Unit 5 ccs354 - Summary Computer Science

Computer Science (Jain College of Engineering and Research)

UNIT V

5 Security Practices

Syllabus

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 securityy

Contents

5.1 Intrusion Detection

AU : May-14,17, Dec.-14,15

- *Intrusion* is the act of gaining unauthorized access to a system so as to cause loss.
- *Intrusion detection* is the act of detecting unwanted traffic on a network or a device.
- Intrusion Detection Systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behavior.
- Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.

Functions of intrusion detection systems

1. Monitoring and analysis of user and system activity
2. Auditing of system configurations and vulnerabilities
3. Assessing the integrity of critical system and data files
4. Recognition of activity patterns reflecting known attacks
5. Statistical analysis for abnormal activity patterns

Benefits of intrusion detection

1. Improving integrity of other parts of the information security infrastructure
2. Improved system monitoring
3. Tracing user activity from the point of entry to point of exit or impact
4. Recognizing and reporting alterations to data files
5. Spotting errors of system configuration and sometimes correcting them
6. Recognizing specific types of attack and alerting appropriate staff for defensive responses
7. Keeping system management personnel up to date on recent corrections to programs
8. Allowing non-expert staff to contribute to system security
9. Providing guidelines in establishing information security policies

rocess model

- Many IDSs can be described in terms of following functional components :
  1. **Information sources :** The different sources of event information used to determine whether an intrusion has taken place. These sources can be drawn from different levels of the system, with network, host, and application monitoring most common.
  2. **Analysis :** The part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection.
  3. **Response :** The set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports.

5.1.1 Types of Intrusion Detection System

5.1.1.1 Anomaly Detection

- An anomaly based intrusion detection system is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- It examines ongoing traffic, activity, transactions, and behaviour in order to identify intrusions by detecting anomalies.
- For instance, anomaly-based IDS will detect that an IP packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.
- The classification is based on heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that falls out of normal system operation.
- Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation.
- The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.

- Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.
- The measures and techniques used in anomaly detection include : Threshold detection, statistical measures, and rule-based measures.

Advantages of anomaly detection

1. IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
2. Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

Disadvantages of anomaly detection

1. Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
2. Anomaly detection approaches often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

5.1.1.2 Signature-based Detection

- A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.
- This is similar to the way most antivirus software detects malware.
- A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. The inherent weakness in relying on signatures is that the signature patterns must be known first.
- New attacks are often unrecognizable by popular IDS. Signatures can be masked as well. The ongoing race between new attacks and detection systems has been a challenge.
- Also called misuse detection.

Advantages of signature-based detection

1. Signatures are easy to develop
2. Understand if you know what network behavior you're trying to identify.

Disadvantages of signature-based detection

1. High false positive rate
2. Largely ineffective at detecting previously unknown threats
3. Signature database must be continually updated and maintained.

5.1.1.3 Comparison between Signature-based and Anomaly Detection

Parameters	Signature-based detection	Anomaly detection
Technique	Detect patterns of interest	Deviations from learned norms
Generalization	Problematic	Yes
Specific	Yes	No
Sensitivity	High	Moderate
False alarms	Low	Moderate
Adaptation	No	Yes

5.1.1.4 Network Based System

- A Network Intrusion Detection System (NIDS) is tries to detect malicious activity such as denial of service attacks; port scans or even attempts to crack into computers by network security monitoring of network traffic.
- Network intrusion detection systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- The majority of commercial intrusion detection systems are network based.
- These IDSs detect attacks by capturing and analyzing network packets.
- Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts.
- Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network.
- These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console.
- As the sensors are limited to running the IDS, they can be more easily secured against attack.
- Many of these sensors are designed to run in stealth mode, in order to make it more difficult for an attacker to determine their presence and location.

Advantages of network-based IDSs

1. A few well-placed network-based IDSs can monitor a large network.
2. The deployment of network-based IDSs has little impact upon an existing network.
3. It can be made very secure against attack.

Disadvantages of network-based IDSs

1. Network-based IDSs may have difficulty processing all packets in a large or busy network.
2. Network-based IDSs cannot analyze encrypted information.
3. Most network-based IDSs cannot tell whether or not an attack was successful
4. Some network-based IDSs have problems dealing with network-based attacks that involve fragmenting packets.

5.1.1.5 Host-based IDSs (HIDS)

- Host based monitors system logs for evidence of malicious or suspicious application activity in real time.
- It requires small programs or agents to be installed on individual systems to be monitored. The agents supervise the OS and write data to log files and activate alarm.
- Host-based IDSs operate on information collected from within an individual computer system.
- This allows host-based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system.
- Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs.
- Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs.
- System logs are much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend.

Advantages

1. With their ability to monitor events local to a host, can detect attacks that cannot be seen by network-based IDS.
2. It can often operate in an environment in which network traffic is encrypted.
3. When host-based IDSs operate on OS audit trails; they can help detect Trojan horse or other attacks that involve software integrity breaches.

Disadvantages

1. Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
2. Since at least the information sources for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
3. Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of-service attacks.
5. When host-based IDSs use OS audit trails as an information source, the amount of information can be immense, requiring additional local storage on the system.

5.1.1.6 Differences between HIDS and NIDS

Sr. No.	NIDS	HIDS
1.	Broad in scope, (watching all network activities).	Narrow in scope (watching only specific host activities).
2.	Easier setup.	More complex setup.
3.	Better for detecting attacks from the outside.	Better for detecting attacks from the inside.
4.	Less expensive to implement.	More expensive to implement.
5.	Detection is based on what can be recorded on the entire network.	Detection is based on what any single host can record.
6.	Examines packet headers.	Does not see packet headers.
7.	Near real-time response.	Usually only responds after a suspicious log entry has been made.
8.	OS-independent.	OS-specific.
9.	Detects network attacks as payload is analyzed.	Detects local attacks before they hit the network.
10.	Detects unsuccessful attack attempts	Verifies success or failure of attacks.

5.1.2 Intrusion Detection Techniques

- Intrusion detection techniques are as follows :
  1. **Threshold detection :** It records each occurrence of suspicious events and compares it with a threshold number. Threshold detection involves counting no occurrences of a specific event type over an interval of time, if count surpasses a reasonable number, then intrusion is assumed establishing threshold number is difficult.
  2. **Anomaly detection :** It requires little knowledge of the actual system beforehand. Usage patterns are established automatically by means of neural networks.
  3. **Rule based detection :** Observe events on system and apply rules to decide if activity is suspicious or not. Analyze historical audit records to identify usage patterns and auto-generate rules for them. Then observe current behavior and match against rules to see if conforms. Like statistical anomaly detection does not require prior knowledge of security flaws.

5.1.3 Tools for Intrusion Detection

- Audit record is a fundamental tool for intrusion detecting. Two forms of audit records are used.

  1. **Native audit records :** • In all multiuser operating system accounting software collects information about user activity.

  2. **Detective specific audit records :** • A system that collects information need by intrusion detection system.

Audit record format

- Each audit record contains following field.
  1. Subject 2. Action 3. Object
  4. Exception - condition 5. Resource - usage 6. Time stamp.

Fig. 5.1.1 shows audit record format.

Subject	Action	Object	Exception condition	Resource-usage	Time-stamp

Fig. 5.1.1 Audit record format

5.1.4 Distributed IDS

- A distributed collection of hosts supported by a LAN or internetwork is called distributed intrusion detection system. Fig. 5.1.2 shows distributed ID architecture.

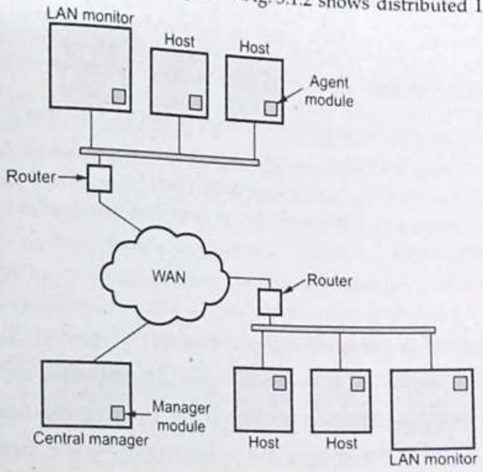

Fig. 5.1.2 Distributed ID architecture

Components of distributed IDS

- The distributed IDS consists of three major components.
  1. Host agent module 2. LAN monitor agent module
  3. Central manager module.

5.1.5 Strengths of IDS

Intrusion detection systems perform the following functions well :

1. Monitoring and analysis of system events and user behaviors.
2. Testing the security states of system configurations.
3. Base lining the security state of a system, then tracking any changes to that baseline.
4. Recognizing patterns of system events that correspond to known attacks.
5. Recognizing patterns of activity that statistically vary from normal activity.
6. Managing operating system audit and logging mechanisms and the data they generate.

7. Alerting appropriate staff by appropriate means when attacks are detected.
8. Measuring enforcement of security policies encoded in the analysis engine.
9. Providing default information security policies.
10. Allowing non-security experts to perform important security monitoring function.

5.1.6 Limitations of IDS

Intrusion detection systems cannot perform the following functions :

1. Compensating for weak or missing security mechanisms in the protection infrastructure. Such mechanisms include firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection and eradication.
2. Instantaneously detecting, reporting, and responding to an attack, when there is a heavy network or processing load.
3. Detecting newly published attacks or variants of existing attacks.
4. Effectively responding to attacks launched by sophisticated attackers.
5. Automatically investigating attacks without human intervention.
6. Resisting attacks that are intended to defeat or circumvent them.
7. Compensating for problems with the fidelity of information sources.
8. Dealing effectively with switched networks.

5.1.7 Differences between IDS and IPS

Sr. No.	IDS	IPS
1.	Installed on network segments (NIDS) and on host (HIDS)	Installed on network segments (NIPS) and on host (HIPS)
2.	Sits on network passively	Sits inline (not passive)
3.	Cannot parse encrypted traffic	Better at protecting applications
4.	Central management control	Central management control
5.	Better at detecting hacking attacks	Ideal for blocking web defacement
6.	Alerting product (reactive)	Blocking product (proactive)

5.1.8 Intrusion Prevention System (IPS)

- Although IDS have been one of the cornerstones of network security, they have covered only one component of the total network security picture since they have been and they a passive component which only detects and reports without preventing.

- A promising new model of intrusion is developing and picking up momentum. It is the Intrusion Prevention System (IPS) which, is to prevent attacks. Like their counterparts the IDS, IPS fall into two categories : Network-based and host-based.

1. Network-based Intrusion Prevention Systems (NIPSs)

- Because NIDSs are passively detecting intrusion into the network without preventing them from entering the networks, many organization in recent times have been bundling up IDS and firewalls to create a model that can detect and then prevent.

- The bundle works as follows.
  a. The IDS fronts the network with a firewall behind it. On the detection of an attack, the IDS then goes into the prevention mode by altering the firewall access control rules on the firewall. The action may result in the attack being blocked based on all the acces control regimes administered by the firewall.

  b. The IDS can also affect prevention through the TCP resets; TCP utilizes the RST (reset) bit in the TCP header for resetting a TCP connection, usually sent as a response request to a non-existent connection. But this kind of bundling is both expensive and complex, especially to an untrained security team. It suffers from *latency* - the time it takes for the IDS to either modify the firewall rules or issue a TCP reset command. This period of time is critical in the success of an attack.

2. Host-based Intrusion Prevention Systems (HIPSs)

a. Most HIPSs work by *sand-boxing*, a process of restricting the definition of acceptable behavior rules used on HIPSs. HIPS prevention occurs at the agent residing at the host. The agent intercepts system calls or system messages by utilizing dynamic linked libraries (dll) substitution.

b. The substitution is accomplished by injecting existing system dlls with vendor stub dlls that perform the interception.

- Fig. 5.1.3 shows the placement of IDS and IPS.
- IDSs are slow and cannot be in-line with the packet stream. IPSs use ASICs for speed; can be in-line with the packet stream. Therefore can stop attacks.

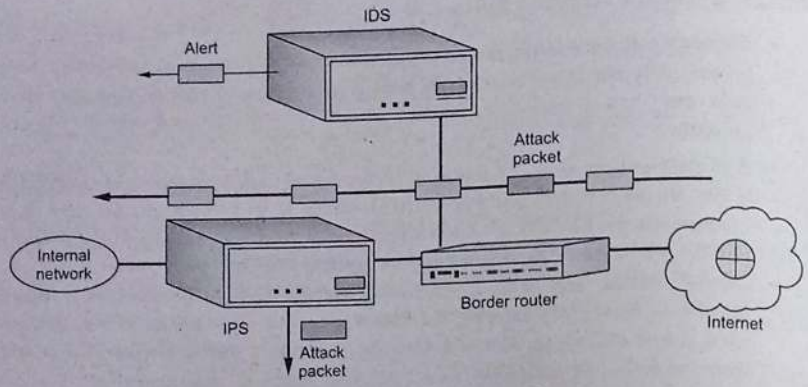

Fig. 5.1.3 IDS and IPS placement

Review Questions

1. *Explain statistical anomaly detection and rule based intrusion detection.* **AU : May-14, Marks 16**
2. *Discuss the architecture of distributed intrusion detection system with the necessary diagrams. Illustrate the three common types of firewalls with diagrams.* **AU : Dec.-14, Marks 16**
3. *Explain the intrusion detection techniques.* **AU : Dec.-15, Marks 16**
4. *Explain Intrusion Detection System (IDS) in detail with suitable diagram.* **AU : May-17, Marks 16**

5.2 Password Management

- In most cases, intruders need to acquire protected information, most often passwords. Password security is a big problem on any system : Hackers may take over someone's user account and use it in a major attack inside that system or against a totally different system; liability may involve the careless user.
- The system protects the user passwords in two ways
  1) Keeps them "encrypted" on the disk; in fact, one keeps on the disk hashes of the password : In this way, nobody can attack the system by trying to "decrypt" the password file.
  2) The file with the user personal information should be public so that when the user initiates login, the login process can check his data.
  3) The password file should be "hidden" : */etc/passwd*, */etc/shadow* in Linux.

- To break the password file, the attacker essentially has to "guess" the password of a user, hash it and then compare it with the entry in the password file.
- In UNIX, the 8 characters of the password are converted to a 56-bit string that serves as key for (modified with 12-bit "salt"value) DES. It start with 64 bits all 0 and iterate DES encryption 25 times: the result will be the hash of the password and will be stored in the file.
- The salt prevents duplicate passwords from showing in the password file. Fig. 5.2.1 shows loading a new password.

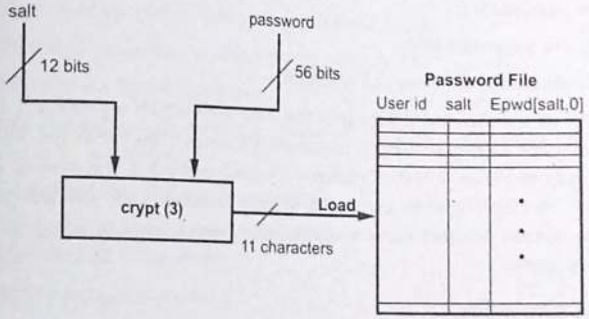

Fig. 5.2.1 Loading a new password

- Ciphertext password is stored in the table together with Salt. UNIX passwords were kept in a publicly readable file, *etc/passwords*. Now they are kept in a "shadow" directory and only visible to "root".
- The salt serves three purposes :
  1) Prevents duplicate passwords from being visible in the password file. //Even if two users choose the same password, their ciphertexts will differ//
  2) Effectively increases the length of the password by two chars. //Makes password guessing difficult//
  3) Prevents the use of hardware implementations of DES.

5.2.1 Password Protection

- Password is a front line protection against the unauthorized access (intruder) to the system. A password authenticate the identifier (ID) and provides security to the system. Therefore almost all systems are password protected.

1] Password vulnerability

Passwords are extremely common. Passwords can often be guessed. Use of mechanisms to keep passwords secret does not guarantee that the system security can not be broken. It only says that it is difficult to obtain passwords. The intruder can always use a trial and error method. A test of only a limited set of potential strings tends to reveal most passwords because there is a strong tendency for people to choose relatively short and simple passwords that they can remember. Some techniques that may be used to make the task of guessing a password difficult are as follows

1. Longer passwords.
2. Salting the password table.
3. System assistance in password selection.

The length of a password determines the ease with which a password can be found by exhaustion. For example, 3-digit password provides 1000 variations whereas a four digit passwords provides 10,000 variations. Second method is the system assistance. A password can be either system generated or user selected. User selected passwords are often easy to guess. A system can be designed to assist users in using passwords that are difficult to guess.

2] Encrypted passwords

Instead of storing the names and passwords in plain text form, they are encrypted and stored in cipher text form in the table. In this case, instead of directly using a user specified name and password for table lookup, they are first encrypted and then the results are used for table lookup. If the stored encoded password is seen, it can not be loaded, so the password cannot be determined. The password file does not need to be kept secret.

3] One time passwords

Set of paired passwords solve the problem of password sniffing. When a session begins, the system randomly selects and presents one part of a password pair; user must supply the other part. In this, user is challenged and must respond with the correct answer to that challenge. In this method, the password is different in each instance. One time passwords are among the only ways to prevent improper authentication due to password exposure. Commercial implementations of one time password system such as secur ID, use hardware calculators.

Password selection strategies

- Too short password is too easy to guess. If the passward is 8 random character, it is impossible to crack the password. In order to eliminate gaussable passwords four basic techniques are suggested.
  1. User education

  2. Computer generated password
  3. Reactive password checking
  4. Proactive password checking

5.2.2 Password Selection Strategies

- Goal : Eliminate guessable passwords while allowing users to select passwords that are memorable.

1. User education
   - ○ Told the importance of hard-to-guess passwords.
   - ○ Provided guidelines to select strong passwords.
   - ○ Many users ignore guidelines.
2. Computer-generated passwords. Passwords will be random in nature and will be hard to memorize.
   - ○ Disadvantage : Difficult to remember.
   - ○ Programs exist to generate random passwords that can be pronounced, but still difficult to remember
3. Reactive password checking.
   - ○ System runs its own password checker to find guessable passwords.
   - ○ Users given a deadline to change the password.
4. Proactive password checking.
   - ○ A user is allowed to select his password.
   - ○ At the time of selection, the system checks to see if the password is allowable.
   - ○ It rejects the password if not allowable.
   - ○ The most promising approach.
   - ○ Problem : How to efficiently and effectively check for passwords. It is not practical to maintain a list of bad passwords and check it.

5.3 Firewalls

AU : May-15,18,19, Dec.-16,17,19

- Information systems in an organization have changed vary rapidly over the years from centralized data processing, LANs, WANs and Internet connectivity.
- The Internet connectivity is essential for the organization enabling access to outside world. Also it is a threat to the organization if not secured from intrusions (unauthorized access/users).

- A firewall is inserted between the Internet and LAN for security purpose. The firewall protects the LAN from Internet-based attacks and also provides security and audits.
- A firewall may be a hardware or a software program running on a secure host computer. A firewall is placed at junction or gateway between the two networks.
- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed to. A firewall placed between a private or corporate network and a public network (Internet) is shown in Fig. 5.3.1.

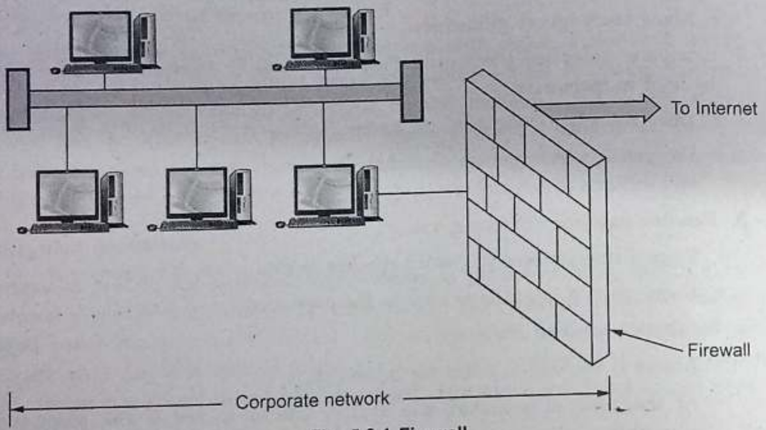

Fig. 5.3.1 Firewall

- The term firewall comes from the fact that by segmenting a network into different physical subnetwork, they limit the damage that could spread from one subnet to other just like firedoors or firewalls.

Capabilites of firewall

- A firewall examines all traffic routed between the two networks to see if it meets the certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.

- Firewalls can filter packets based on their source and destination addresses and port numbers. This known as **address filtering**.
- Firewalls can also filter specific types of network called **protocol filtering** because the decision to forward or reject traffic is dependent upon the protocol used. For example, HTTP, FTP, Telnet.
- Firewalls can also filter traffic by packet attribute or state.

Limitations of firewall

- A firewall cannot prevent individual users with modems from dialing into or out of the network, by passing the firewall altogether.
- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone.

Firewall technology

- Firewall technology generally falls into one of the two categories. Network level and application level.

  1. Network level : This guards the entire network from unauthorised intrusion. An example of this technology is packet filtering, which simply reviews all information coming into a network and rejects the data that does not meet a predefined set of criteria.

  2. Application level : This technology controls access on an application by application basis. For example, proxy servers can be set up to permit access to some application, such as HTTP, while blocking access to others, such as FTP.

Design goals

- Firewalls are very effective means for network based security threats. The design goals for firewall are as under
  1. All the traffic must pass through firewall both from inside to outside and outside to inside.
  2. Only authorized traffic defined by local security is allowed to pass.
  3. Firewall itself is immune to penetration.

- Generally four techniques are used to control access and enforce the security policy, these techniques are -
  1. Service control
  2. Direction control
  3. User control
  4. Behavior control.

1. Service control : • Service control determines the types of Internet services that are allowed to access both inbound and outbound traffic.

- The firewall may filter the traffic on the basis of IP address and TCP port number. The firewall provide proxy software to receive and interpret each service request before passing it on.

2. Direction control : • Direction control determines the direction in which particular service requests may be initiated and is allowed to flow through the firewall.

3. User control : • User control gives access to a service according to which user is attempting to access it. This feature is usually applied for local user inside the firewall perimeter.

4. Behavior control : • Behavior control allows to control the use of any particular service. For example, the firewall may filter e-mails to eliminate spam.

5.3.1 Types of Firewall

- Commonly used firewalls from threats of security are
  1. Packet filtering router
  2. Application level gateways
  3. Circuit level gateways.

5.3.1.1 Packet Filtering Router

- Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router. A router is a device that receives packets from one network and forwards them to another network.
- In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator. Rules can include source and destination IP address, source and destination port number and protocol used.

- The advantage of packet filtering firewalls is their low cost and low impact on network performance. Most routers support packet filtering. Even if other firewalls are used, implementing packet filtering at the router level affords an initial degree of security at a low network layer.
- This type of firewall only works at the network layer however and does not support sophisticated rule based models.
- Network Address Translation (NAT) routers offer the advantages of packet filtering firewalls but can also hide the IP addresses of computers behind the firewall, and offer a level of circuit based filtering.
- Packet filtering router applies rule to each incoming and outgoing IP packet, according forward or discards it. Fig. 5.3.2 shows packet filtering router.

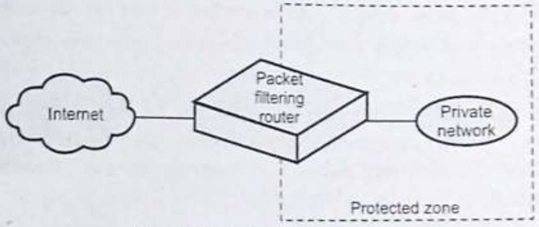

Fig. 5.3.2 Packet filtering router

- Filtering rules are based on information contained in the network packet such as
  i. Source IP address
  ii. Destination IP address
  iii. Source and destination transport level address.
  iv. IP field.
  v. Interface
- Attackers can try and break the security of the packet filter by using following techniques.
  i. IP address spoofing.
  ii. Source routing attacks
  iii. Tiny fragment attacks
- Packet filtering provides a useful level of security at low cost. The type of router used in packet filtering is a screening router.

Screening router

- Each packet has two parts : The data that is part of the document and a header. If the packet is an envelope, then the data is the letter inside the envelope and the header is the address information on the outside.
- Here packet filter to refer to the technology or the process that is taking place and the screening router to refer to the thing that's doing it.
- Screening router can be a commercial router or a host-based router with some kind of packet filtering capability. Typical screening routers have the ability to block traffic between networks or specific hosts, on an IP port level. Some firewalls consist of nothing more than a screening router between a private network and the Internet.
- Screening routers operate by comparing the header information with a table of rules set by the network administrator to determine whether or not to send the packet on to its destination. If there is a rule that does not allow the packet to be sent on, the router simply discards it.

Working of packet filters

- Packet filters work by dropping packets based on their source and destination addresses or ports. Configuring a packet filter is a three step process.
  1) First of course, one must know what should and what should not be permitted.
  2) The allowable types of packets must be specified, in terms of lofical expression on packet fileds.
  3) Finally the expression should be rewritten in whatever syntax your vendor supports.
- In general, for each packet, the router applies the rules sequentially, starting with the first one, until the packet fits or until it runs out of rules.
- For examples a router has 3 rules in its table.
- **Rule 1 :** Don't allow packets from a particular host, called TROUBLEHOST.
- **Rule 2 :** Let in connections into out mail gateway (using SMTP), located at port 25 on out host.
- **Rule 3 :** Block everything else.
- When a packet arrives at the screening router, the process works like this
  1. The packet filter extracts the information it needs from the packet header. In this example, it uses the local and external host identification and the local and external port numbers.
  2. The packet filter compares that information with the rules in the table.

  3. If the packet is from TROUBLEHOST, no matter what its destination, discard it.
  4. If the packet makes it past the first rule i.e. it's not from TROUBLEHOST, check to see if it's intended for port 25 on out SMTP-Mail host. If it is, send it on ; otherwise, discard it.
  5. If neither of the first two rules apply, the packet is rejected by rule three.
- Every packet has a set of headers containing certain information. The information is
  a) IP source address. b) IP destination address.
  c) Protocol (whether the packet is a TCP, UDP or ICMP packet).
  d) TCP or UDP source port. e) TCP or UDP destination port.
  f) TCP ack flag.

1. Inspection module

- If the header information listed above doesn't give you enough elements for setting up rules, you can use a packet filter that has an inspection module. An inspection module looks at more of the header information ; some can even look at the application data itself.
- For example, by inspecting the application data, the module can deny packets the contain certain application commands, such as the FTP put command or the SNMP set command.

2. State evaluation

- The header of a TCP packet contains an indicator called the ACK flag. When the ACK flag is set, it means that the incoming packet is a response to an earlier outgoing packet.
- If the flag is not set, the packet is not a response to an earlier outgoing packet, and therefore is suspect.
- It's common to set a screen rule to allow incoming packets that have the ACK flag set and reject those that don't.
- UDP doesn't use an ACK flag or any other similar indicator, so there's no way for the screening router to know whether an incoming packet was sent in response to an outgoing packet. The only safe thing to do in that situation is to reject the packet.
- That's where state evaluation comes in a screening router that has the state evaluation capability, "remembers" the original outgoing packet for a certain length of time (set by system administrator).

Advantages of packet filters

1. Low impact on network performance.
2. Packet filters are normally transparent to user.
3. Relatively inexpensive price.

Disadvantages of packet filtering firewall

1. They are vulnerable to attacks aimed at protocol higher than the network layer protocol.
2. They cannot hide the network topology.
3. Packet filtering firewall can not support all Internet applications.
4. These firewalls have very limited auditing capabilities.
5. Sometimes user level authentication do not supported by packet filtering firewall.

5.3.1.2 Application Level Gateways

- Application level gateways, also called proxies, are similar to circuit level gateways except that they are application specific. They can filter packets at the application layer of the OSI model.
- Incoming or outgoing packets cannot access services for which there is no proxy.
- In plain terms, an application level gateway that is configured to be a web proxy will not allow any FTP, gopher, Telnet or other traffic through.
- Because they examine packets at application layer, they can filter application specific commands such as http:post and get, etc. This cannot be accomplished with either packet filtering firewalls or circuit level neither of which know anything about the application level information.
- Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance. This is because of context switches that slow down network access dramatically. They are not transparent to end users and require manual configuration of each client computer.

Fig. 5.3.3 shows application level gateway.

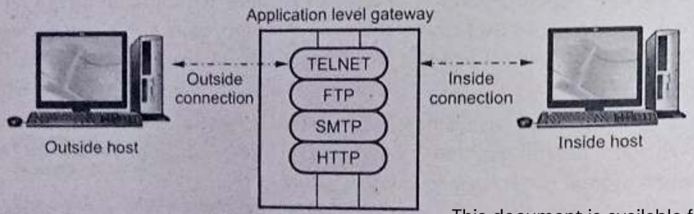

Fig. 5.3.3 Application gateway

Advantages

1. Application gateway provides high level of security than packet filters.
2. Easy to configure.
3. They can hide the private network topology.
4. It support user level authentication.
5. Capability to examine the all traffic in detail.

Disadvantages

1. High impact on network performance.
2. Slower in operation because of processing overheads.
3. Not transparent to users.

5.3.1.3 Circuit Level Gateways

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks.
- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.
- The circuit level gateway does not permit end-to-end TCP connection but two TCP connections are set-up. A typical use of circuit level gateway is in situations when system administrator trusts the internal users.

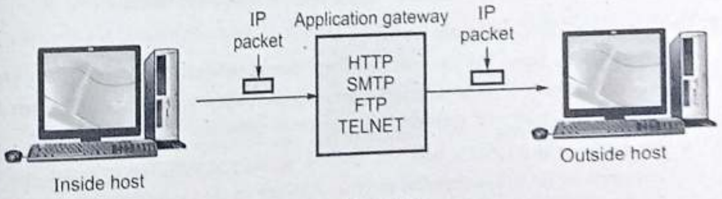

Fig. 5.3.4 Circuit gateway

5.3.1 Comparison between Packet Filter and Proxies

Sr. No.	Packet filter	Proxy (Application level)
1.	Works at network layer of OSI and IP layer of TCP.	Works at application layer of OSI, TCP layer of TCP.
2.	Low impact on network performance.	High impact on network performance.
3.	Low level of security as compare to proxi.	High level of security.
4.	Packet filtering is not effective with the FTP protocol.	FTP and Telnet are allowed into the protected subnet.
5.	Simple level of security and faster than proxy firewall.	Capability to examine the traffic in detail, so slower than packet filtering.
6.	Normally transparent to the users.	Not transparent to the users.
7.	Difficult to configure as compare to proxy.	Easier to configure than packet filtering.
8.	They cannot hide the private network topology.	They can hide the private network topology.

5.3.2 Firewall Location

1. DMZ network (Demilitarized Zone)
2. Virtual Private Network (VPN)
3. Distributed firewall

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

1. DMZ Network (Demilitarized Zone)

- Connections from the internal and the external network to the DMZ are permitted, while connections from the DMZ are only permitted to the external network, hosts in the DMZ may not connect to the internal network.
- This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ. The DMZ is typically used for connecting servers that need to be accessible from the outside world, such as e-mail, web and DNS servers.
- Fig. 5.3.5 shows DMZ network.

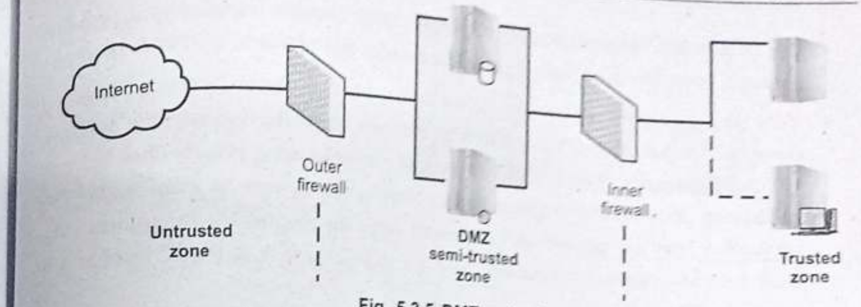

Fig. 5.3.5 DMZ network

- Traffic from the Internet is filtered, but some of it is allowed to reach systems in the DMZ i.e. like web servers and mail servers. If an attacker succeeds in breaking into a system in your DMZ, they won't gain access to your internal network as traffic coming from the DMZ is filtered before being allowed into the internal network.
- To create a DMZ, you can use two firewalls. Our illustration shows an outer firewall that separates the DMZ from the Internet and an inner firewall that separates the DMZ from the internal network. The outer firewall controls the traffic from the Internet to the DMZ. The inner firewall controls traffic from the DMZ to the internal network.
- The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network.
- Internal firewalls serve three purposes :

  i. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.

  ii. The internal firewall provides two-way protection with respect to the DMZ.

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

2. Virtual Private Networks (VPN)

- Virtual Private Networks (VPN) provide an encrypted connection between a user's distributed sites over a public network (e.g., the Internet). By contrast, a private network uses dedicated circuits and possibly encryption.

- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, a VPN is needed.
- VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. 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.

3. Distributed Firewall

- A distributed firewall configuration involves stand-alone firewall devices plus host based firewalls working together under a central administrative control. Security policy is defined centrally and enforcement of policy is done by network endpoint(s).
- Administrators can configure host resident firewalls on hundreds of servers and workstations as well as configure personal firewalls on local and remote user systems.
- Tools let the network administrator set policies and monitor security across the entire network. These firewalls protect against internal attacks and provide protection tailored to specific machines and applications. Stand-alone firewalls provide global protection, including internal firewalls and an external firewall.

5.3.3 Firewall Configuration

- Firewall configuration are of three types :
  1. Screened host, single homed bastion host
  2. Screened host, dual homed bastion host
  3. Screened subnet.

1. Screened host, single homed bastion host

- In this system, firewall consists of two systems : A packet filtering router and a bastion host.
- The router is configured so that,
  1. For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
  2. For traffic from the internal network, only IP packets from the bastion host allowed out.

- Fig. 5.3.6 shows screened host, single homed bastion host.

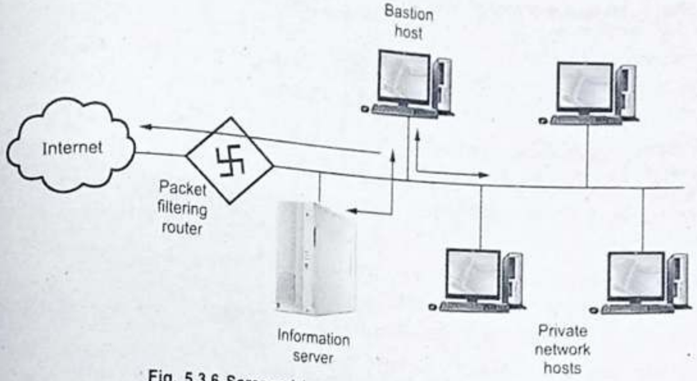

Fig. 5.3.6 Screened host, single homed bastion host

- The bastion host performs authentication and proxy functions.
- This configuration affords flexibility in providing direct internet access.

2. Screened host, dual homed bastion

- Fig. 5.3.7 shows dual homed bastion.

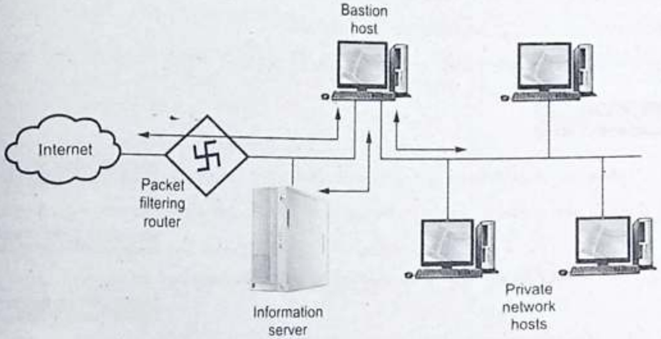

Fig. 5.3.7 Dual homed bastion

- This configuration prevents a security breach. The advantages of dual layers of security that were present in the previous configuration are present as well.
- An information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy.

3. Screened subnet

- Fig. 5.3.8 shows screened subnet.

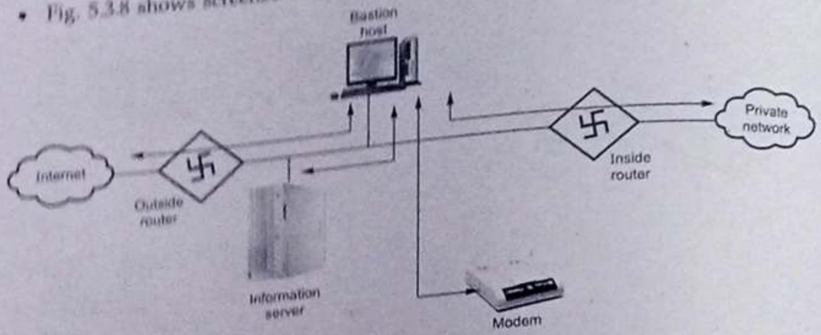

Fig. 5.3.8 Screened subnet

- This configuration creates an isolated subnetwork which may consists of simply the bastion host but may also include one or more information servers and modems for dial-up capability.

Advantages

1. There are now three levels of defense to thwart intruders.
2. Internal network is invisible to the Internet.
3. The systems on the inside network cannot construct direct routes to the internet.

Review Questions

1. *Explain the characteristics and types of firewall.* **AU : May-15, Marks 16**
2. *Explain the technical details of firewall and describe any three types of firewall with neat diagram.* **AU : Dec.-16, Marks 16**
3. *Discuss how firewalls help in the establishing a security framework for an organization.* **AU : Dec.-17, Marks 16**
4. *How does screened host architecture for firewalls differ from screened subnet firewall architecture ? Which offers more security for information assets on trusted network ? Explain with neat sketch.* **AU : May-18, Marks 16**
5. *Explain the various types of firewalls with neat diagrams.* **AU : May-19, Marks 13**
6. *Explain in detail about the types of firewalls and mention the design criteria of a firewall to protect the host machines in an educational institution.* **AU : Dec.-19, Marks 13**

5.4 Blockchain

- Blockchain technology is a decentralized, distributed ledger that stores the record of ownership of digital assets. Any data stored on blockchain is unable to be modified, making the technology a legitimate disruptor for industries like payments, cyber-security and healthcare.
- Bitcoin stores all its transactions onto a public database called as **blockchain**.
- A blockchain is a computer file for storing data. Or, it is an open, distributed database. The data is distributed (i.e. duplicated) across many computers, and the whole blockchain is entirely decentralised.
- This means no one person or entity (say, a government or corporation) has control over the blockchain; this is a radical departure from the centralised databases that are controlled and administered by businesses and other entities.
- A blockchain is an open, distributed database - Essentially, a computer file for storing information (data). The name comes from its structure : The file is made up of blocks of data and each block is linked to the previous block, forming a chain. Each block contains data (such as transaction records), plus a record of when that block was edited or created.
- Blockchain technology consists of three important concepts : blocks, nodes and miners
- A blockchain can be broken down into two components: the block and the chain.
- A block is a collection of data that is linked to other blocks chronologically in a virtual chain. Each block also contains a timestamp and so it is clear when the data was recorded and stored.
- Attractive properties of Blockchain.
  1 Log of data with digital signature
  2 Immutable
  3 Cryptographically secure , privacy preserving
  4 Provides a basis for trusted computing on top of which applications can be built.

5.4.1 Blockchain Technology Layers

- Blockchain technology consists of five layers : Application and presentation layers, data layer, network layer, consensus layer, infrastructure or hardware layer.
- However, blockchain technology layers can also be categorized as : Layer 0, Layer 1, Layer 2 and Layer 3

- Fig. 5.4.1 shows Blockchain technology layers.

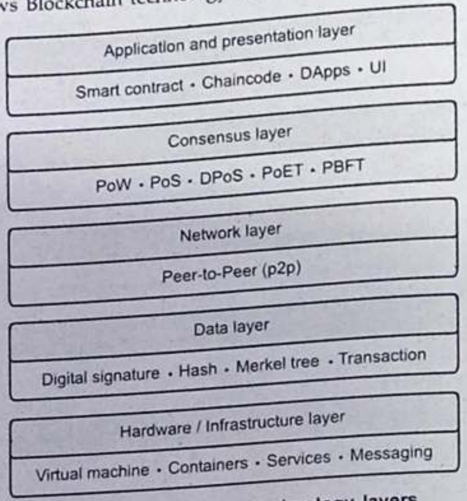
Application and presentation layer
Smart contract · Chaincode · DApps · UI
Consensus layer
PoW · PoS · DPoS · PoET · PBFT
Network layer
Peer-to-Peer (p2p)
Data layer
Digital signature · Hash · Merkel tree · Transaction
Hardware / Infrastructure layer
Virtual machine · Containers · Services · Messaging

Fig. 5.4.1 Blockchain technology layers

1. The Hardware Infrastructure Layer

- Blockchain data lies securely stored in a data server. When users browse the web or use any blockchain apps, machines request access to this data from the server. The framework that facilitates this data exchange is known as the **client-server architecture.**
- Blockchains are peer-to-peer networks that allow clients to connect with 'peer-clients' to make data sharing faster and easier.

2. The Data Layer

- A blockchain is a series of hashed blocks carrying transactional records. The first block of the blockchain is the Genesis block. After that, every new block added to the blockchain is linked to the Genesis block through an iterative process. And thus, in this way, the blockchain keeps on expanding.
- Every transaction is 'digitally signed' using the sender's wallet private key.

3. The Network Layer

- The P2P framework enables various nodes to exchange transaction data to arrive at a consensus about the validity of a transaction. This means that every node must be able to discover other nodes on the network for fast communication.

- It is the network layer that facilitates this 'inter-node communication'. As node discovery, block creation and block addition are also managed by this layer, it is also referred to as the 'propagation layer.'

4. The Consensus Layer

- This layer is responsible for transaction authentication. Without this layer, the transaction validation will not take place, thus leading to system failure. This layer implements the protocol, which needs a specific number of nodes to validate a single transaction.
- Multiple blocks may be formed concurrently, resulting in a branch in the blockchain due to a large number of nodes processing transactions, bundling them and adding them to the blockchain. However, a single chain block addition is required at all times and the consensus layer guarantees that this dispute is addressed.

5. Application and Presentation Layer

- The application layer consists of the programs that end-users take advantage of to establish blockchain network communication. Smart contracts, decentralized applications, Scripts, User Interfaces, APIs and Frameworks Constitute the application layer.

5.4.2 Types of Blockchain Platforms

- Four different kinds of blockchain architecture are public, private, consortium and hybrid blockchains.

1. Public Blockchain

- A public blockchain is a fully decentralized platform where anyone can read and send transactions. The valid transactions are included in the ledger.
- A public blockchain is a non-restrictive, permission-less distributed ledger system.
- Public blockchains are secured by cryptoeconomics, a combination of economic incentives and cryptographic verification. The degree of influence in the consensus process is proportional to the quantity of economic resources brought in the system.
- Public blockchains are being used extensively in the mining and trading of bitcoins in the modern day.
- Ethereum, provider of a decentralized platform and programming language that helps running smart contracts and allows developers to publish distributed applications.
- Public blockchains tend to have longer validation times for new data than private blockchains.

- Example : Bitcoin, Ethereum, Litecoin.

2. Private Blockchain

- In a private blockchain, write permissions are kept centralized to one organization. In this system the access and permissions are tightly controlled and rights to modify are restricted to the central authority.
- Private blockchains are usually used within an organization or enterprises where only selected members are participants of a blockchain network.
- Private blockchains are more vulnerable to fraudulent activity and malicious actors.
- Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc.
- Examples of private blockchains are; multichain and hyperledger projects (Fabric, Sawtooth), Corda, etc.

3. Hybrid Blockchain

- Hybrid blockchains use both private and public blockchains, rather than being a standalone solution.
- Hybrid blockchains are blockchains that are controlled by a single organization but also have some supervision given by the public blockchain. This supervision is required to carry out specific transaction validations, hence hybrid blockchains are important.
- With hybrid blockchains, a company may put their data or transactions on a private blockchain to keep the information confidential but put a digital fingerprint of the data on a public blockchain to secure it.
- Example of a hybrid blockchain is Dragonchain.

4. Consortium Blockchain

- Consortium blockchains are permissioned blockchains governed by a group of organizations, rather than one entity, as in the case of the private blockchain.
- Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security.
- Consortium or federated blockchains operate with a particular group of participants who control the blockchain, rather than a single entity. This group sets the rules, edits or cancels incorrect transactions and solicits cooperation among its members, according to a Blockchain Council report.
- However, setting up consortiums can be a fraught process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk.

- Consortium blockchains are only useful for smaller groups where the identity of the participants can be determined.
- Examples of a consortium or federated blockchain include Hyperledger, Corda and Quorum.

5.4.3 The Challenges for Adoption of Blockchain

- Inefficient Technological Design.
- Low Scalability : Another one of the challenges of implementing blockchain is scalability. In reality, blockchains work fine for a small number of users. When the user number increases on the network, the transitions take longer to process. As a result, the transactions cost higher than usual and this also restricts more users on the network.
- High Energy Consumption : Energy consumption is another blockchain adoption challenge. Most of the blockchain technology follows Bitcoin's infrastructure and uses proof of work as a consensus algorithm.
- No Regulation : This is one of the main challenges of implementing blockchain in an organization. Many organizations are making blockchain technology a means of transaction. There aren't any specific regulations about it. So, no one follows any specific rules when it comes to the blockchain.
- Blockchains Can Be Slow : The blockchain is complex. That's why it takes more time to process any transactions. Also, the encryption of the system makes it even slower.
- Data Format : The success of utilizing Blockchain capabilities depends on how well the transaction data format has been defined in a multi-party environment and keenly observing its related characteristics such as its dependency on other information.

5.4.4 Advantages and Disadvantages of Blockchain

Advantages :

- Reduced cost and increased efficiency.
- Improved security by protection.
- Secure transactions : The blockchain responsible for keeping record of all the transactions cannot be edited or manipulated.
- High availability and accessibility
- Reliability

Disadvantages :

- High implementation costs.
- Inefficiency : It is inefficient to have several network users validating the same operations.
- Regulations : Regulatory regimes in the financial arena are a challenge for blockchain's implementation.

5.5 Cloud Security

- The NIST define cloud computing as : "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models and four deployment models."
- Cloud provider is responsible for the physical infrastructure and the cloud consumer is responsible for application configuration, personalization and data.
- Broad network access refers to resources hosted in a cloud network that are available for access from a wide range of devices. Rapid elasticity is used to describe the capability to provide scalable cloud computing services.
- Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage and deletion.
- Methods of providing cloud security include firewalls, penetration testing, tokenization, Virtual Private Networks (VPN) and avoiding public internet connections.
- Cloud security refers to an array of policies, technological procedures, services and solutions designed to support safe functionality when building, deploying and managing cloud-based applications and associated data.
- Cloud security is designed to protect the following,
  a) **Physical networks** - Routers, electrical power cabling, climate controls, etc.
  b) **Data storage** - Hard drives, etc.
  c) **Data servers** - Core network computing hardware and software
  d) **Computer virtualization frameworks** - Virtual machine software, host machines and guest machines.
  e) **Operating Systems (OS)** - Software that houses
  f) **Middleware** - Application Programming Interface (API) management.
  g) **Runtime environments** - Execution and upkeep of a running program.

  h) **Data** - All the information stored, modified and accessed.
  i) **Applications** - Traditional software services (email, tax software, productivity suites, etc.)
  j) **End-user hardware** - Computers, mobile devices, Internet of Things (IoT) devices, etc.

- Cloud computing security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. It also addresses how these services are delivered in the Public, Private, Hybrid and Community delivery models.

5.5.1 Cloud Security Challenges and Risks

- Cloud computing security challenges fall into three broad categories :
  1. **Data Protection :** Securing data both at rest and in transit.
  2. **User Authentication :** Limiting access to data and monitoring who accesses the data.
  3. **Disaster and Data Breach :** Contingency planning.
- **Data Protection :** Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys.
- **User Authentication :** Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud.
- In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data.
- **Contingency Planning :** With the cloud serving as a single centralized repository for a company's mission-critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns.
- If information is encrypted while passing through the cloud, who controls the encryption/decryption keys? Is it the customer or the cloud vendor? Most customers probably want their data encrypted both ways across the Internet using Secure Sockets Layer protocol.
- They also most likely want their data encrypted while it is at rest in the cloud vendor's storage pool. Be sure that, the customer control the encryption/decryption keys, just as if the data were still resident on own servers.
- Data integrity means ensuring that data is identically maintained during any operation.

- Cloud-based services will result in many mobile IT users accessing business data and services without traversing the corporate network. This will increase the need for enterprises to place security controls between mobile users and cloud-based services.
- Placing large amounts of sensitive data in a globally accessible cloud leaves organizations open to large distributed threats, attackers no longer have to come onto the premises to steal data and they can find it all in the one "virtual" location.
- Virtualization efficiencies in the cloud require virtual machines from multiple organizations to be co-located on the same physical resources. Although traditional data center security still applies in the cloud environment, physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server.
- Operating system and application files are on a shared physical infrastructure in a virtualized cloud environment and require system, file and activity monitoring to provide confidence and auditable proof to enterprise customers that their resources have not been compromised or tampered with.
- In the cloud computing environment, the enterprise subscribes to cloud computing resources and the responsibility for patching is the subscriber's rather than the cloud computing vendors.
- The need for patch maintenance vigilance is imperative. Lack of due diligence in this regard could rapidly make the task unmanageable or impossible, leaving with "virtual patching" as the only alternative.
- Confidentiality : Confidentiality refers to limiting information access. Sensitive information should be kept secret from individuals who are not authorized to see the information.
- In cloud environments, confidentiality primarily pertains to restricting access to data in transit and storage.
- Integrity can extend to how data is stored, processed and retrieved by cloud services and cloud-based IT resources.
- Some common cloud security threats include :
  a) Risks of cloud-based infrastructure including incompatible legacy IT frameworks and third-party data storage service disruptions.
  b) Internal threats due to human error such as misconfiguration of user access controls.
- External threats caused almost exclusively by malicious actors, such as malware, phishing, and DDoS attacks.

5.5.2 General Issues Securing the Cloud

- The common security issues around cloud computing divided into four main categories :
  a) **Cloud infrastructure, platform and hosted code :** This comprises concerns related to possible virtualization, storage and networking vulnerabilities.
  b) **Data :** This category comprises the concerns around data integrity, data lock in, data remanence, provenance and data confidentiality and user privacy specific concerns.
  c) **Access :** This comprises the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication and user identity management.
  d) **Compliance :** Because of its size and disruptive influence, the cloud is attracting attention from regulatory agencies, especially around security audit, data location; operation trace - ability and compliance concerns.

5.6 IoT Security

- Internet of Things (IoT) security is an approach to safeguard IoT devices connected across a network with protective measures while also preventing cyber-attacks.
- IoT security refers to a strategy of safeguards that help protect these internet-enabled devices from cyber attacks. It's a fairly new discipline of cybersecurity, given the relatively recent introduction to these non-standard computing devices.
- IoT security provides blanket protection to networks, systems, devices and data from a host of IoT security attacks.
- The two key goals of IoT security are to :
  1. Make sure all data is collected, stored, processed and transferred securely.
  2. Detect and eliminate vulnerabilities in IoT components.
- IoT security is part of the organization's overall cybersecurity strategy. It is important to treat connected devices with the same level of security as they would a traditional endpoint, such as a computer or smartphone.

5.6.1 IoT Security Challenges

- IoT devices encounter several security challenges that pose a risk for organizations and enterprises using them.

- Certain notable IoT security challenges :
  1. Many IoT devices lack built-in security - Improper handling of device-related security risks, which primarily emerges because these devices don't get regular updates.
  2. Weak credentials and default passwords make devices vulnerable to brute force attacks or password hacking.
  3. Ongoing hybridization of both ransomware and malware strains makes devices vulnerable to different types of attacks.
  4. Use of IoT botnets for mining cryptocurrency risks the confidentiality, integrity and availability of data in IoT devices.
  5. Lack of encryption - One of the greatest threats to IoT security is the lack of encryption on regular transmissions. Many IoT devices don't encrypt the data they send, which means if someone penetrates the network, they can intercept credentials and other important information transmitted to and from the device.

5.7 Two Marks Questions with Answers

Q.1 What is an intruder ?

Ans. : Accessing a network unauthorizedly is called intrusion.

Q.2 What is intrusion detection system ?

Ans. : An Intrusion Detection System (IDS) is a system for detection unauthorized access to the system.

Q.3 What are the design goals of firewalls ?

Ans. : 1. All the traffic must pass through it.

2. Only authorized traffic is allowed to pass.

3. Firewall itself is immune to penetration.

Q.4 Who is masquerader and who is clandestine user ?

Ans. : 1. **Masquerader :** An unauthorized user who penetrates a system access control and exploit an user account.

2. **Clandestine user :** A user who seizes supervisory control of system to suppress audit collection.

Q.5 What are the major issues derived by Porras about the design of a distributed intrusion detection system ?

AU : May-10, CSE

Ans. : Porras points out foll