo conjunto entre los agentes para que el sistema de correo electrónico funcione de manera eficiente y segura. Los agentes intercambian información clave como mensajes, metadatos, claves efímeras para cifrado simétrico, firmas digitales para verificar la autenticidad, códigos hash SHA-256 para garantizar la integridad de los datos, y alertas de seguridad cuando detectan posibles amenazas o fallos en el sistema.

La colaboración entre agentes se organiza mediante grupos dinámicos que se forman según la tarea a realizar. Por ejemplo, cuando un correo necesita ser enviado al servidor del destinatario, los agentes de envío, cifrado y enrutamiento trabajan juntos para validar el mensaje, proteger su contenido y asegurar que llegue a su destino. De manera similar, cuando llega un nuevo correo, los agentes de recepción y notificación cooperan para almacenarlo correctamente y avisar al usuario.

Cada agente tiene un rol específico y permanente dentro del sistema, pero solo se activa cuando recibe una señal o mensaje relacionado con su función. Además, para acciones críticas como entregar un correo, los agentes requieren aprobación mutua.

c. Capa de Controlador de red

Esta capa establece cómo se gestiona el flujo de operaciones y las decisiones dentro del sistema. Cada agente funciona de manera autónoma, siguiendo algoritmos distribuidos que le permiten validar datos, activar otros agentes o incluso detener procesos cuando sea necesario.

La arquitectura de control combina elementos centralizados y distribuidos. El acceso inicial está centralizado en el Agente de Autenticación, que actúa como punto único de entrada, pero el resto de las decisiones se toman de forma descentralizada, permitiendo que cada agente opere según su lógica y responsabilidades específicas.

Además, esta capa incluye funciones de evaluación y supervisión en tiempo real. El Agente de Enrutamiento, por ejemplo, determina la mejor ruta para enviar un correo mediante consultas DNS, mientras que el Agente de Amenazas calcula el nivel de riesgo de un mensaje utilizando filtros heurísticos y listas negras. El sistema también monitorea constantemente el comportamiento de los agentes y la red, detectando posibles anomalías que puedan afectar el rendimiento o la seguridad.

d. Capa de Evaluación

Esta capa monitorea el sistema analizando datos operativos para garantizar su correcto funcionamiento, integridad y seguridad. El Agente de Detección de Amenazas es el principal en esto, examinando mensajes para identificar spam, malware, phishing u otras anomalías mediante reglas predefinidas, listas negras y algoritmos básicos de aprendizaje automático.

Esta supervisión detecta comportamientos sospechosos como intentos fallidos de autenticación repetidos, envíos masivos inusuales o mensajes con estructuras anómalas. Según los hallazgos, los agentes actúan de forma autónoma: bloqueando correos peligrosos, marcando elementos

sospechosos, permitiendo el tráfico legítimo, generando alertas o notificando al usuario cuando sea necesario.

e. **Capa de Tolerancia a fallos**

Esta capa permite que el sistema se mantenga en funcionamiento aunque ocurran errores o condiciones inesperadas. Cada agente incluye mecanismos para detectar fallos tanto internos como externos.

Por ejemplo, el agente de recepción puede detectar errores en la sincronización del buzón o fallas del servidor IMAP, mientras que el agente de enrutamiento puede identificar fallas de resolución DNS o tiempos de espera prolongados.

El sistema cuenta con mecanismos de robustez que permiten continuar operando aunque uno o más agentes fallen temporalmente. Además, implementa resiliencia mediante reintentos automáticos de envío, notificación de fallos al usuario, y reconfiguración dinámica de tareas para redirigir procesos a agentes disponibles.

Todo esto, logra dar una buena experiencia de uso a los usuarios del servicio de correo electrónico.

Figura 2: Esquema FC-MAS para el sistema de correo electrónico