# UNIT IV APPLICATION LAYER SECURITY

Electronic Mail Security: Pretty Good Privacy, S/MIME, DomainKeys Identified Mail. Wireless Network Security: Mobile Device Security

## ELECTRONIC MAIL SECURITY: PRETTY GOOD PRIVACY

**PGP provides the confidentiality and authentication service that can be used for electronic mail and file storage applications.**

### Operational description

The actual operation of PGP consists of five services:

1. Authentication
2. Confidentiality
3. Compression
4. E-mail compatibility
5. Segmentation.

### 1. Authentication

The sequence for authentication is as follows:

The sender creates the message. SHA-1 is used to generate a 160-bit hash code of the message. The hash code is encrypted with RSA using the sender's private key and the result is pretended to the message.

The receiver uses RSA with the sender's public key to decrypt and recover the hash code.

The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

### 2. Confidentiality

Confidentiality is provided by encrypting messages to be transmitted.

The sequence for confidentiality is as follows:

The sender generates a message and a random 128-bit number to be used as a session key for this message only. The message is encrypted with the session key.

The session key is encrypted with RSA, using the receiver's public key and is prepended to the message. The receiver uses RSA with its private key to decrypt and recover the session key. The session key is used to decrypt the message.

## 3. Compression

PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space for both e-mail transmission and for file storage.

Message encryption is applied after compression to strengthen cryptographic security. The compression algorithm used is ZIP.

## 4. E-mail compatibility

PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters.

## 5. Segmentation and reassembly

PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all the other processing, including the radix-64 conversion. At the receiving end, PGP must strip off all e-mail headers and reassemble the entire original block before performing the other steps.

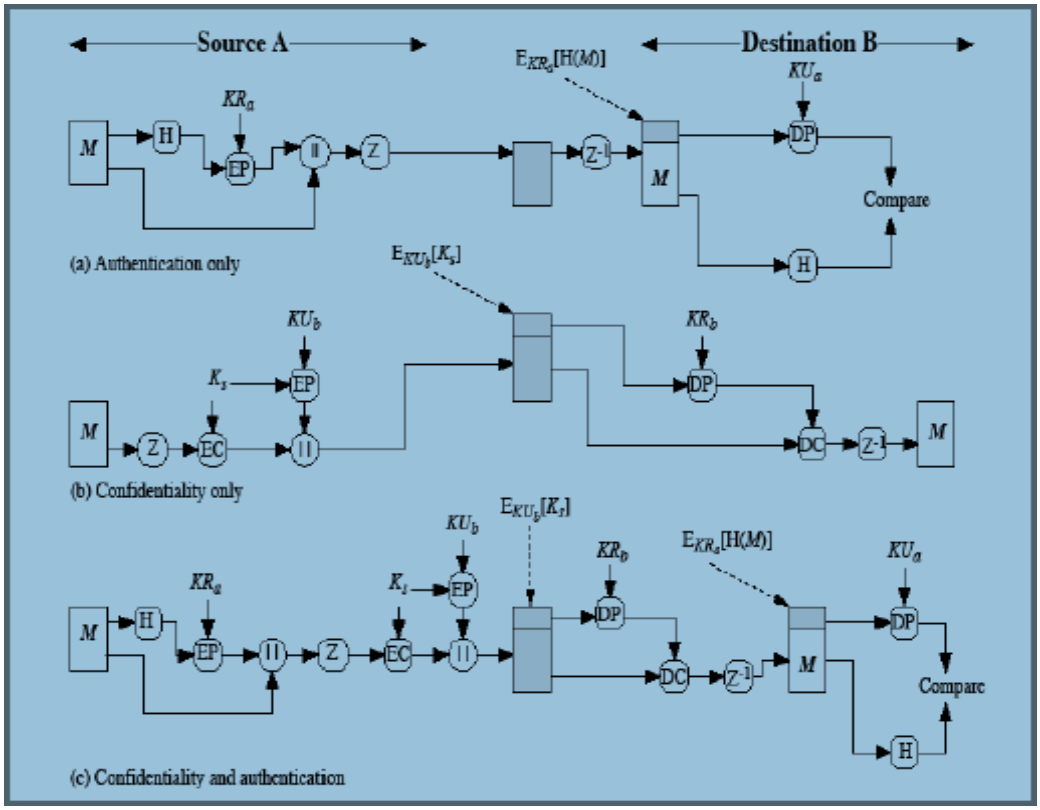



**Fig: Transmission and Reception of PGP message**

**PGP message generation**

First consider message transmission and assume that the message is to be both signed and encrypted. The sending PGP entity performs the following steps

**1. Signing the message**

- PGP retrieves the sender's private key from the private key ring using user ID as an index. If user ID was not provided, the first private key from the ring is retrieved.
- PGP prompts the user for the passphrase (password) to recover the unencrypted private key.
- The signature component of the message is constructed.

**2. Encrypting the message**

- PGP generates a session key and encrypts the message.
- PGP retrieves the recipient's public key from the public key ring using user ID as index.

## S/MIME

- S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME.
- Secure/Multipurpose Internet Mail Extension (S/MIME) is an industry-standard for email encryption and signature.
- S/MIME encrypts and digitally signs emails to verify that they are verified and that their contents have not been tampered with.
- S/MIME is a commonly-used protocol for sending encrypted and digitally-signed email messages and is implemented using S/MIME certificates.

**Multipurpose Internet Mail Extensions**

- MIME is an extension to SMTP (Simple Mail Transfer Protocol).
- MIME enables the transmission of a wide variety of file types over the internet, including images, audio, video, and other multimedia content.
- It is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol).

- Following are the limitations of SMTP scheme:

1. SMTP cannot transmit executable files.
2. SMTP cannot transmit text data that includes national language characters
3. SMTP servers may reject mail message over a certain size.

**Uses of S/MIME**

S/MIME can be used to:

- Check that the email you sent has not been tampered with by a third party.
- Create digital signatures to use when signing emails.
- Encrypt all emails.
- Check the email client you're using.

**Functions of S/MIME**

- **Authentication**

It refers to the verification of a computer user's or a website's identity.

- **Message Integrity**

This is a guarantee that the message's contents and data have not been tampered with.

- **Non repudiation**

This is a circumstance in which the original sender's identity and digital signatures are validated so that there is no doubt about it.

- **Privacy**

A data breach cannot be caused by an unintentional third party.

- **Data security**

Data security is ensured by a mix of public and private keys

**Services of S/MIME**

- **Digital signature**
- **Message encryption**

**Why Need a S/MIME Certificate?**

S/MIME certificates ensure that the emails you send are only accessible by the intended recipient.

They employ asymmetric encryption.

Public and private keys will be used to encrypt and decrypt emails, ensuring that the emails you send cannot be read by anyone other than the receiving party.

S/MIME certificates protect emails by preventing hackers from accessing or changing their contents.

Offer both digital signatures and encryption.

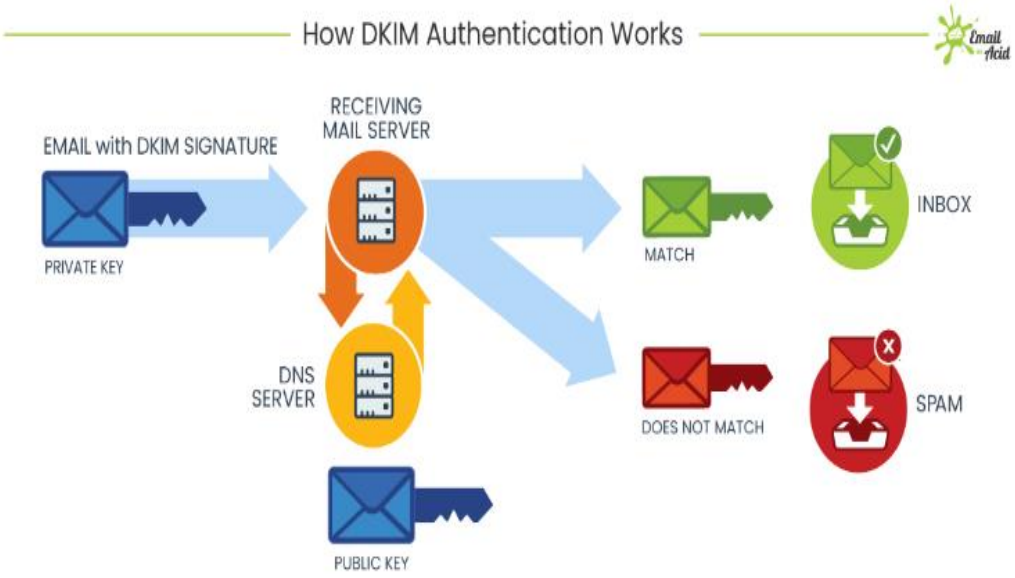
While asymmetric encryption keeps your data private, digital signatures provide authentication and message integrity.

S/MIME certificates are installed on email clients.

## DOMAINKEYS IDENTIFIED MAIL

- DKIM is the abbreviation for 'Domain Keys Identified Mail.'
- DomainKeys Identified Mail (DKIM) is a digital signature added to every email sent from a given email address.
- It is used for authenticating emails sent from specific servers. DKIM is a signature-based email authentication standard that gives emails a signature header and secures it with encryption. Thus, emails get a **tamper-proof seal** in the form of a DKIM signature.

- It confirms that the email has originated from the domain it claims. Secondly, it also certifies that there is no tampering with the email contents.
- The main purpose of DKIM is to prevent spoofing. Email spoofing is changing the original message's content and sending it from an alternative sender that looks like a trusted source. This type of cyber attack is widely used for fraud — for example, someone sending payment request messages from an email address that looks like yours (mark@whatevercompany.io vs. mark@whatever-company.io).



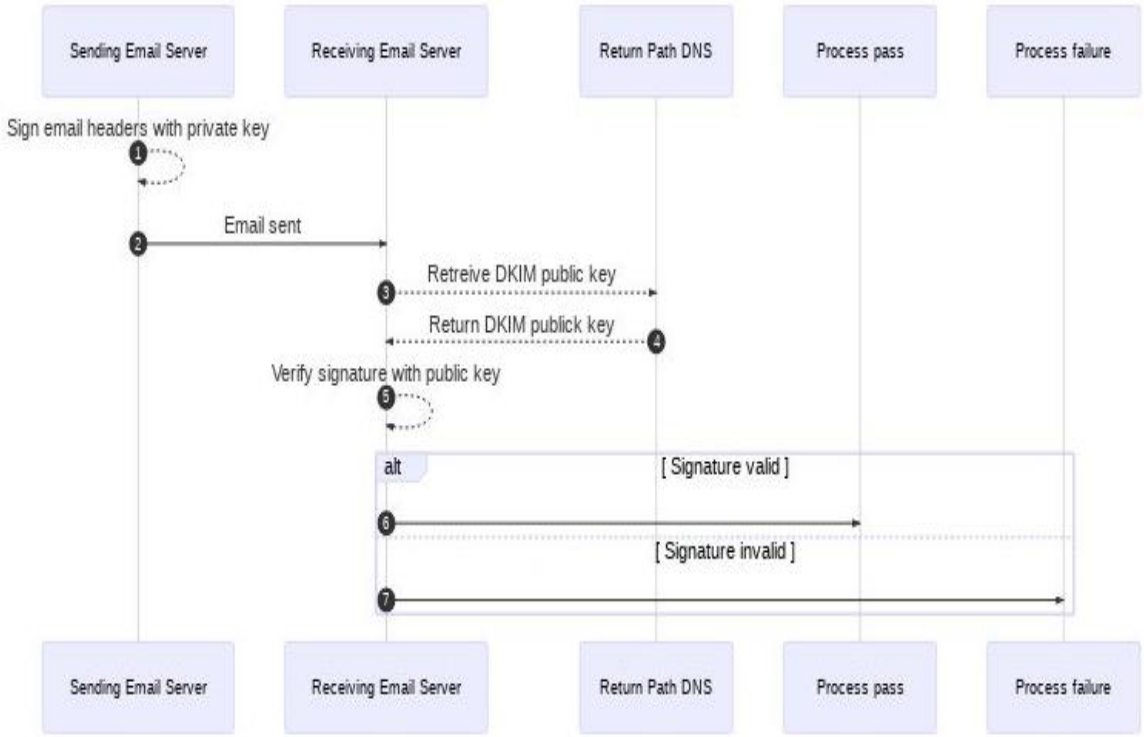

DKIM itself does not filter emails. However, it helps the receiving mail servers decide how to best filter incoming messages. A successful DKIM verification often means a reduced spam score for a message.

**DKIM mail flow**

To understand DKIM, it may be helpful to understand how email is sent when DKIM is added to the process.

Imagine an email sent by sender@example.com. For DKIM to work properly, the following steps take place:

1. Before sending the message, the sending server signs the email using a private key.
2. When the message is delivered, the receiving server obtains the DKIM record from the DNS records for example.com.
3. The receiving server then uses the public key in the DKIM record to verify the message's signature.
4. If the DKIM check passes, the receiving server can be confident the message was sent by the address in the return-path and wasn't altered in transit.
5. If the DKIM check fails, the message is likely illegitimate and will be processed using the receiving server's failure process.




## WIRELESS NETWORK SECURITY

- Wireless networks are computer networks that are not connected by cables of any kind.
- Wireless security is the prevention of unauthorized access or damage to computers using wireless networks.

**Factors contributing to risk of wireless networks:**

• **Channel:** Eavesdropping and jamming than wired networks. Wireless networks are also more vulnerable to active attacks that exploit

• **Mobility:** Mobility results in a number of risks.

• Resources: Limited memory and processing resources with which to counter threats, including denial of service and malware.

• **Accessibility:** Greatly increases their vulnerability to physical attacks.

**Wireless Network Threats**

- **Accidental association:** A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network.

• **Malicious association**: a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.

• **Ad hoc networks:** peer-to-peer networks between wireless computers with no access point between them

- **Nontraditional networks**: Nontraditional networks and links, such as personal network Bluetooth devices, barcode readers, and handheld PDAs, pose a security risk in terms of both eavesdropping and spoofing.

  • **Man-in-the middle attacks:** This attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device. Wireless networks are particularly vulnerable to such attacks.

- **Identity theft (MAC spoofing):** This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.

• **Denial of service (DoS):** The wireless environment lends itself to this type of attack, because it is so easy for the attacker to direct multiple wireless messages at the target.

• **Network injection:** A network injection attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages.

**Measures for Wireless Security**

**1.Securing Wireless Transmissions:** The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption.

To deal with eavesdropping, two types of countermeasures are appropriate:

- ✓ **Signal-hiding techniques:** Organizations can take a number of measures to make it more difficult for an attacker to locate their wireless access points, including turning off service set identifier (SSID) broadcasting by wireless access points; assigning cryptic names to SSIDs; reducing signal strength to the lowest level that still provides requisite coverage; and locating wireless access points in the interior of the building, away from windows and exterior walls.
- ✓ **Encryption:** Encryption of all wireless transmission is effective against eaves-dropping to the extent that the encryption keys are secured.

**2.Securing Wireless Access Points:** The main threat involving wireless access points is unauthorized access to the network. The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network.

**3.Securing Wireless Networks:** Recommends the following techniques for wireless network security:

1. **Use encryption.** Wireless routers are typically equipped with built-in encryption mechanisms for router-to-router traffic.
2. **Use antivirus and antispyware software, and a firewall.** These facilities should be enabled on all wireless network endpoints.
3. **Turn off identifier broadcasting.** Wireless routers are typically configured to broadcast an identifying signal so that any device within range can learn of the router's existence. If a network is configured so that authorized devices know the identity of routers, this capability can be disabled, so as to thwart attackers.
4. **Change the identifier on your router from the default.** Again, this measure thwarts attackers who will attempt to gain access to a wireless network usingdefault router identifiers.
5. **Change your router's pre-set password for administration.** This is another prudent step.
6. **Allow only specific computers to access your wireless network.** A router can be configured to only communicate with approved MAC addresses. Of course, MAC addresses can be spoofed, so this is just one element of a security strategy.

## MOBILE DEVICE SECURITY

**Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices.**

At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network.

**Security Threats**

**• Lack of Physical Security Controls**

Mobile device is required to remain on premises, the user may move the device within the organization between secure and nonsecured locations. Theft and tampering are realistic threats. The threat is two fold:

1) A malicious party may attempt to recover sensitive data from the device itself

2) may use the device to gain access to the organization's resources.

- **Use of Untrusted Mobile Devices**

In addition to company-issued and company-controlled mobile devices, virtually all employees will have personal smartphones and/or tablets. The organization must assume that these devices are not trustworthy.

**• Use of Untrusted Networks**

If a mobile device is used on premises, it can connect to organization resources over the organization's own in-house wireless networks.

Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the- middle types of attacks.

- **Use of Applications Created by Unknown Parties**

By design, it is easy to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software.

**• Interaction with Other Systems**

Unless an organization has control of all the devices involved in synchronization, there is considerable risk of the organization's data being stored in an unsecured location, plus the risk of the introduction of malware.

- **Use of Untrusted Content**

Mobile devices may access and use content that other computing devices do not encounter.

**• Use of Location Services**

The GPS service, it creates security risks. An attacker can use the location information to determine where the device and user are located, which may be of use to the attacker.

**Mobile device security strategy**

- ✓ **There are 3 elements in Mobile device security.**

1. **Device security**
2. **Traffic security**
3. **Barrier security**

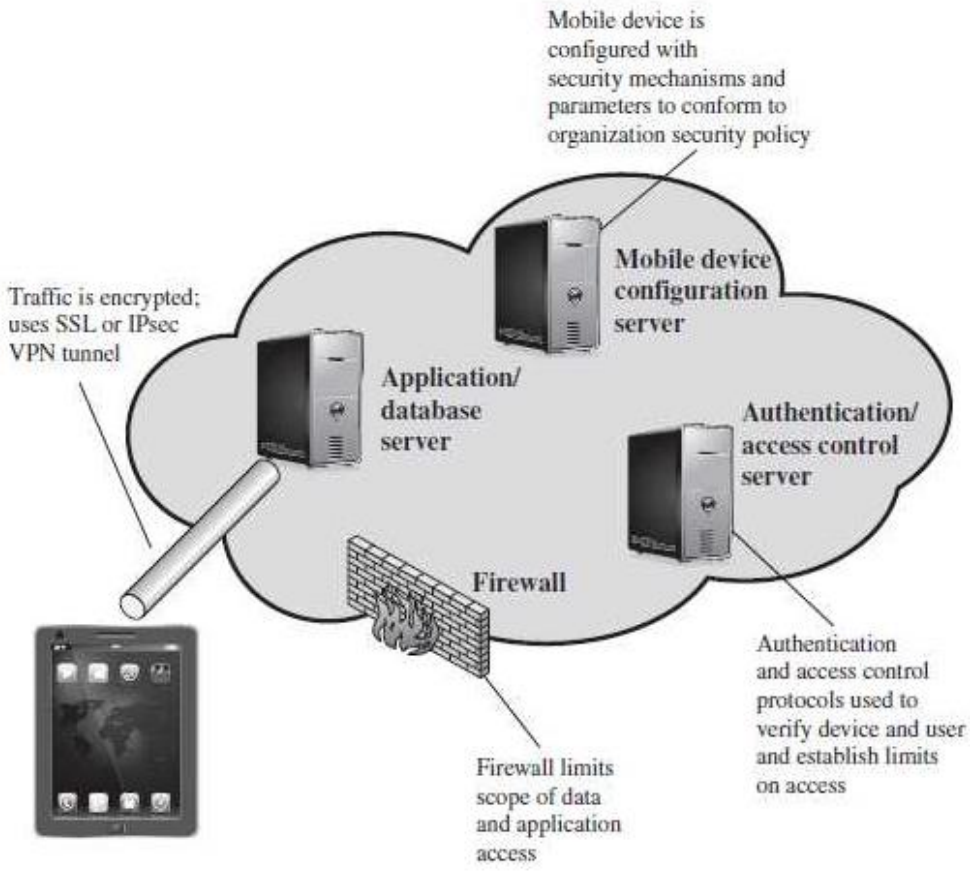



Fig1. Mobile Device Security Elements

**Device security**

- ✓ Jail broker devices should not be used
- ✓ Autolock enabled
- ✓ Password/ PIN protection

- ✓ Auto fill username and passwords should be avoided.
- ✓ Software and OS should be up to date
- ✓ Disable location services
- ✓ Avoid installing third party application
- ✓ Security trainings should be given to employees

**Traffic security**

- ✓ All traffic in the network should be encrypted
- ✓ All traffic should travel in secured channel
- ✓ VPN should be used
- ✓ Strong authentication protocols

**Barrier security**

- ✓ Establishing barriers to prevent unauthorized sources into the network

## UNIT V SECURITY PRACTICES

Firewalls and Intrusion Detection Systems: Intrusion Detection Password Management, Firewall Characteristics Types of Firewalls, Firewall Basing, Firewall Location and Configurations. Blockchains, Cloud Security and IoT security

## FIREWALLS AND INTRUSION DETECTION SYSTEMS

### INTRUDERS

- An intruder is someone who enters a system without permission.
- An intruder is a person who goes into a place where they are not supposed to be.
- Intruder is generally referred to as hacker or cracker.

Three classes of intruders are as follows:

- **Masquerader —** an individual who is not authorized to use the computer and who penetrates a system"s access controls to exploit a legitimate user"s account.
- **Misfeasor —** a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuse his or her privileges.
- **Clandestine user** – an individual who grabs supervisory control of the system and uses this control to avoid auditing and access controls or to suppress audit collection.

**Intrusion Techniques:**

**The objective of the intruders is to gain access to a system or to increase the range of privileges accessible on a system.** Generally, this requires the intruders to acquire information that should be protected. In most cases, the information is in the form of a user password. Typically, a system must maintain a file that associates a password with each authorized user. If such a file is stored with no protection, then it is an easy matter to gain access to it. The password files can be protected in one of the two ways:

• **One way encryption —** the system stores only an encrypted form of user"s password.

• **Access control** – access to the password file is limited to one or a very few accounts.

**The following techniques are used for learning passwords.**

1. **Try default passwords.**
2. **Try all short passwords**

Try words in the system"s online dictionary or a list of likely passwords. Collect information about users such as their full names, the name of their spouse and children, pictures in their office and books in their office that are related to hobbies.

**Two countermeasures:**

• **Detection**

• **Prevention**

## INTRUSION DETECTION

An intrusion detection system (IDS) is a device or software that monitors a network for malicious activity.

1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.
2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

### Approaches to Intrusion Detection

The approaches to Intrusion detection are,

• Statistical anomaly detection

• Rule-based detection

1. **Statistical anomaly detection**:

- Involves the collection of data relating to the behavior of legitimate users over a period of time.
- Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

a. **Threshold detection**:

- This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

b. **Profile based:**

- A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

2. **Rule-based detection:**

- Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

a. **Anomaly detection**:

Rules are developed to detect deviation from previous usage patterns

b. **Penetration identification**:

An expert system approach is used which searches for suspicious behaviour.

**PASSWORD MANAGEMENT**

- Set of principles and practices followed by users while storing and managing passwords to protect it from unauthorized access.

1. **Password Protection**

**Password Protection can be done in 4 ways.**

1. User education
2. Using computer generated password
3. Reactive password checking
4. Proactive password checking

## 2. The Vulnerability of Passwords

- Vulnerability of Passwords is nothing but weakness in passwords.
- Vulnerability of Passwords can happen in 2 ways.

**1.** From end user/ organizational vulnerabilities.

- Weak and easy to guess passwords
- Passwords are rarely changed.
- Same passwords used for all websites
- Noting password in non-secured places

**2.** Technical vulnerabilities.

- Weak encryption schemes
- Application that display passwords on screen while typing

## 3. Access Control

One way to thwart a password attack is to deny the opponent access to the password file. If the encrypted password portion of the file is accessible only by a privileged user, then the opponent cannot read it without already knowing the password of a privileged user.

### Password Selection Strategies

Four basic techniques are in use:

1. User education
2. Computer-generated passwords
3. Reactive password checking
4. Proactive password checking

### User education

Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.

### Computer-generated passwords

If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have

difficulty remembering it and so be tempted to write it down.

**Reactive password checking**

**A reactive password checking** strategy is one in which the system periodically runs its own password cracker to find guessable passwords. The system cancels passwords that are guessed and notifies user.

**Proactive password checking**

In this scheme, a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it

## FIREWALL

**A firewall:**

1. Defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

2. provides a location for monitoring security-related events

3. is a convenient platform for several Internet functions that are not security related, such as NAT and Internet usage audits or logs

4. A firewall can serve as the platform for IPSec to implement virtual private networks.

## FIREWALL CHARACTERISTICS

**Design goals for a firewall:**

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.

3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system.

**Techniques that firewalls use to control access and enforce the sites security policies are:**

 **Service control**: Determines the types of Internet services that can be accessed, inbound or outbound

 **Direction control**: Determines the direction in which particular service requests are allowed to flow

 **User control:** Controls access to a service according to which user is attempting to access it

 **Behavior control**: Controls how particular services are used (e.g. filter e-mail)

**Limitations of Firewall**

- The firewall cannot protect against attacks that bypass the firewall.
- The firewall does not protect against internal threats.
- The firewall cannot protect against the transfer of virus-infected programs or files.

## TYPES OF FIREWALLS

There are 3 common types of firewalls.

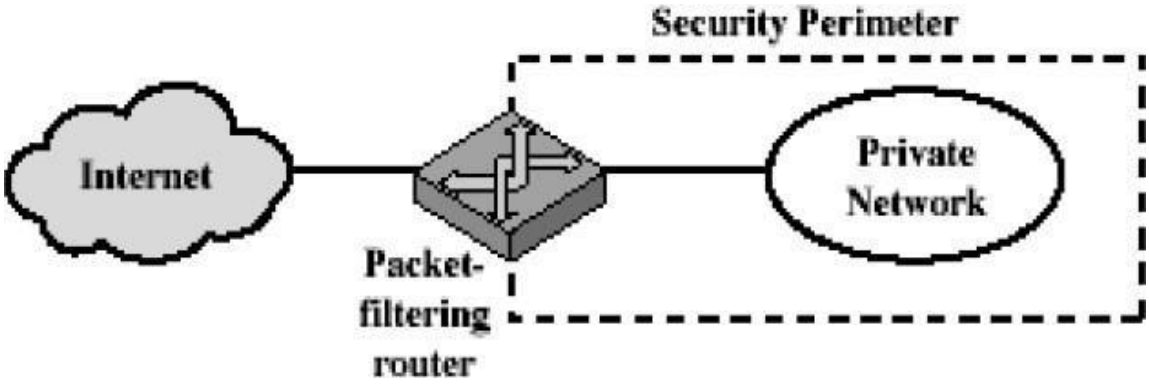
1. **Packet Filtering Router**
2. **Application-level gateways**
3. **Circuit-level gateways**

**Packet Filtering Router**

A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet.

The router is typically configured to filter packets going in both directions. Filtering rules are based on the information contained in a network packet:

- **Source IP address** – IP address of the system that originated the IP packet.
- **Destinations IP address** – IP address of the system, the IP is trying to reach.
- **Source and destination transport level address** – transport level port number.
- **IP protocol field** – defines the transport protocol
- **Interface —** for a router with three or more ports, which interface of the router the packet come from or which interface of the router the packet is destined for.




The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

**Advantages of packet filter router**

- Simple
- Transparent to users
- Very fast

**Weakness of packet filter firewalls**

- Packet filter firewalls do not examine upper-layer data; They cannot prevent attacks that employ application specific vulnerabilities or functions.
- As limited information is available to the firewall, the logging functionality present in packet filter firewall is limited.
- It does not support advanced user authentication schemes.
- They are generally vulnerable to attacks such as IP address spoofing.

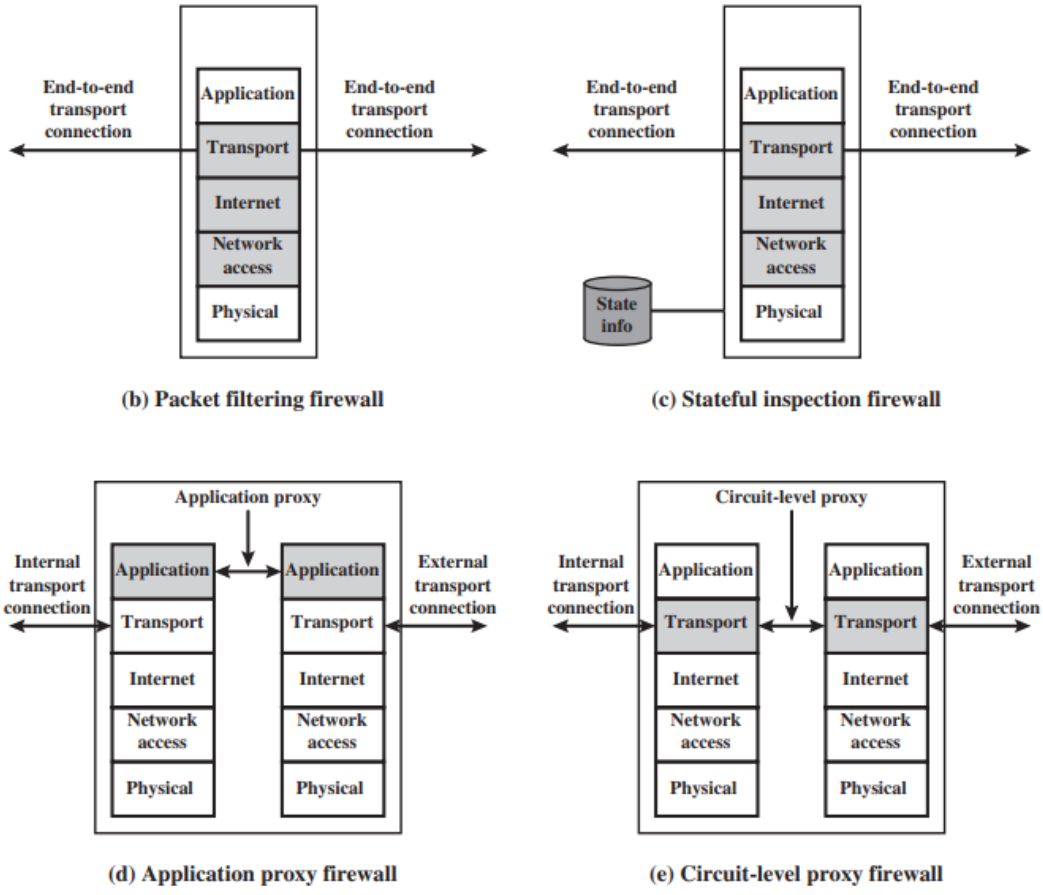



Figure 22.1 Types of Firewalls

**Attacks on Packet Filtering Routers**

➢ **IP address spoofing** — the intruders transmit packets from the outside with a source IP address field containing an address of an internal host.

**Countermeasure:** to discard packet with an inside source address if the packet arrives on an external interface.

➢ **Source routing attacks** — the source station specifies the route that a packet should take as it crosses the internet; i.e., it will bypass the

firewall.

**Countermeasure**: to discard all packets that uses this option.

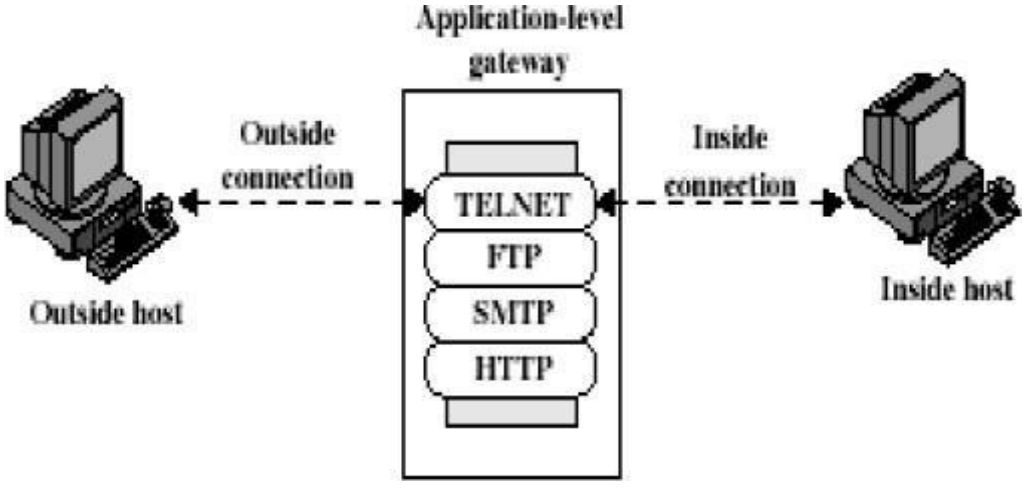
- **Tiny fragment attacks —** the intruder create extremely small fragments and force the TCP header information into a separate packet fragment. The attacker hopes that only the first fragment is examined and the remaining fragments are passed through.

**Countermeasure:** to discard all packets where the protocol type is TCP and the IP fragment offset is equal to 1.

**Application Level Gateway**

An Application level gateway also called a proxy server, acts as a relay of application level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

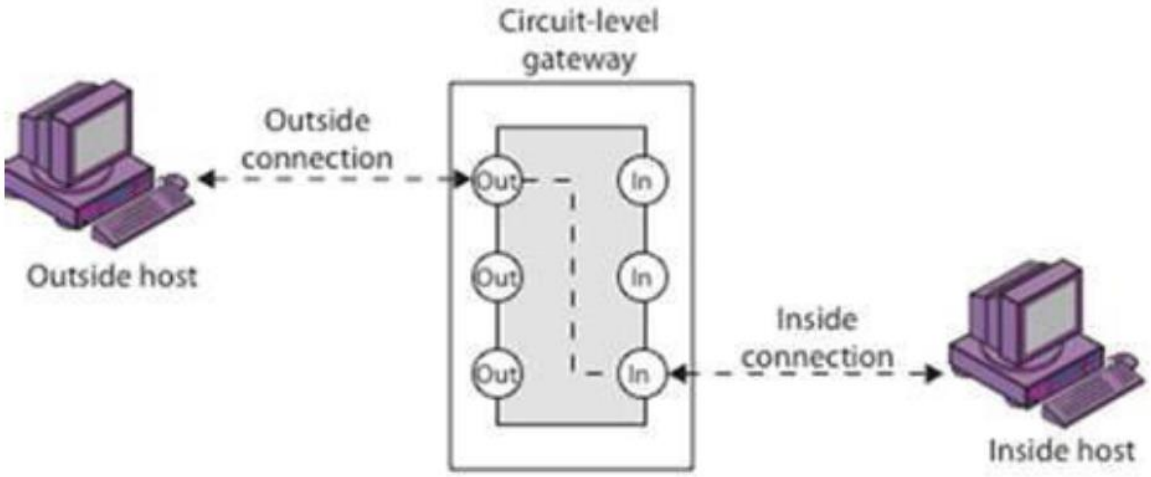
When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.




Application level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level. A prime disadvantage is the additional processing overhead on each connection.

**Circuit Level Gateway**

Circuit level gateway can be a stand-alone system or it can be a specified function performed by an application level gateway for certain applications. A Circuit level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host.




(c) Circuit-level gateway

Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

A typical use of Circuit level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.

**Stateful Inspection Firewalls**

A simple packet filtering firewall must permit inbound network traffic on all these high-numbered ports for TCP-based traffic to occur. This creates a vulnerability that can be exploited by unauthorized users. A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also

records information about TCP connections

## FIREWALL BASING

**It is common to base a firewall on a stand-alone machine running a common operating system, such as UNIX or Linux.**

**A bastion host is a critical strong point in the network's security, serving as a platform for an application-level or circuit-level gateway, or for external services.**

Common **characteristics of a bastion host** include that it:

- executes a secure version of its OS, making it a trusted system has only essential services installed on the bastion host.
- may require additional authentication before a user is allowed access to the proxy services

✓ is configured to support only a subset of the standard application's command set, with access only to specific hosts

✓ maintains detailed audit information by logging all traffic

✓ has each proxy module a very small software package specifically designed for network security

✓ has each proxy independent of other proxies on the bastion host

✓ have a proxy performs no disk access other than to read its initial configuration file

✓ have each proxy run as a non-privileged user in a private and secured directory

✓ A bastion host may have two or more network interfaces (or ports), and must be trusted to enforce trusted separation between these network connections, relaying traffic only according to policy.

### Host-Based Firewalls

A host-based firewall is a software module used to secure an individual host.

**Advantages to the use of a server-based or workstation based firewall:**

• Filtering rules can be tailored to the host environment. Specific corporate

security policies for servers can be implemented, with different filters for servers used for different application.

• Protection is provided independent of topology. Thus both internal and external attacks must pass through the firewall.

• Used in conjunction with stand-alone firewalls, the host-based firewall provides an additional layer of protection. A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

**Personal Firewall**

- ✓ A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side.
- ✓ Personal firewall functionality can be used in the home environment and on corporate intranets. Typically, the personal firewall is a software module on the personal computer.
- ✓ Personal firewalls are typically much less complex than either server-based firewalls or stand-alone firewalls. The primary role of the personal firewall is to deny unauthorized remote access to the computer. The firewall can also monitor outgoing activity in an attempt to detect and block worms and other malware.

**Firewall Location and Configurations**

A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.

**DMZ Networks**

An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network.

Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks.

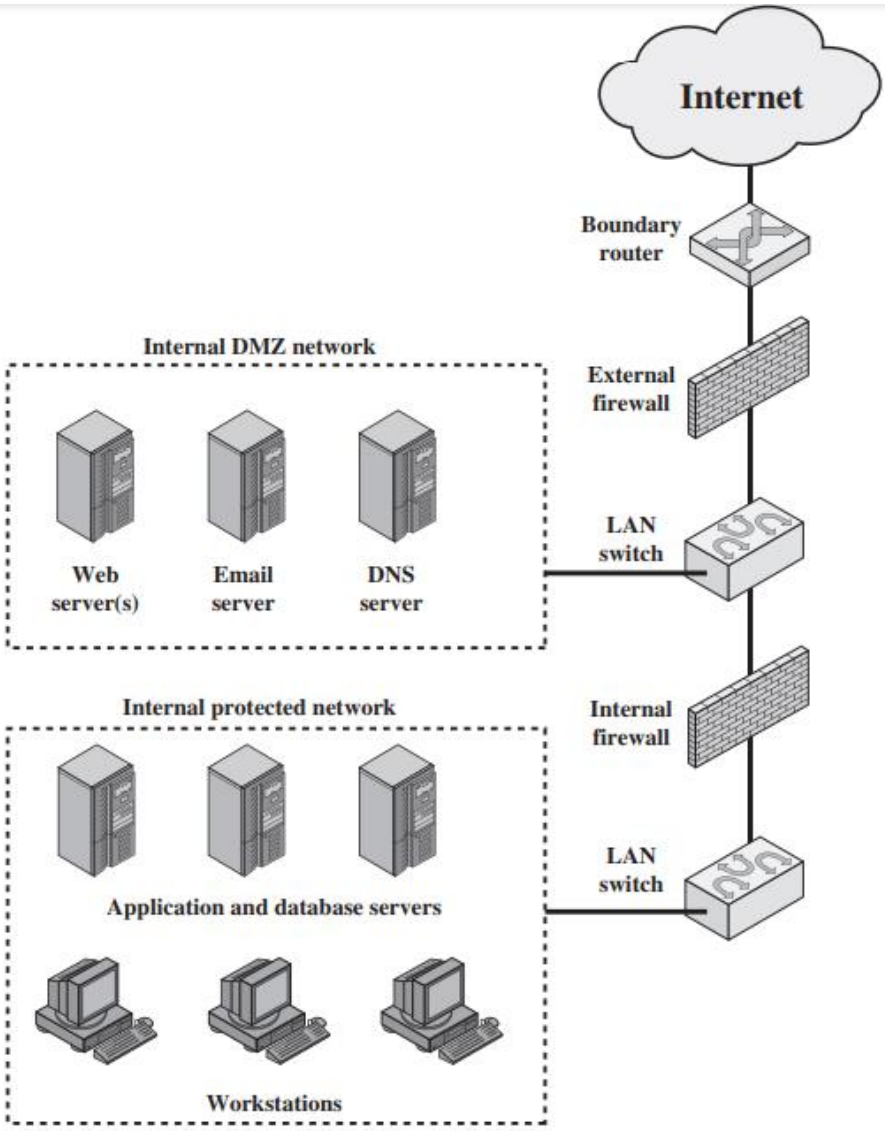



Figure 22.3 Example Firewall Configuration

The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity.

In this type of configuration, internal firewalls serve three purposes:

**1.** The internal firewall adds more stringent filtering capability, compared to the

external firewall, in order to protect enterprise servers and workstations from external attack.

**2.** The internal firewall provides two way protection with respect to the DMZ.

First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other ma lware lodged in a DMZ system.

Second, an internal firewall can protect the DMZ systems from attack from the internal protected network.

**3.** Multiple internal firewalls can be used to protect portions of the internal network from each other.

**Virtual Private Networks**

**Virtual private network (VPN)** consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.

At each corporate site, workstations, servers, and databases are linked by one or more local area net- works (LANs).

VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.

The encryption may be performed by firewall software or possibly by routers.

The most common protocol
mechanism used for this purpose is at the IP level and is known as IPsec.

**Distributed Firewalls**

A distributed firewall configuration involves stand-alone firewall devices plus host-based firewalls working together under a central administrative control.

Figure suggests a distributed firewall configuration.

Administrators can configure host- resident

firewalls on hundreds of servers and workstations as well as configure personal firew alls on local and remote user systems.

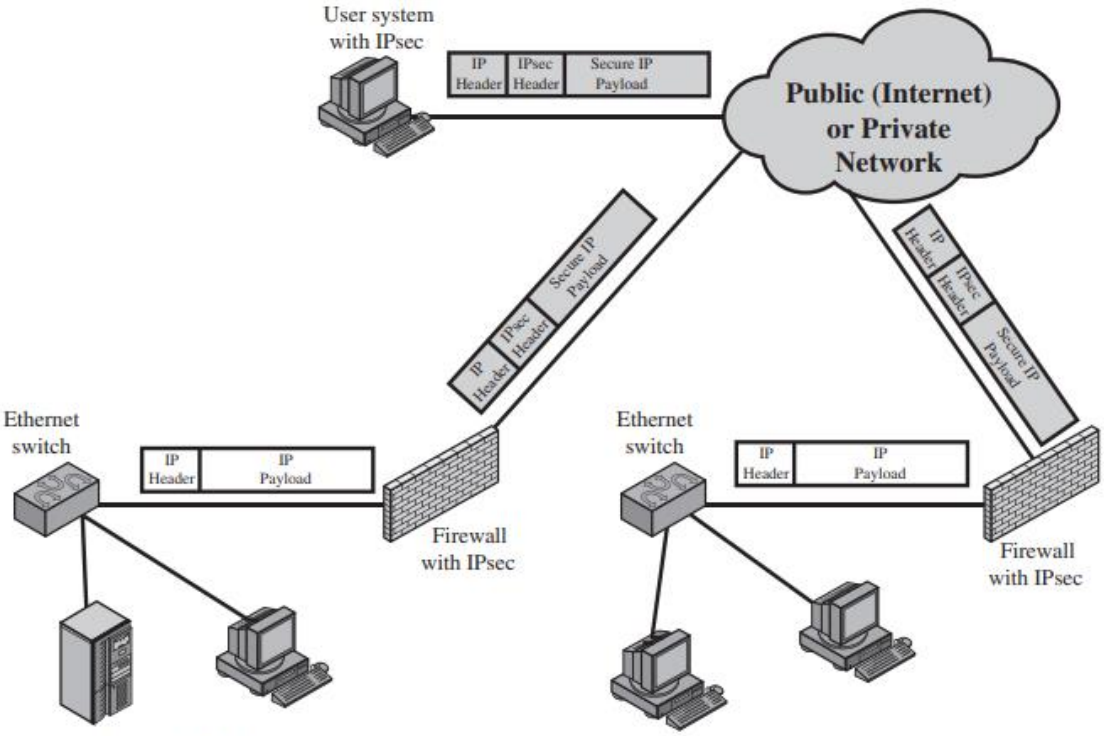



Figure 22.4 A VPN Security Scenario

## BLOCKCHAINS

- The blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties.
- Each transaction is verified by the majority of participants of the system.
- It contains every single record of each transaction.
- Bitcoin is the most popular cryptocurrency an example of the blockchain.
- Blockchain Technology first came to light when a person or group of individuals name ‘Satoshi Nakamoto’ published a white paper on “BitCoin: A peer-to-peer electronic cash system” in 2008.
- Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible.
- Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

- Blockchain is a secure series or chain of timestamped records stored in a
- database that a group of users manages who are a part of a decentralized network.
- Blockchain is a decentralized or distributed ledger where each node in the network has access to the data or records stored in a blockchain.

**Characteristics of Block chain**

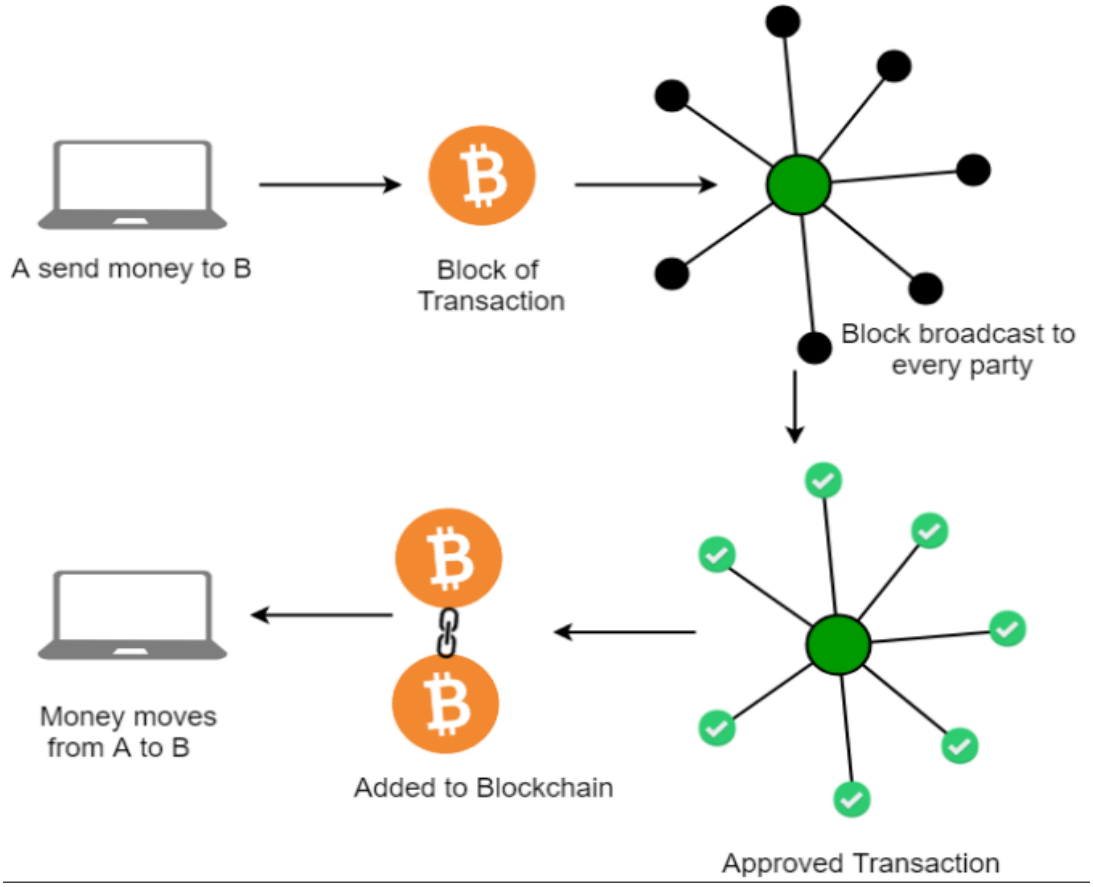
•Ledger – Append only

•Secure – Cryptographically secure

•Shared- Multiple participants

•Distributed – Scaling of nodes

**How does Blockchain Technology Work?**

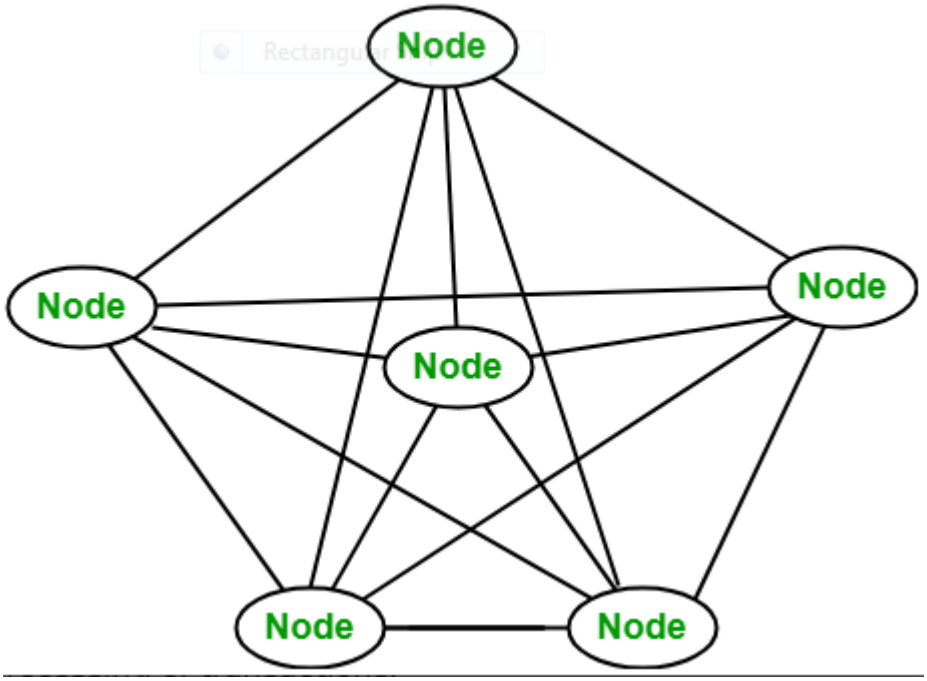



One of the famous use of Blockchain is Bitcoin. Bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic

proof instead of third-party trust for two parties to execute transactions over the Internet. Each transaction protects through a digital signature.

**Blockchain nodes**

A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. The client helps in validating and propagating transactions onto the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.




**Disadvantages of the current transaction system:**

- ✓ Cash can only be used in low-amount transactions locally.
- ✓ The huge waiting time in the processing of transactions.
- ✓ The need for a third party for verification and execution of Transactions makes the process complex.

- ✓ If the Central Server like Banks is compromised, the whole system is affected including the participants.
- ✓ Organizations doing validation charge high process thus making the process expensive.

**What are the benefits of Blockchain?**

- **Time-saving:** No central Authority verification is needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of the shared ledger.
- **Tighter security:** No one can tamper with Blockchain Data as it is shared among millions of Participants. The system is safe against cybercrimes and Fraud.
- **Collaboration:** It permits every party to interact directly with one another while not requiring third-party negotiation.
- **Reliability:** Blockchain certifies and verifies the identities of every interested party. This removes double records, reducing rates and accelerating transactions.

# IOT SECURITY

- **IoT (Internet of Things) security** refers to the measures and practices implemented to protect the Internet of Things devices, systems, and networks from unauthorized access, data breaches, and other potential threats.
- The Internet of Things involves connecting various physical devices and objects to the internet, enabling them to collect and exchange data.
- Examples of IoT devices include smart home devices, industrial sensors, medical devices, and connected vehicles.

**What are the Challenges of IoT Security?**

1. **Embedded Passwords**. Embedding passwords in IoT devices make it easy for remote support technicians to access devices for troubleshooting and simplifies the installation of multiple devices. Of course, it also simplifies access to devices for malicious purposes.
2. **Lack of device authentication.** Allowing IoT devices access to the network without authenticating opens the network to unknown and unauthorized devices. Rogue devices can serve as an entry point for attacks or even as a source of attacks.
3. **Patching and upgrading**. Some IoT devices do not provide a simple (or any) means to patch or upgrade software. This results in many IoT devices with vulnerabilities continuing to be in use.

4. **Physical hardening**. Physical access to IoT devices can introduce risk if those devices are not hardened against physical attack. Such an attack may not be intended to damage the device, but rather to extract information.

5. **Outdated components**. When vulnerabilities are discovered in hardware or software components of IoT devices, it can be difficult and expensive for manufacturers or users to update or replace them. As with patches, this results in many IoT devices with vulnerabilities continuing to be used.

6. **Device monitoring and management**. IoT devices do not always have a unique identifier that facilitates asset tracking, monitoring, and management. IT personnel do not necessarily consider IoT devices among the hosts that they

monitor and manage. Asset tracking systems sometimes neglect to include IoT devices, so they sit on the network without being managed or monitored.

**Types of IoT Security**

- **Network Security:** Users need to protect their devices against unauthorized access and potential exploitation. IoT network security implements a zero-trust security strategy to minimize the corporate attack surface.

- **Embedded:** Nano agents provide on-device security for IoT devices. Runtime protection monitors the current state of the device and takes action based on anomalies to identify and remediate zero-day attacks.

- **Firmware Assessment:** Firmware security starts with assessing the firmware of a protected IoT device. This finds potential vulnerabilities within an IoT device's firmware.

## Cloud Security

Cloud security, also known as cloud computing security, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data and resource access control, and data privacy protection.

**Benefits of Cloud Security System**

- Protecting the Business from Dangers
- Protect against internal threats
- Preventing data loss
- Top threats to the system include Malware, Ransomware, and
- Break the Malware and Ransomware attacks
- Malware poses a severe threat to the businesses.

**DDoS Security**

Distributed Denial of Service (DDoS)is flooded with requests. Website slows down the downloading until it crashes to handle the number of requests.

**Types of Cloud Computing Security Controls :**

1. **Deterrent Controls :**

   Deterrent controls are designed to block immoral attacks on a cloud system.

2. **Preventive Controls :**

   Preventive controls make the system robust to attacks by eliminating vulnerabilities in it.

3. **Detective Controls** :

   It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.

4. **Corrective Controls :**

   In the event of a security attack these controls are activated. They limit the damage caused by the attack.