1. Secure inter bank payment transaction:

Architecture of connect ips/VISA/Khalti/E-sewa etc....

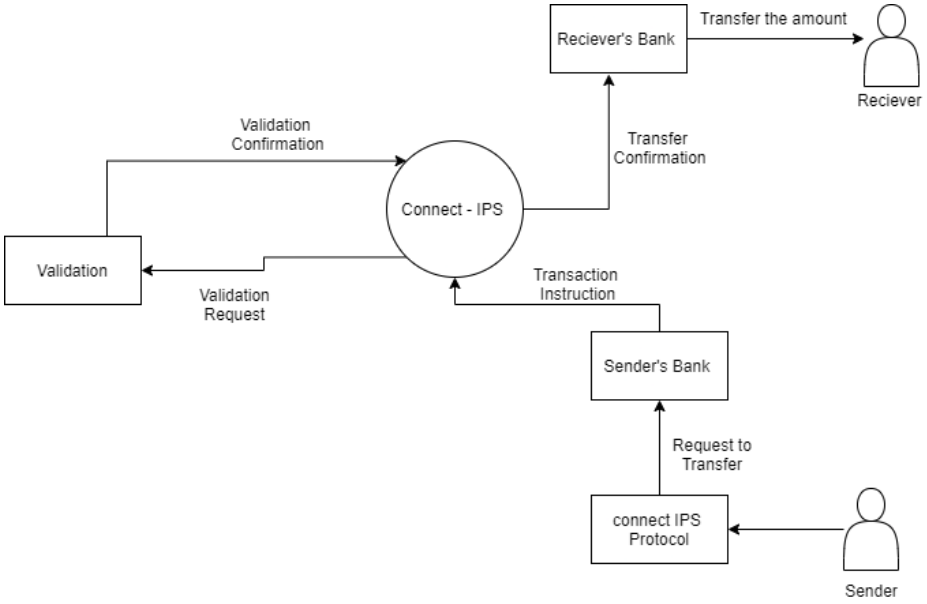
Analogy with SET protocol

In this case study, you have to formulate a conceptual design of payment gateway system (like esewa, khalti, visa etc) and also you need to provide the analogy with SET protocol which means, how SET protocol have been incorporated in the design and to what extent it has been used.

Interbank payment transaction refers to the transfer of money from the account of one user to the account of another user of the same bank or different bank. To make this transaction more effective and faster, the banking sector often uses a payment system. The transactions are done usually over the networks, specifically the internet. The most important aspect to be considered while carrying out these transactions is always security. The insecure payment system poses a serious threat to the confidence of the whole financial system.

connectIPS is an e-payment system designed to serve as a single payment platform for bank clients to make fund transfers and service payments through a variety of channels. It incorporates the NCHL-IPS technology for secure interbank payment transactions. Nepal Clearing House Limited (NCHL), licensed and controlled by Nepal Rastra Bank (NRB), develops and operates both ConnectIPS and NHCL-IPS. Payment transactions are performed directly from/to bank accounts, and they are usually instantaneous at both the sender and the receiver. The system is accessible 24 hours a day, seven days a week via web, mobile app, and payment process/gateway. This can also be accessed from the mobile/internet banking of major banks & financial institutions and App/Web of various mobile wallets.

Architecture of Connect ips



Based on the above diagram, transaction are carried out on Connect ips on following way -

1. Sender requests or authorizes its bank (called as originating bank) to issue a credit instruction for payment to account(s) held at one or more of the member banks.
2. The originating bank then initiates a direct credit transaction in the NCHL-IPS system and sends it to the beneficiary bank (called as receiving bank).
3. The receiving bank acknowledges the transaction and credits the beneficiary account after the settlement confirmation is received from the central bank i.e NRB.
4. The originating bank's customer account (receiver) will be debited after the settlement confirmation is received from the central bank.

Analogy with SET Protocol

Secure Electronic Transaction (SET) is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards.

Process involved in SET

1. The customer opens a Mastercard or Visa bank account. Any issuer of a credit card is some kind of bank.
2. The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.
3. Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.
4. The customer places an order over a web page, by phone, or some other means.
5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.
7. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
8. The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.
9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
10. The bank digitally signs and sends authorization to the merchant, who can then fill the order.

We can conclude that the design of the ConnectIPS can be considered a reduced version of the SET protocol because it only has a few of the protocol's components. However, the receiver, or merchant, is absent in this architecture. Because the sender is required to provide the receiver's financial information in the ConnectIPS. Because communication between the sender and the receiver is not necessary, there are no purchase requests containing order and payment information in the ConnectIPS architecture. In contrast to the payment gateway in the SET protocol, which does not save the user's banking information, the ConnectIPS database stores the essential banking information for the user.

2 .a. Study report on SMTP, IMAP and POP3 protocol

i. SMTP Protocol

Simple Mail Transfer Protocol (SMTP) is the standard protocol for email services on a TCP/IP network. SMTP provides the ability to send and receive email messages. 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 addresses. SMTP is an application-layer protocol that enables the transmission and delivery of email over the Internet. SMTP is created and maintained by the Internet Engineering Task Force (IETF). 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 addresses.

The SMTP model is of two type :

1. **End-to- end method** - The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization. A SMTP client who wants to send the mail will contact the destination's host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.
2. **Store-and- forward method** - This method works, if exchange of the message is between the same organization. In this method, SMTP clients can't send messages directly to the destination point because firstly those messages are stored on the server then their copy of those messages move to the destination email box.

Components of SMTP

User Agent (UA)- User Agent has the task to create a message, and makes the envelope then insert that message into the envelope to facilitate Mail Transfer Agent to move the message over the internet.

Mail Transfer Agent (MTA)- Mail Transfer Agent or Message Transfer Agent (MTA) is software that transfers electronic mail messages from one computer to another using a client–server application architecture. An MTA implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol.

Mail Gateway - Gateway is ideal for Exchange and other SMTP servers and requires no hardware, software or maintenance. It also acts as a backup server where your mail is held if your mail server or Internet connectivity fails.

Working of SMTP Protocol

1. **Composition of Email** - Users compose all e-mail messages, and then use MUA to send those messages (Mail User Agent). Mail User Agent is a piece of software that facilitates the movement and access of emails. The email message is divided into two sections: "body" and "header." The main message area is contained in the body segment, while the header segment contains the sender and recipient addresses, as well as the main heading of the message, such as the subject of an email.
2. **Submission of Mail:** After composing an email, the mail client then submits the completed email to the SMTP server by using SMTP on TCP port 25.
3. **Delivery of Email** - Mail Submission Agent (MSA) will move emails to MTA (Mail Transfer Agent) after they have been submitted. The Mail Transfer Agent will then use the "Domain Name System" to determine the destination domain and IP (Internet Protocol) of the recipient's domain name. MTA connects to the server for broadcasting messages after locating the recipient's domain.
4. **Receipt and Processing of Mail:** Once the message is received the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the email where it waits for the user to retrieve it.
5. **Access and Retrieval of Mail** – All emails are saved in the MDA, and these messages are accessed by the MUS (Mail User Agent).

Advantages

1. SMTP provides the simplest form of communicating through email messages between various computers in a particular network.
2. Since SMTP is developed from a simple platform, email messages may be sent easily and quickly.
3. SMTP also offers reliability in terms of outgoing email messages.
4. If there are instances where a particular message was not successfully sent, the SMTP server will always try to resend the same email until the transmission becomes successful.
5. With SMTP, companies and organizations may opt to have a Dedicated Server to handle outgoing email messages.

Disadvantages

1. It is insecure.
2. It can be easily hacked.
3. When you send an email through an SMTP server, you will be limited by the rules of your hosting or the limitations of the connection with the internet.

ii. **IMAP Protocol**

IMAP (Internet Message Access Protocol) is a standard protocol for a local client to access email on a remote server. IMAP is an application layer Internet Protocol that establishes host-to-host communication services for applications by utilizing the underlying transport layer protocols. This enables users to use a remote mail server. There are two ports used by IMAP which are:

- Port 143: It is a non-encrypted IMAP port.

- Port 993: This port is used when an IMAP client wants to connect through IMAP securely.

The client/server model is used by IMAP. On the one hand, we have an IMAP client, which is a computer program. On the other hand, we have an IMAP server, which is also a computer-based process. The two computers are linked by a network.

Features of IMAP

1. **Access and retrieve mail from a remote server:** The user can access and retrieve mail from a remote server while keeping the messages there.
2. **Set message flags:** The user can keep track of which messages he has already seen by setting message flags.
3. **Manage multiple mailboxes:** The user has the ability to manage multiple mailboxes and transfer messages between them. For those working on various projects, the user can organize them into various categories.
4. **Determine information prior to downloading:** Before downloading the mail from the mail server, it decides whether to retrieve or not.
5. **Organize mails on the server:** POP3 users are not permitted to manage their mails on the server. Users, on the other hand, can organize their emails on the server according to their needs, such as by creating, deleting, or renaming mailboxes.
6. **Search:** Users can conduct a search for the contents of emails.
7. **Check the email header:** Before downloading, users can check the email header.

Working of IMAP

Its working can be explained using the following example. All of the devices are synchronized with the main server using the IMAP protocol. Assume we have three devices: a desktop, a mobile phone, and a laptop. If all of these devices access the same mailbox, the mailbox will be synchronized across all of them. When mail is opened on one device, it is marked as open on all other devices; similarly, when mail is deleted on one device, it is deleted on all other devices. As a result, all of the devices are synchronized. We can see all of the folders in IMAP, such as spam, inbox, sent, and so on. We can also make our own folder, referred to as a custom folder, which will be visible on all other devices.

Advantages

1. Mail stored on a remote server, i.e. accessible from multiple different locations.
2. Internet connection needed to access mail.
3. Faster overview as only headers are downloaded until content is explicitly requested.
4. Mail is automatically backed up if the server is managed properly.
5. Saves local storage space.
6. Option to store mail locally.

Disadvantages

1. Mails won’t work without an active internet connection.
2. In case email usage is more, you would need a larger mailbox storage which might cost more.

3. Accessing mail is a little slower as compared to others as all folders get synchronized everytime there is a send / receive.

iii. POP3 Protocol

The Post Office Protocol (POP3) is an Internet standard protocol used by local email software clients to retrieve emails from a remote mail server over a TCP/IP connection. . In the POP3 protocol, the POP3 client is installed on the recipient system while the POP3 server is installed on the recipient's mail server. POP3 is designed to delete mail on the server as soon as the user has downloaded it. By default, the POP3 protocol works on two ports:

- **Port 110** – this is the default POP3 unencrypted port.
- **Port 995** – this is the port you need to use if you want to connect using POP3 securely.

Working of POP3

The client connects to the POP3 server when a user checks for new email. The email client then provides the server with its username and password for authentication. When the client is connected, it issues a series of text-based commands to retrieve all of the email messages. The user's local system then stores the downloaded messages as new emails, deletes the server copies, and disconnects from the server. Once the server emails are retrieved, they are deleted by default. As a result, the emails are tied to that specific machine, and you won't be able to access them from another machine's email client.

Advantages of POP3

1. Emails are downloaded to the user's computer. Messages can be read when the user is offline.
2. It provides easy and fast access to the emails as they are already stored on our PC.
3. There is no limit on the size of the email which we receive or send.
4. It requires less server storage space as all the mails are stored on the local machine.
5. There is maximum size on the mailbox, but it is limited by the size of the hard disk.
6. It is a simple protocol so it is one of the most popular protocols used today.
7. It is easy to configure and use.

Disadvantages of POP3

1. Emails are not accessible from other computers (unless configured to do so).
2. It can be difficult to move the local mail folder to another email client or physical machine.
3. Email folders can become corrupted, resulting in the loss of the entire mailbox.
4. Email attachments may contain viruses that can harm a user's computer if they are opened locally and their antivirus software fails to detect them.

b. Study report on Gmail and Signal app

Gmail

Gmail is a Google-provided free email service. Gmail is similar to other email services in that it allows you to send and receive emails, block spam, create an address book, and perform other basic email functions. However, it has a few more unique features that contribute to its popularity as one of the most popular online email services. You need a Google account to use this service. Users can receive emails up to 50 megabytes in size, including attachments, while they can send emails up to 25 megabytes. In order to send larger files, users can insert files from Google Drive into the message. Gmail offers a search-friendly layout as well as a "conversation view" that resembles an Internet forum. Google's mail servers scan emails automatically for a variety of reasons, including spam and virus filtering and the placement of context-sensitive advertising next to emails.

Issues regarding unlimited data retention, ease of monitoring by third parties, users of other email providers not agreeing to the policy when sending emails to Gmail addresses, and the potential for Google to change its policies to further decrease privacy by combining information with other Google data uses have all been brought up by privacy advocates.

Protocols in Gmail

Gmail uses two different protocols which are described as below:

The IMAP protocol is used in the web-based version of Gmail. All mail messages and email folders are stored on the server using the IMAP email email protocol, so any changes made when you use Gmail on one device will appear on any other device you use to check your Gmail emails. If you need to access email from several desktops or mobile devices, IMAP is a good option.

The POP email protocol downloads all email messages from a mail server to an email program on a computer or mobile device, then deletes the messages from the server. Unless extra synchronization software is installed, changes made to an email account, such as deleting a read message from the inbox or sending a new message to a contact, will not be visible when accessing the same email account from another computer or mobile device. POP email is excellent for accessing email while you're offline since it downloads messages rather than leaving them on the server.

Before configuring PC or mobile device email software to work with Gmail, one must enable IMAP or POP access in the Settings section of the Web-based Gmail account.

Security Features provided by Gmail

i. Two step verification - 2-step verification is one of the most essential security measures in Gmail, which was created by Google to add an extra degree of security. A code is given to a Gmail account holder's registered mobile phone via text, voice call, or mobile app every time they want to access their email account. After entering the code, the user will be prompted to input their password. Hackers will not be able to access the user's Gmail account because the code is unique and produced on the spot.

ii. Review suspicious activity - When Google detects suspicious behavior on a user's Gmail account, it sends a notification to the user. When an email account is accessed from an unusual location or device, Google sends a notification to the user's registered cellphone number or recovery email address. Users can then examine the information of their account by clicking on the check activity link.

iii. Security Sandbox - By 'executing' attachments in a private, secure sandbox environment, Security Sandbox for Gmail beta identifies the existence of unknown malware in attachments. It examines the operating system's side effects to determine malicious behavior. "Email attachments are detonated within a sandbox in the exact same manner they would if an actual user had clicked on it," Google writes in a blog post. According to Google, the security sandbox was created with the goal of providing protection against malware sent via embedded scripts.

iv. Confidential Mode - Gmail has a confidential mode, which allows account holders to secure sensitive content by setting expiration dates or canceling already sent messages. It also helps protect data even if the recipient's email account is hacked while the message is in transit.

v. Advanced phishing and malware detection - This Gmail function detects emails with odd attachment types and automatically displays a warning message before marking the message as spam. It also adds new controls to quarantine emails, protect Google Groups from inbound spoofing emails, and guard against anomalous attachment types.

Advantages

1. Gmail is a Web-based email service that lets you see all your emails from anywhere. The service has native mobile apps for iOS and Android, and a mobile-optimized version for viewing on the go. It's free to use on any computer or mobile device.
2. Gmail is a popular email search engine, allowing you to filter your emails by date and keywords. Google has added the ability to filter emails automatically as they arrive in your inbox.

Disadvantages

1. When the internet goes down, Gmail's email archives are out of reach. It cannot show the past messages as they are not stored on the hard drive. But it does have a limited amount of capability when offline but it's not the same as having all of your past messages.
2. Gmail is a free service, but it comes with the condition that it will target adverts around the edges of communications based on emails and internet activity. The company says its scanning is an automated and anonymous process. It's not clear if this means people may view it to be an invasion of privacy.

Signal App

Signal is a messaging app created by Open Whisper Systems whose goal is to provide top notch privacy and security while maintaining a simple yet functionally robust design. Every commit in its GitHub repositories is visible to the public.

Messaging apps are different from other social networking apps in that there are fewer points of entry for new users. Other social networking apps, such as Instagram, can entice new users with features such as video chat, shareable stories, photo posting, live streams, and social clout. Signal, on the other hand, has a relatively narrow purpose — secure, text-based communication with people you know — which makes it difficult for new users to discover the app. Direct invitation from friends, work, or an inherent interest in security and privacy technologies would be the most common modes of adoption.

Although the Signal Protocol hasn't been thoroughly examined, researchers have discovered no major flaws in its design. "The protocol satisfies several standard security properties, and we have found no serious flaws," they wrote. The first formal security analysis of Signal was conducted by researchers from Oxford, London, and McMaster University.

Security Features of Signal App

1. **Strong End-To-End Encryption & No User Records**

   Signal has very strong end-to-end encryption as well as no user records. This means Signal does not keep logs of your calls, except the last time you logged onto the service. So your phone number might reveal you to be a Signal user but nobody will ever know who you are talking to or what you are talking about.

2. **Set a Screen Lock PIN On Signal Itself**

   Users can add an additional screen lock PIN to Signal for extra security. They can also use Touch ID to open Signal but that would not be recommended.Users are also asked when they want the screen lock to time out, choosing “Instant” option will be good.

3. **Make Sure You’re Talking To The Correct Person**

   Since there is end-to-end encryption, the chances of a “man-in-the-middle” attack is slim. But nothing is guaranteed which is why we should still take additional steps to ensure that the person you are talking to is the right person. There are two verification methods. One for voice calls and one for text chats. With the voice call, once the call is connected, a two word verification phrase appears on the screen. Both sides see this on their screen. So one person says the first word and the other person says the second word (for example). Anyone trying to break into the conversation and impersonate one of the callers will not know what the phrase is because they will not have it on their phone. For text chats, when you send a message to someone, an identity key from them is downloaded onto your device and Signal automatically trusts that key as coming from the right person.

4. **Self Destructing Messages**

   Signal has a disappearing messages feature. This is where you send a message to one of your Signal contacts, and once the message has been read, it is wiped from your device and theirs – with no way to get it back. You can specify when the messages should disappear giving the other person a reasonable amount of time to read the message.

Protocol Used in Signal

Signal Protocol, formerly known as TextSecure Protocol, is a non-federated cryptographic protocol for voice and video communications that provides end-to-end encryption. The Signal Protocol uses the Curve25519, AES-256, and HMAC-SHA256 encryption methods, as well as the Double Ratchet Algorithm and the Extended Triple Diffie–Hellman (X3DH) handshake.

Signal protocol, which is the fundamental technology that Signal employs, allows two people who have never met before to construct a shared "secret key" across an insecure channel. Instead of sending a trusted courier to provide personal keys, two strangers can meet and exchange media in a common "secret location" without disclosing the keys to their encrypted messages.

Advantages

1. It is designed from the ground up to be nothing but a secure platform.
2. It’s not hacked onto an existing platform.
3. It is fully open source.
4. Allows audio chat with verification.

Disadvantages

1. The user interface and some of the user experience design has some glitches.
2. It requires a phone number for contact discovery.
3. Anyone intent on tracking a user's internet use can see using Signal. However, they won’t be able to read the messages.

3. Study report regarding Cookies and privacy.

Cookies

Cookies are text files containing small bits of information -such as a username and password- that are used to identify your computer when you connect to the internet. HTTP cookies are used to identify and improve your web browsing experience by allowing you to identify specific users.

When you connect to the server, the server creates data in a cookie. This information is identified by a number that is unique to you and your computer. When your computer and the network server exchange cookies, the server reads the ID and knows what information to serve you specifically.

HTTP cookies are necessary for modern Internet use, but they present a risk to your privacy. HTTP cookies are a necessary part of web browsing because they allow web developers to provide you with more personalized and convenient website visits. Cookies allow websites to remember you, your logins, shopping carts, and other information. They can, however, be a gold mine of personal information for criminals to snoop on.

There are four types of cookies: session, personalization, tracking and third-party.

Session Cookies - These cookies are short-term cookies and last only for the length of a browser "session " and are automatically deleted when the browser is closed.

Personalization Cookies - These cookies are for remembering and personalizing information. E-commerce sites use these kinds of cookies.

Tracking Cookies - Tracking cookies have more benefits to the sites rather than the end users. The cookie data is distributed and shared across multiple websites for the purpose of gathering information, or to present customized content to users such as advertisements.

Third party Cookies - Third-party cookies operate with iframes, which are occasionally used to present website elements by taking data from another website and displaying it on the one you're viewing.

Privacy

Privacy relates to any rights you have to control your personal information and how it's used. The privacy of personal information which relates to personal data stored on computer systems is called information privacy or data privacy. Privacy is one of the biggest problems in this new electronic age. The protection of personal information is regarded as a crucial aspect of information sharing. Personal information vulnerabilities have grown as the digital age has advanced.

Information privacy can be achieved in a variety of ways, including encryption, authentication, and data masking, all of which aim to ensure that information is only accessible to those who have been granted permission. These security measures are intended to prevent data mining and the unauthorized use of personal data, both of which are prohibited in many parts of the world.