SOS POLITICAL SCIENCE AND PUBLIC ADMINISTRATION

MBA FA 401

SUBJECT NAME: COMPUTER APPLICATIONS IN FINANCIAL ADMINISTRATION

UNIT-V

TOPIC NAME: E- MAIL

Electronic mail (email or e-mail) is a method of exchanging messages ("mail") between people using electronic devices. Email first entered limited use in the 1960s, but users could only send to others who used the same computer, and some early email systems even required the author and the recipient to both is online at the same time, similar to instant messaging. Ray Tomlinson is credited as the inventor of email, as in 1971 he developed the first system able to send mail between users on different hosts across the ARPANET, using the @ sign to link the user name with a destination server. By the mid-1970s this had taken the form now recognized as email.

Email operates across computer networks, which today is primarily the Internet. Today's email systems are based on a store-and-forward model.

Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need to connect only briefly, typically to a mail server or a webmail interface for as long as it takes to send or receive messages or to download it.

Originally an ASCII text-only communications medium, Internet email was extended by Multipurpose Internet Mail Extensions (MIME) to carry text in other character sets and multimedia content attachments. International email, with internationalized email addresses using UTF-8, has been standardized but has not been widely adopted.

The history of modern Internet email services reaches back to the early ARPANET, with standards for encoding email messages published as early as 1973 (RFC 561). An email message sent in the early 1970s looks very similar to a basic email sent today.

TERMINOLOGY:

Historically, the term electronic mail was used generically for any electronic document transmission. For example, several writers in the early 1970s used the term to refer to fax document transmission. As a result, it is difficult to find the first citation for the use of the term with the more specific meaning it has today.

Electronic mail has been most commonly called email or e-mail since around 1993, but several variations of the spelling have been used:

- Email is now the most common form used, and recommended by style guides. It is the form required by IETF Requests for Comments (RFC) and working groups. This spelling also appears in most dictionaries.
- Email is the form that was favored in edited, published American English and British English writing as reflected in the Corpus of Contemporary American English data, but is falling out of favor in some style guides.
- Email is a traditional form that has been used in RFCs for the "Author's Address" and is expressly required "for historical reasons".
- E-mail is sometimes used, capitalizing the initial E as in similar abbreviations like E-piano, E-guitar, A-bomb, and H-bomb.

In the original protocol standard, RFC 524, none of these forms was used. The service is simply referred to as mail, and a single piece of electronic mail is called a message.

An Internet e-mail consists of an envelope and content; the content in turn consists of a header and a body.

ORIGIN:

Computer-based mail and messaging became possible with the advent of time-sharing computers in the early 1960s, and informal methods of using shared files to pass messages were soon expanded into the first mail systems. Most developers of early mainframes and minicomputers developed similar, but generally incompatible, mail applications. Over time, a complex web of gateways and routing systems linked many of them. Many US universities were part of the ARPANET (created in the late 1960s), which aimed at software portability between its systems. In 1971 the first ARPANET network email was sent, introducing the now-familiar address syntax with the '@' symbol designating the user's system address. The Simple Mail Transfer Protocol (SMTP) protocol was introduced in 1981.

For a time in the late 1980s and early 1990s, it seemed likely that either a proprietary commercial system or the X.400 email system, part of the Government Open Systems Interconnection Profile (GOSIP), would predominate. However, once the final restrictions on carrying commercial traffic over the Internet ended in 1995, a combination of factors made the current Internet suite of SMTP, POP3 and IMAP email protocols the standard.

USES:

A. BUSINESS AND ORGANIZATIONAL USE:

Email has been widely accepted by businesses, governments and non-governmental organizations in the developed world, and it is one of the key parts of an 'e-revolution' in workplace communication (with the other key plank being widespread adoption of high speed Internet). A sponsored 2010 study on workplace communication found 83% of U.S. knowledge workers felt email was critical to their success and productivity at work.

It has some key benefits to business and other organizations, including:

Facilitating logistics:

Much of the business world relies on communications between people who are not physically in the same building, area, or even country; setting up and attending an in-person meeting, telephone call, or conference call can be inconvenient, time-consuming, and costly. Email provides a method of exchanging information between two or more people with no set-up costs and that is generally far less expensive than a physical meeting or phone call.

Helping with synchronization:

With real time communication by meetings or phone calls, participants must work on the same schedule, and each participant must spend the same amount of time in the meeting or call. Email allows asynchrony: each participant may control their schedule independently.

Reducing cost:

Sending an email is much less expensive than sending postal mail, or long distance telephone calls, telex or telegrams.

Increasing speed:

Much faster than most of the alternatives.

Creating a "written" record

Unlike a telephone or in-person conversation, email by its nature creates a detailed written record of the communication, the identity of the sender(s) and recipient(s) and the date and time the message was sent. In the event of a contract or legal dispute, saved emails can be used to prove that an individual was advised of certain issues, as each email has the date and time recorded on it.

Email marketing**:**

Email marketing via "opt-in" is often successfully used to send special sales offerings and new product information. Depending on the recipient's culture, email sent without permission—such as an "opt-in"—is likely to be viewed as unwelcome "email spam".

B. PERSONAL USE:

Personal computer**:**

Many users access their personal emails from friends and family members using a personal computer in their house or apartment.

Mobile**:**

Email has become used on smart phones and on all types of computers. Mobile "apps" for email increase accessibility to the medium for users who are out of their homes. While in the earliest years of email, users could only access email on desktop computers, in the 2010s, it is possible for users to check their email when they are away from home, whether they are across town or across the world. Alerts can also be sent to the smart phone or other devices to notify them immediately of new messages. This has given email the ability to be used for more frequent communication between users and allowed them to check their email and write messages throughout the day. As of 2011, there were approximately 1.4 billion email users worldwide and 50 billion non-spam emails that were sent daily.

Individuals often check emails on smart phones for both personal and work-related messages. It was found that US adults check their email more than they browse the web or check their Face book accounts, making email the most popular activity for users to do on their smart phones. 78% of the respondents in the study revealed that they check their email on their phone. It was also found that 30% of consumers use only their smart phone to check their email, and 91% were likely to check their email at least once per day on their smart phone. However, the percentage of consumers using email on a smart phone ranges and differs dramatically across different countries. For example, in comparison to 75% of those consumers in the US who used it, only 17% in India did.

Declining use among young people:

As of 2010, the number of Americans visiting email web sites had fallen 6 percent after peaking in November 2009. For persons 12 to 17, the number was down 18 percent. Young people preferred instant messaging, texting and social media. Technology writer Matt Richtel said in The New York Times that email was like the VCR, vinyl records and film cameras—no longer do cool and something older people.

A 2015 survey of Android users showed that persons 13 to 24 used messaging apps 3.5 times as much as those over 45, and were far less likely to use email.

FEATURES OF EMAIL:

The many different features of email include:

- automatic reply to messages
- auto-forward and redirection of messages
- facility to send copies of a message to many people
- automatic filing and retrieval of messages
- addresses can be stored in an address book and retrieved instantly
- notification if a message cannot be delivered
- emails are automatically date and time stamped
- signatures can be attached
- files, graphics or sound can be sent as attachments, often in compressed formats
- webmail and mobile email can be used to receive and send messages while on the move

ISSUES IN Email:

1. **Attachment size limitation**:

Email messages may have one or more attachments, which are additional files that are appended to the email. Typical attachments include Microsoft Word documents, PDF documents and scanned images of paper documents. In principle there is no technical restriction on the size or number of attachments, but in practice email clients, servers and Internet service providers implement various limitations on the size of files, or complete email - typically to 25MB or less. Furthermore, due to technical reasons, attachment sizes as seen by these transport systems can differ to what the user sees, which can be confusing to senders when trying to assess whether they can safely send a file by email. Where larger files need to be shared, various file hosting services are available and commonly used.

2. **Information overload**:

The ubiquity of email for knowledge workers and "white collar" employees has led to concerns that recipients face an "information overload" in dealing with increasing volumes of email. With the growth in mobile devices, by default employees may also receive work-related emails outside of their working day. This can lead to increased stress, decreased satisfaction with work, and some observers even argue it could have a significant negative economic effect, as efforts to read the many emails could reduce productivity.

3. **Spam**:

Email "spam" is unsolicited bulk email. The low cost of sending such email meant that, by 2003, up to 30% of total email traffic was spam, and was threatening the usefulness of email as a practical tool. The US CAN-SPAM Act of 2003 and similar laws elsewhere had some impact, and a number of effective anti-spam techniques now largely mitigate the impact of spam by filtering or rejecting it for most users, but the volume sent is still very high—and increasingly consists not of advertisements for products, but malicious content or links. In September 2017, for example, the proportion of spam to legitimate email rose to 59.56%.

4. **Malware**:

A range of malicious email types exist. These range from various types of email scams, including "social engineering" scams such as advance-fee scam "Nigerian letters", to phishing, email bombardment and email worms.

5. **Email spoofing**:

Email spoofing occurs when the email message header is designed to make the message appear to come from a known or trusted source. Email spam and phishing methods typically use spoofing to mislead the recipient about the true message origin. Email spoofing may be done as a prank, or as part of a criminal effort to defraud an individual or organization. An example of a potentially fraudulent email spoofing is if an individual creates an email that appears to be an invoice from a major company, and then sends it to one or more recipients. In some cases, these fraudulent emails incorporate the logo of the purported organization and even the email address may appear legitimate.

6. **Email bombing**:

Email bombing is the intentional sending of large volumes of messages to a target address. The overloading of the target email address can render it unusable and can even cause the mail server to crash.

7. **Privacy concerns**:

Today it can be important to distinguish between the Internet and internal email systems. Internet email may travel and be stored on networks and computers without the sender's or the recipient's control. During the transit time it is possible that third parties read or even modify the content. Internal mail systems, in which the information never leaves the organizational network, maybe more secure, although information technology personnel and others whose function may involve monitoring or managing may be accessing the email of other employees.

Email privacy, without some security precautions, can be compromised because:

- Email messages are generally not encrypted.
- Email messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.
- Many Internet Service Providers (ISP) store copies of email messages on their mail servers before they are delivered. The backups of these can remain for up to several months on their server, despite deletion from the mailbox.
- The "Received:"-fields and other information in the email can often identify the sender, preventing anonymous communication.
- Web bugs invisibly embedded in email content can alert the sender of any email whenever an email is read, or re-read, and from which IP address. It can also reveal whether an email was read on a smart phone or a PC, or Apple Mac device via the user agent string.

There are cryptography applications that can serve as a remedy to one or more of the above. For example, Virtual Private Networks or the Tor anonymity network can be used to encrypt traffic from the user machine to a safer network while GPG, PGP, Steamily, or S/MIME can be used for end-to-end message encryption, and SMTP STARTTLS or SMTP over Transport Layer Security/Secure Sockets Layer can be used to encrypt communications for a single mail hop between the SMTP client and the SMTP server.

Additionally, many mail user agents do not protect logins and passwords, making them easy to intercept by an attacker. Encrypted authentication schemes such as SASL prevent this. Finally, the attached files share many of the same hazards as those found in peer-to-peer file sharing. Attached files may contain Trojans or viruses.

8. **Legal contracts**:

Emails can now often be considered as binding contracts as well, so users must be careful about what they send through email correspondence.

9. **Flaming**:

Flaming occurs when a person sends a message (or many messages) with angry or antagonistic content. The term is derived from the use of the word incendiary to describe particularly heated email discussions. The ease and impersonality of email communications mean that the social norms that encourage civility in person or via telephone do not exist and civility may be forgotten.

10. **Email bankruptcy**:

Also known as "email fatigue", email bankruptcy is when a user ignores a large number of email messages after falling behind in reading and answering them. The reason for falling behind is often due to information overload and a general sense there is so much information that it is not possible to read it all. As a solution, people occasionally send a "boilerplate" message explaining that their email inbox is full, and that they are in the process of clearing out all the messages. Harvard University law professor Lawrence Lessing is credited with coining this term, but he may only have popularized it.

11. **Internationalization**:

Originally Internet email was completely ASCII text-based. MIME now allows body content text and some header content text in international character sets, but other headers and email addresses using UTF-8, while standardized have yet to be widely adopted.

12. **Tracking of sent mail**:

The original SMTP mail service provides limited mechanisms for tracking a transmitted message, and none for verifying that it has been delivered or read. It requires that each mail server must either deliver it onward or return a failure notice (bounce message), but both software bugs and system failures can cause messages to be lost. To remedy this, the IETF introduced Delivery Status Notifications (delivery receipts) and Message Disposition Notifications (return receipts); however, these are not universally deployed in production. (A complete Message Tracking mechanism was also defined, but it never gained traction; see RFCs 3885 through 3888.

Many ISPs now deliberately disable non-delivery reports (NDRs) and delivery receipts due to the activities of spammers:

- Delivery Reports can be used to verify whether an address exists and if so, this indicates to a spammer that it is available to be spammed.
- If the spammer uses a forged sender email address (email spoofing), then the innocent email address that was used can be flooded with NDRs from the many invalid email addresses the spammer may have attempted to mail. These NDRs then constitute spam from the ISP to the innocent user.

In the absence of standard methods, a range of system based around the use of web bugs have been developed. However, these are often seen as underhand or raising privacy concerns, and only work with email clients that support rendering of HTML. Many mail clients now default to not showing "web content". Webmail providers can also disrupt web bugs by pre-caching images.

EMAIL SERVERS (SMTP AND MTA):

1. SMTP (SIMPLE MAIL TRANSFER PROTOCOL):

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

WORKING OF SMTP:

1. **Composition of Mail:** A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
2. **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
3. **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name. If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the

recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.

4. **Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
5. **Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

2. MTA (MESSAGE TRANSFER AGENT):

A message transfer agent or mail transfer agent (MTA) or mail relay is software that transfers electronic mail messages from one computer to another using SMTP. The terms mail server, mail exchanger, and MX host are also used in some contexts.

Messages exchanged across networks are passed between mail servers, including any attached data files (such as images, multimedia or documents). These servers also often keep mailboxes for email. Access to this email by end users is typically either via webmail or an email client.

MTA refers to Message Transfer Agent or Mail Transfer Agent. It is responsible for transferring and routing an Electronic-mail message from the sender's computer to the recipient's computer. Most probably, MTA receives emails from other MTA. A message transfer agent receives incoming emails and forwards the messages to individual clients/users. The main function of the MTA is forwarding the incoming message to the perfect end-user or destination. Microsoft Exchange and UNIX send mail are good examples of MTAs.

How MTAs work:

An MTA is just an element of the email delivery process. It receives an email from the mail/message submission agent (MSA), which, in turn, receives it from the mail user agent (MUA). The MUA is commonly known as an email client – an app you use to handle the email-related stuff.

Once the MTA gets the email, relaying comes into play. That's why mail transfer agents are often called mail relays. Check out our blog post about SMTP relay if you’re interested in details. The email can be forwarded to other MTAs if the recipient is not hosted locally. Then it hits the mail delivery agent (MDA). This is the email’s last stopover before it will be delivered to the recipient’s mailbox. The email sending is carried out using SMTP (or extended SMTP), and for the final stage (MDA to MUA), POP3 or IMAP4 is used. For more on differences between these e mails protocols, read SMTP vs. IMAP vs. POP3.

To sum up, MTAs do the following:

- accept emails sent from mail user agents
- query the MX records and select a mail server to transfer emails
- send auto-response messages if an email has failed to reach the destination

HOW DOES E-MAIL WORKS:

1. First the sender needs to enter the email address of the recipient along with the message using an email application. This should be done at the local computers. Once it is finished and the “Send” button is clicked, the email will be going to the MTA (The Mail Transfer Agent). This communication is done via the SMTP protocol.

2. The next step is DNS lookup. The system sends a request to find out the corresponding MTA of the recipient. This will be done with the help of the MX record. In the DNS zone, for the receiver address’ domain, there will be an MX record (stands for Mail Exchanger record). This is a DNS resource record which specifies the mail server of a domain. So, after the DNS lookup, a response is given to the requested mail server with the IP address of the recipient’s mail server. This way the ‘to’ mail server is identified.

3. The next step is transferring the message between the mail servers. The SMTP protocol is used for this communication. Now our message is with the recipient mail server (MTA).

4. Now, this message is transferred to the Mail Delivery Agent and then it is transferred to the recipient’s local computer. As we have seen earlier, two protocols can be used here. If we use POP3, then the whole email will be

downloaded to the local computer and the copy at the server gets deleted. If the protocol used is IMAP, then the email message is stored in the mail server itself, but the user can easily manipulate the emails on the mail server as in the local computer. This is the difference when using both the protocols and this is how your email gets delivered. If some error occurred to send the email, the emails will be delayed. There is a mail queue in every mail server. These mails will be pending in the mail queue. The mail server will keep trying to resend the email. Once the email sending fails permanently, the mail server may send a bounce back email message to the sender's email address.

5. This explains why you may be getting bounce back emails sometimes. The reason for bouncing back will be explained in the message. There are many reasons for getting an email to bounce back such as incorrect email address in the 'to' field.