Web-Based Mail & Email Security

Introduction to Email Types

✓ Traditional Email

✓ Web-Based Email

What is Web-Based Email?

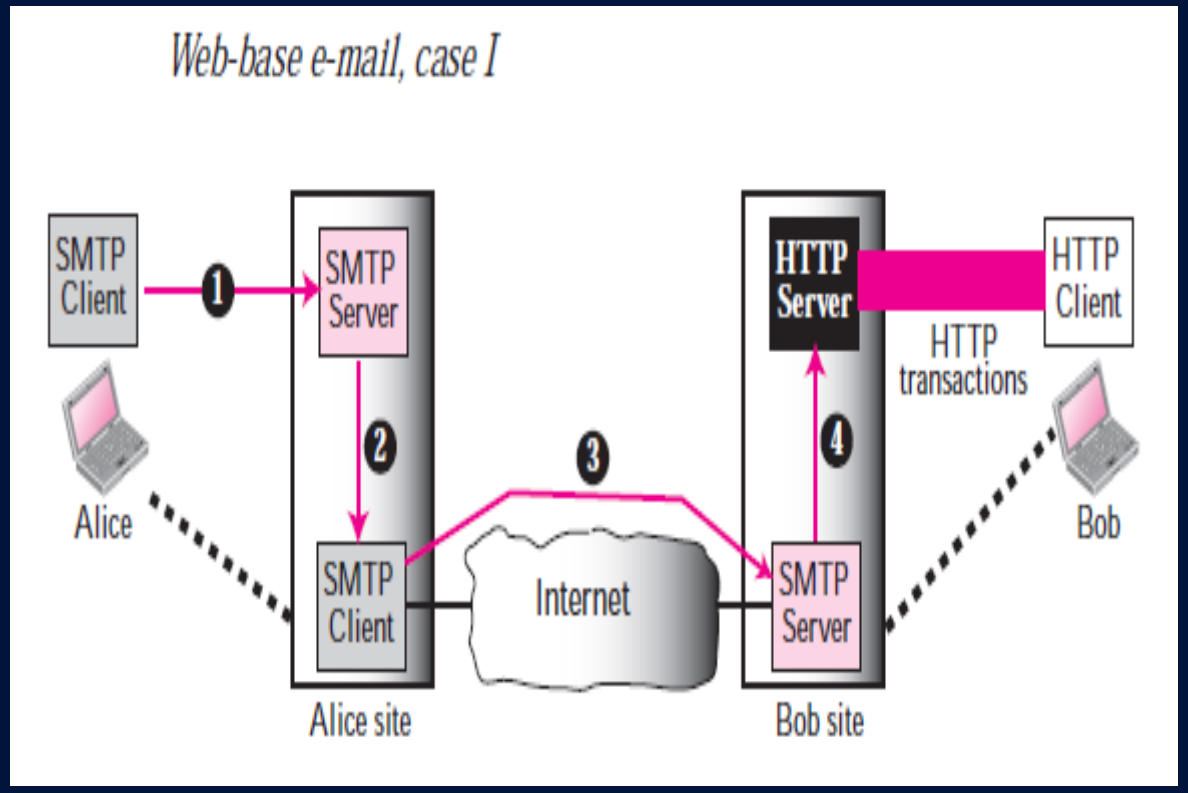
Access emails via web browser

No software installation required

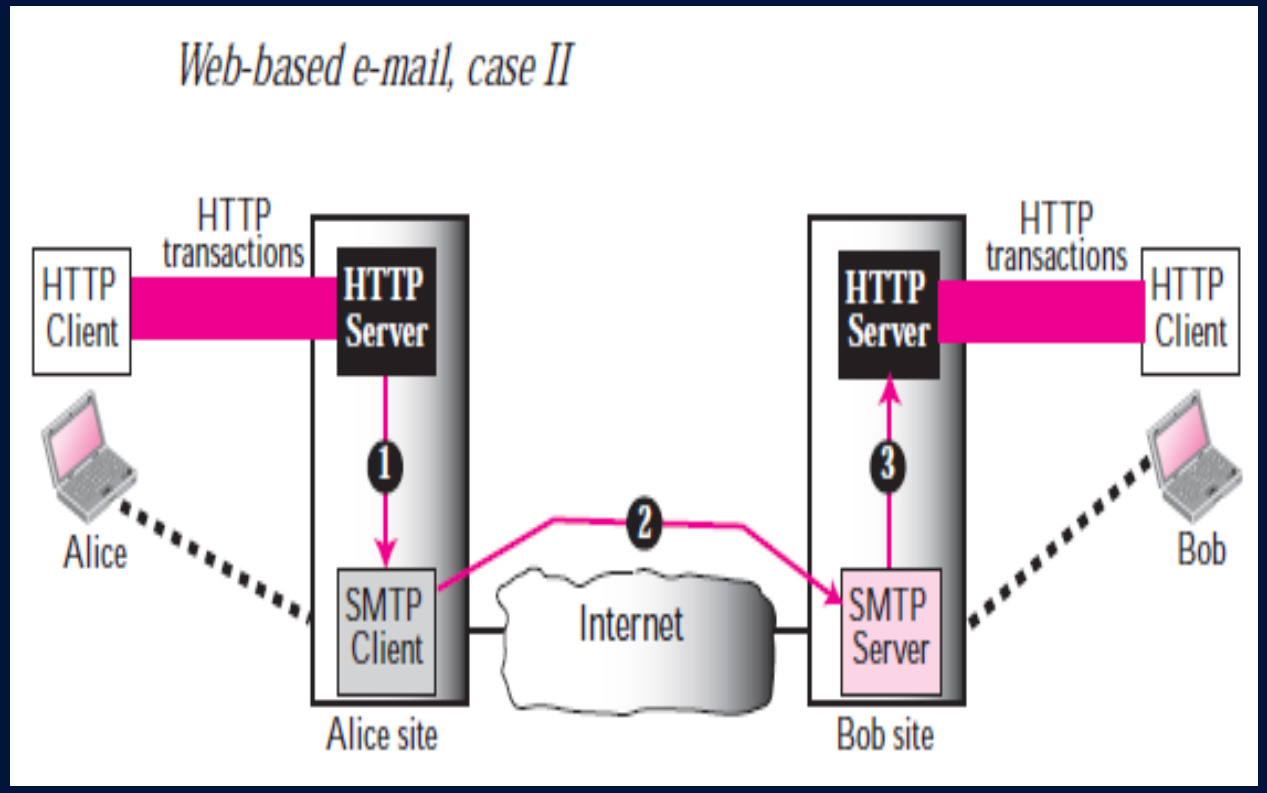
Accessible from any device, anytime, anywhere with internet

Examples: Gmail, Yahoo Mail, Outlook.com

Architecture Of Web-Based Email



Case I: Half Web-Based Email
(Only the receiver uses webmail — sender uses a normal email client)



Case II: Fully Web-Based Email
(Both sender and receiver use webmail through browsers)

Working & Key Components

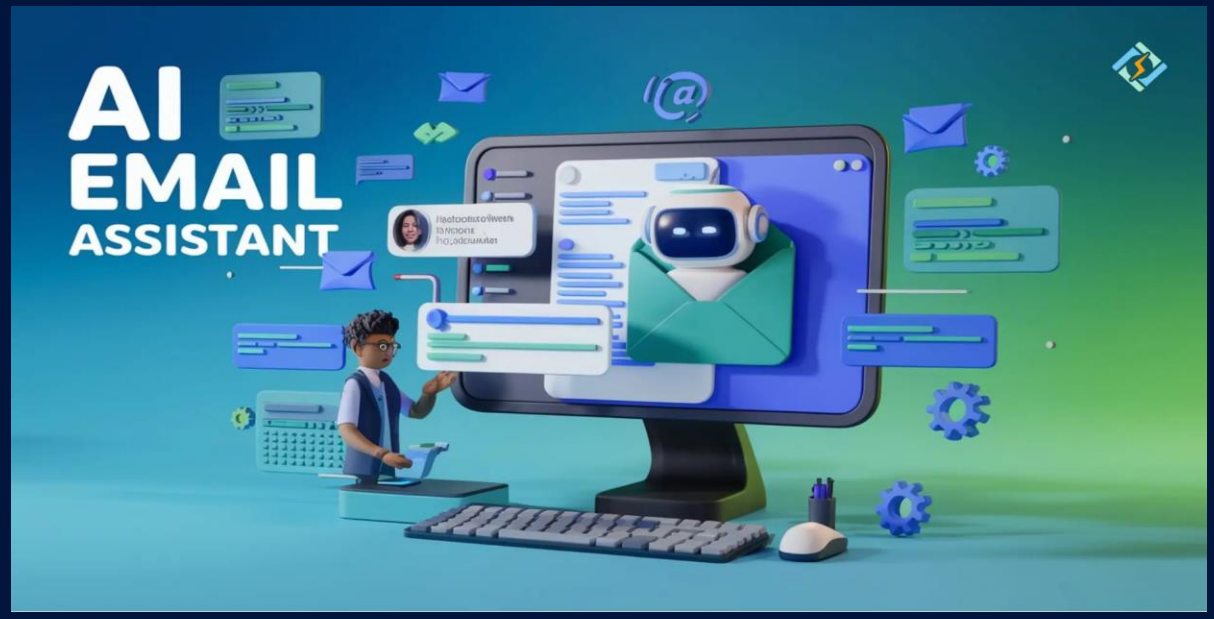
- User Interface: For login, composing, reading, and managing emails.
- Web Server: Stores and delivers mail pages that are sent or received.
- Email Server: Sends and receives emails using SMTP and POP/IMAP.
- Database: Keeps user details, emails, and attachments safely.
- Security Layer: Protects data and login through encryption.

Advantages

- Web-Based Access
- Zero Setup
- Auto updates & backups
- Cloud mail & Storage
- Seamless app integration

Challenges

- Limited offline features.
- Requires active internet connection.
- Privacy and data protection concerns.



Future Trends

- AI for smart replies and spam detection.
- Machine Learning for automatic email categorization.
- Progressive Web Apps (PWAs): Provide desktop-like experience in browser.

Email Security

- Protects emails & attachments from unauthorized access or tampering
- Involves spam filtering, malware detection, encryption, user awareness
- Phishing causes nearly 80% of security incidents, with an estimated $17,700 loss per minute.
- Ensures confidentiality, integrity, and trust in communication.

Key Areas of Email Security

- Monitoring & Filtering
- Encryption & Authentication

Common Email Threats

- Phishing & Social Engineering
- Malware & Ransomware
- Business Email Compromise (BEC)
- Spam & Spoofing

How Email Security Works

- **Multi-layer defense:** Spam filters, link protection, attachment scans
- **Authentication protocols:** SPF, DKIM, DMARC verify senders
- **Encryption:** Protects message contents during transmission
- **Quarantine:** Suspicious emails held for admin review

Best Practices & Importance

- Follow MFA, strong passwords
- Avoid clicking unknown links or attachments
- Regular security audits & encryption of sensitive emails
- Builds compliance with laws (GDPR, HIPAA, etc..)

Thank You…