Correo Electrónico Seguro Empleando Infraestructura de Terceros

Juan Camilo Corena Bossa

Politécnico Grancolombiano

ACIS

Motivación

- El correo electrónico es un activo vital en las comunicaciones de las empresas.
- Tener una infraestructura propia con alta disponibilidad es algo costoso en términos de equipos y personal.
- Servicios gratuitos como Gmail o Hotmail son una alternativa económica para solucionar el problema. Sin embargo esta alternativa le brinda a terceros acceso a información confidencial.

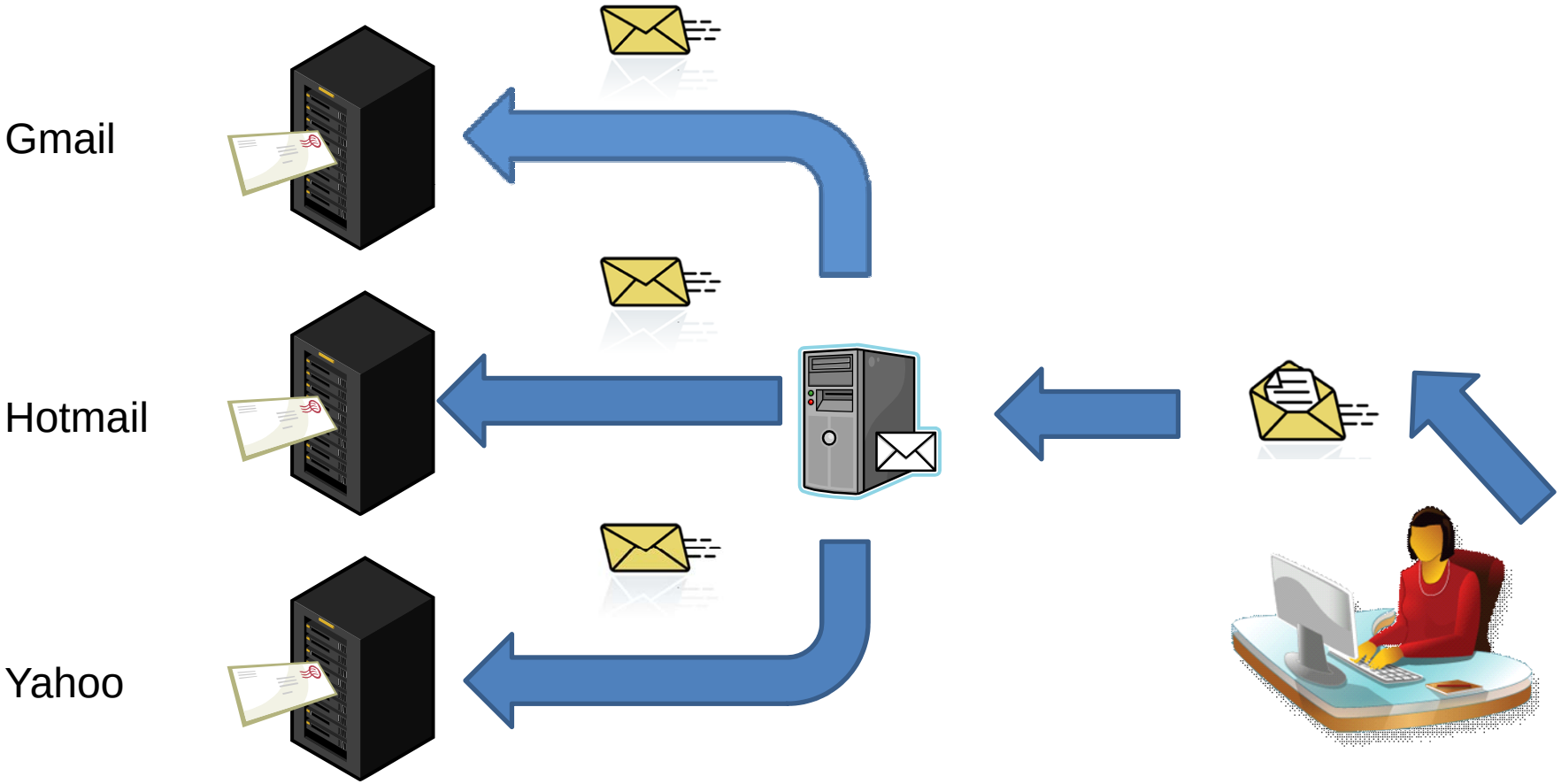
ACIS

Escenarios de Uso

- Usuarios finales y empresas que deseen mantener su información segura.
- Servicios de correo que deseen ofrecer almacenamiento anónimo de información: Hushmail.
- Servicios de almacenamiento de información: RapidShare, MediaFire.

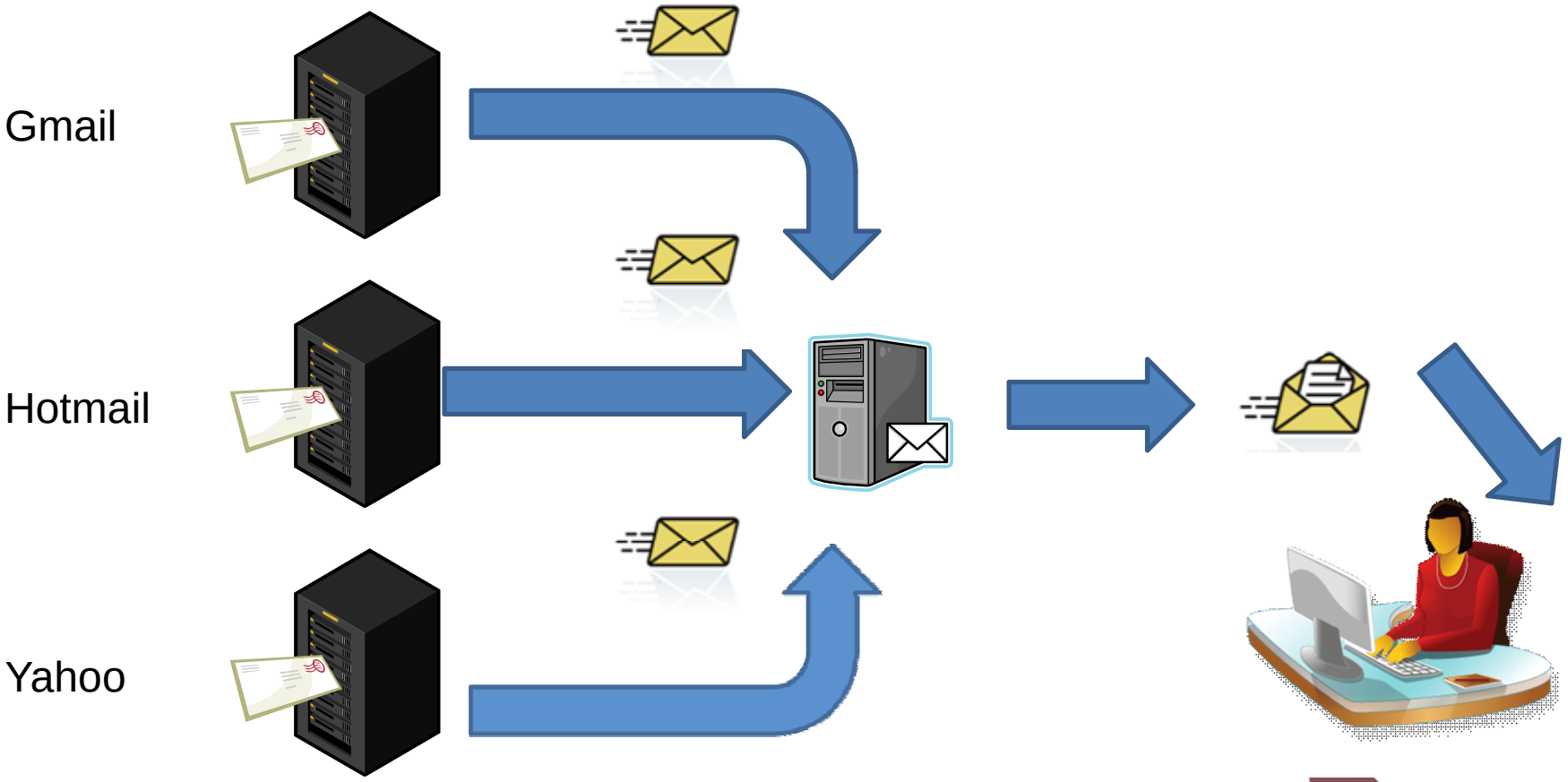
ACIS

Esquema Propuesto de Envío



ACIS

Esquema Propuesto de Recepción



ACIS

Formato de los Mensajes para Envió y Recepción

Estructura de los datos del correo:

$$m_i.data = A(E_{P_r}(k), E_k(m.data, E_{S_p}(H(m.data))))$$

Datos enviados:

$$(m_i.header, m_i.data)$$

A(x)=Convierte a x en base 64.
Epk(x)=Cifra x con la llave pública de p.
Ek(x)=Cifra x con la llave simétrica k.
H(x)=Obtiene el hash de x.
m.data=Datos del mensaje original.
m.data=Cifrado de los datos del mensaje original.

ACIS

Ventajas

- Ahorro de costos.
- Mejora de disponibilidad.
- Almacenamiento de informacion segura.
- Transparencia de uso para el usuario final.

ACIS

Términos de Servicio de los Proveedores de Correo

- Los términos de servicio de varios proveedores no hacen referencia explícita a la prohibición del uso de criptografía en los archivos adjunto.
- Las pruebas preliminares han sido exitosas, ya que los mensajes no han sido filtrados ni borrados.

ACIS

Conclusiones

- Se ha presentado un esquema para uso de seguro de correo electrónico que salvaguarda la confidencialidad, integridad y disponibilidad de la información incluso sobre infraestructura provista por terceros.
- Adicionalmente el sistema es compatible con la base instalada.

ACIS