Notes In Hindi

SUBJECT

Information Security

PREPARED BY

TEAM NOTESINHINDI

Notesinhindi.com

2026 Edition

Unit 1: Introduction to Information Security

Information Security की Introduction, Various Aspects (PAIN), और Operating Systems की Security Features — Authentication, Logs, Audit, File System Protection, User Privileges, RAID Options, Anti-Virus Software

1. Introduction to Information Security

> **Information Security** एक ऐसी practice है जिसमें digital information (data) को **unauthorized access, use, disclosure, modification, ya destruction** से बचाया जाता है। आसान भाषा में कहें तो, यह एक तरीका है जिससे हमारे important data, systems और networks को hackers, viruses aur अन्य खतरों से सुरक्षित रखा जाता है।

- आज के digital युग में data ही सबसे बड़ा asset है — बैंक details, personal information, company records — इन सबको protect करना बहुत ज़रूरी है, इसीलिए Information Security की ज़रूरत पड़ती है।
- Information Security सिर्फ computer viruses से बचाव तक सीमित नहीं है, बल्कि इसमें physical security (जैसे server room को lock रखना), network security, और policies/procedures भी शामिल होती हैं।
- इसका main goal होता है data की **Confidentiality (गोपनीयता)**, **Integrity (सत्यनिष्ठा)**, और **Availability (उपलब्धता)** को बनाए रखना — इसे **CIA Triad** भी कहा जाता है।
- Information Security को organizations, government agencies, और individuals — सभी level पर लागू किया जाता है, क्योंकि data breach किसी को भी बहुत नुकसान पहुँचा सकता है।

1.1 Information Security की ज़रूरत क्यों है?

- Sensitive data (जैसे passwords, bank details, personal records) को unauthorized लोगों से बचाने के लिए।
- Cyber attacks (hacking, malware, phishing) से systems और networks को सुरक्षित रखने के लिए।
- Business की reputation और customer का trust बनाए रखने के लिए, क्योंकि data breach से company की image खराब हो सकती है।
- Legal और compliance requirements को पूरा करने के लिए (जैसे data protection laws)।
- Financial losses से बचने के लिए, क्योंकि data breach से बहुत बड़ा monetary नुकसान हो सकता है।

1.2 CIA Triad — Information Security के तीन मुख्य Goals

> Information Security के तीन core objectives को मिलाकर **CIA Triad** बनता है। यह किसी भी security system को design करते समय foundation की तरह काम करता है।

Goal	Meaning
Confidentiality (गोपनीयता)	यह ensure करना कि data सिर्फ authorized लोग ही access कर पाएँ, बाकी किसी को उसे देखने की permission न हो
Integrity (सत्यनिष्ठा)	यह ensure करना कि data बिना अनुमति के बदला (modify) न जाए, यानी data accurate और trustworthy बना रहे

Availability (उपलब्धता)	यह ensure करना कि authorized users जब भी data या system चाहें, तब वह उन्हें उपलब्ध (available) रहे

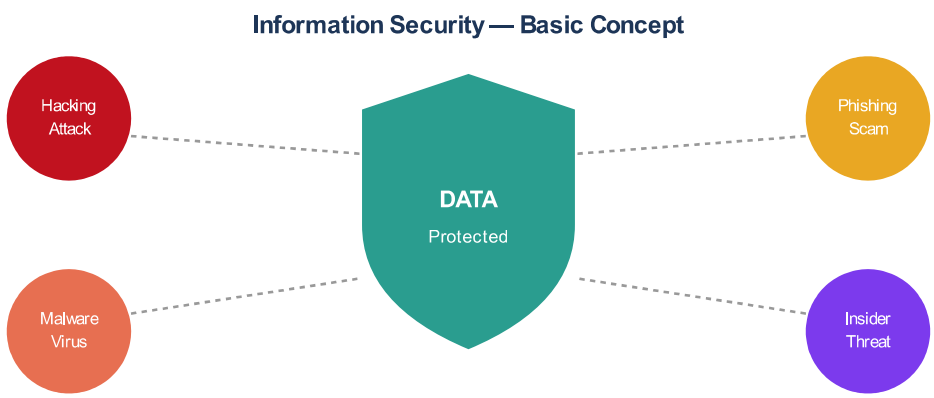
1.3 Information Security के Domains (क्षेत्र)

- **Physical Security** — hardware, servers aur equipment को physical नुकसान (जैसे चोरी, आग) से बचाना।
- **Network Security** — network से गुज़रने वाले data और traffic को unauthorized access से सुरक्षित रखना।
- **Application Security** — software aur applications में मौजूद vulnerabilities को ठीक करके उन्हें सुरक्षित बनाना।
- **Operational Security** — data को handle करने और store करने से जुड़ी processes और decisions को सुरक्षित बनाना।
- **End-User Education** — users को cyber threats (जैसे phishing) के बारे में जागरूक करना, क्योंकि इंसानी गलती security की सबसे बड़ी कमजोरी होती है।

1.4 Common Security Threats (मुख्य खतरे)

Threat	Description
Malware	Malicious software (viruses, worms, trojans) जो system को नुकसान पहुँचाने या data चुराने के लिए बनाया जाता है
Phishing	Fake emails/websites के through users को धोखा देकर उनकी sensitive information चुराना

Hacking	बिना authorization के किसी system या network में घुसकर data access करना
Denial of Service (DoS)	किसी system या server को इतने requests भेजना कि वह normal users के लिए काम करना बंद कर दे
Insider Threats	Organization के अंदर के ही लोगों (employees) द्वारा जानबूझकर या गलती से data को नुकसान पहुँचाना

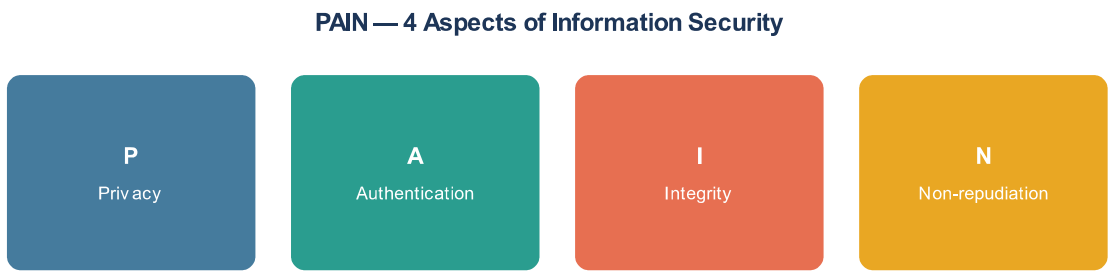


चित्र 1.1 — Information Security का काम है data को चारों तरफ से आने वाले खतरों (hacking, malware, phishing, insider threats) से सुरक्षित रखना।

Real-life Example: जब आप अपने bank के mobile app में login करते हैं, तो आपका password encrypt होकर server तक जाता है, OTP verification होता है, और आपकी transaction history secure तरीके से store होती है — यह सब Information Security की practices का ही हिस्सा है, जो आपके पैसों और डेटा को सुरक्षित रखता है।

2. Various Aspects of Information Security (PAIN)

> Information Security को अच्छे से समझने के लिए इसके चार मुख्य aspects (पहलुओं) को याद रखा जाता है, जिन्हें छोटे नाम **PAIN** से जाना जाता है — **Privacy, Authentication, Integrity, और Non-repudiation**। यह चारों मिलकर यह सुनिश्चित करते हैं कि data सुरक्षित रहे, सही व्यक्ति के पास पहुँचे, बदला न जाए, और भेजने वाला उससे मुकर न सके।



चित्र 2.1 — PAIN model के चारों aspects data को हर तरह से सुरक्षित बनाने के लिए मिलकर काम करते हैं।

2.1 Privacy (गोपनीयता)

> **Privacy** का मतलब है कि data को सिर्फ authorized (अनुमति प्राप्त) लोग ही access कर सकें, बाकी किसी को उसे देखने की permission न हो। इसे **Confidentiality** भी कहा जाता है।

- Data को unauthorized access से बचाने के लिए encryption, passwords, और access control का उपयोग किया जाता है।

- Privacy बनाए रखने से sensitive information (जैसे personal details, financial data) leak नहीं होती।
- Organizations अपने customers की privacy बनाए रखने के लिए data protection policies और legal regulations follow करती हैं।
- Privacy सिर्फ data storage तक सीमित नहीं है, बल्कि data transmission (जैसे internet पर भेजते समय) के दौरान भी बनाए रखनी होती है।

> **Example:** जब आप WhatsApp पर message भेजते हैं, तो **end-to-end encryption** की वजह से सिर्फ आप और receiver ही उस message को पढ़ सकते हैं, बीच में कोई और नहीं।

2.2 Authentication (प्रमाणीकरण)

> **Authentication** वह process है जिससे यह verify (पुष्टि) किया जाता है कि कोई व्यक्ति या system वाकई वही है जो वह होने का दावा कर रहा है।

- Authentication के बिना कोई भी व्यक्ति खुद को कोई और बताकर system access कर सकता है, इसलिए यह security का पहला कदम है।
- यह username-password, biometric (fingerprint, face), या OTP जैसे तरीकों से किया जाता है।
- Authentication हमेशा किसी resource को access करने से पहले पहला step होता है, इसके बाद ही authorization (क्या-क्या access मिलेगा) decide होता है।
- Strong authentication methods (जैसे multi-factor authentication) से account compromise होने का खतरा काफी कम हो जाता है।

> **Example:** जब आप अपने phone को fingerprint से unlock करते हैं, तो phone यह verify करता है कि यह fingerprint वाकई आपका ही है — यह authentication का example है।

2.3 Integrity (सत्यनिष्ठा)

> **Integrity** का मतलब है कि data transmission या storage के दौरान बिना अनुमति के बदला (modify) न जाए। यह ensure करता है कि receiver को वही data मिले जो sender ने भेजा था।

- Integrity check करने के लिए hashing algorithms (जैसे MD5, SHA) का उपयोग किया जाता है, जो data में हुए किसी भी छोटे से बदलाव को भी पकड़ लेते हैं।
- अगर data बीच में tamper (छेड़छाड़) हो जाए, तो integrity check यह पकड़ लेता है कि original data से mismatch है।
- Integrity सिर्फ transmission के दौरान ही नहीं, बल्कि storage में रखे गए data के लिए भी ज़रूरी होती है।
- Digital signatures भी integrity बनाए रखने में मदद करते हैं, क्योंकि इनसे data में कोई भी बदलाव तुरंत पकड़ा जा सकता है।

> **Example:** जब आप कोई software download करते हैं, तो website पर दिया गया **checksum/hash value** match करके यह verify किया जाता है कि file के साथ कोई छेड़छाड़ तो नहीं हुई।

2.4 Non-repudiation (अस्वीकृति-निषेध)

> **Non-repudiation** का मतलब है कि message भेजने वाला व्यक्ति बाद में यह इनकार (deny) नहीं कर सकता कि उसने वह message नहीं भेजा था। यानी sender अपनी action से मुकर नहीं सकता।

- यह digital signatures के through achieve किया जाता है, जो cryptographically यह prove करते हैं कि message किसने भेजा।

- Legal aur financial transactions में यह बहुत ज़रूरी होता है, ताकि disputes को solve किया जा सके।
- Non-repudiation दोनों तरफ लागू होता है — sender यह नहीं कह सकता कि उसने message नहीं भेजा, और receiver यह नहीं कह सकता कि उसे message मिला ही नहीं।
- यह Authentication और Integrity दोनों पर आधारित होता है, क्योंकि पहले identity verify होनी चाहिए और data भी unchanged होना चाहिए, तभी non-repudiation प्रभावी होता है।

> **Example:** जब कोई bank employee digitally किसी document पर sign करता है, तो वह बाद में यह नहीं कह सकता कि उसने sign नहीं किया, क्योंकि digital signature उसकी identity से permanently जुड़ी होती है।

Aspect	यह क्या Ensure करता है	Technique
Privacy	सिर्फ authorized लोग ही data access कर सकें	Encryption, Access Control
Authentication	User की identity verify हो	Password, Biometric, OTP
Integrity	Data बीच में बदला न जाए	Hashing (MD5, SHA)
Non-repudiation	Sender अपने भेजे message से मुकर न सके	Digital Signature

3. Security Features of Operating Systems

> Operating System (OS) कंप्यूटर का वह core software है जो हार्डवेयर और user के बीच bridge का काम करता है, इसलिए इसकी security बहुत महत्वपूर्ण होती है। OS कई built-in security features देता है, जो मिलकर system और data को सुरक्षित रखते हैं — जैसे Authentication, Logs, Audit Features, File System Protection, User Privileges, RAID Options, aur Anti-Virus Software।

3.1 Authentication

> Operating System में **Authentication** वह security feature है जो यह verify करता है कि system को access करने वाला व्यक्ति वाकई वही है जो वह दावा कर रहा है, इसके बाद ही उसे login करने की अनुमति मिलती है।

3.1.1 Types of Authentication

Type	Description
Password-based Authentication	User एक secret password enter करता है जो पहले से system में set किया गया होता है
Biometric Authentication	Fingerprint, face recognition, या retina scan जैसी physical characteristics से identity verify की जाती है
Token-based Authentication	Smart card या security token के through authentication किया जाता है
Multi-Factor Authentication (MFA)	दो या ज़्यादा तरीकों (जैसे password + OTP) को मिलाकर authentication किया जाता है, जिससे security और भी मजबूत हो जाती है

3.1.2 Features

- Unauthorized users को system access करने से रोकता है।
- हर user का अलग account होता है, जिससे उनकी activities को track करना आसान हो जाता है।
- Failed login attempts को limit किया जा सकता है, ताकि brute-force attacks से बचा जा सके।
- Session timeout जैसे features अपने आप user को logout कर देते हैं, अगर वह लंबे समय तक inactive रहे।
- Password policies (जैसे minimum length, special characters) enforce करके authentication को और मजबूत बनाया जा सकता है।

Advantages

- System को unauthorized access से सुरक्षित रखता है।
- हर user की identity अलग से track की जा सकती है।
- Multi-factor authentication के साथ security और भी मजबूत हो जाती है।
- Accountability बढ़ती है, क्योंकि हर action किसी specific user से जुड़ी होती है।

Disadvantages

- Password भूल जाने पर access में दिक्कत हो सकती है।
- Weak passwords use करने पर security कमजोर पड़ जाती है।
- Biometric hardware (जैसे fingerprint scanner) महंगा हो सकता है।
- Repeated authentication prompts कभी-कभी user experience को धीमा कर देते हैं।

Example: Windows या Linux में login करते समय username और password enter करना, या Gmail में login करते समय OTP verification होना — यह सब authentication के example हैं।

3.2 Logs

> **Logs** वह records होते हैं जो operating system automatically generate करता है, जिनमें system में हुई सभी important activities (जैसे login, file access, errors) का detail होता है। यह एक तरह की digital diary की तरह काम करते हैं।

3.2.1 Types of Logs

Type	Description
System Logs	OS की internal activities record करते हैं, जैसे startup, shutdown, hardware errors
Security Logs	Login attempts, authentication failures, और access control से जुड़ी events record करते हैं
Application Logs	किसी specific software/application से related events record करते हैं

3.2.2 Features और Importance

- Logs की मदद से यह पता चलता है कि system में कब, किसने, क्या किया।
- अगर कोई security incident (जैसे hacking attempt) होता है, तो logs को check करके यह पता लगाया जा सकता है कि क्या हुआ था।
- Logs troubleshooting में भी मदद करते हैं, जब system में कोई error आ रही हो।

- Logs को timestamp के साथ record किया जाता है, जिससे events का exact समय पता चलता है।
- बहुत से logs को centralized location में भेजा जा सकता है, ताकि पूरे network की activities एक जगह से monitor हो सकें।

Advantages

- Security incidents को detect और investigate करने में मदद करते हैं।
- System की performance और errors को monitor करने में useful हैं।
- Legal aur compliance requirements के लिए ज़रूरी evidence provide करते हैं।
- Unusual या suspicious pattern (जैसे बार-बार login fail होना) को पहचानने में मदद करते हैं।

Disadvantages

- बहुत ज़्यादा logs generate होने से storage space ज़्यादा लगती है।
- अगर logs को regularly analyze न किया जाए, तो वे बेकार साबित होते हैं।
- बड़ी मात्रा में logs में से सही information ढूँढना समय लेने वाला काम हो सकता है।
- अगर logs को properly secure न किया जाए, तो attacker खुद logs को भी बदल (tamper) सकता है।

Example: Windows का **Event Viewer** tool सभी system, security और application logs दिखाता है, जिससे administrator यह track कर सकता है कि system में क्या-क्या हुआ।

3.3 Audit Features

> **Auditing** एक ऐसी process है जिसमें system की activities को systematically review और analyze किया जाता है, ताकि यह check किया जा सके कि सभी security policies सही से follow हो रही हैं या नहीं।

3.3.1 Audit करने का Process

1. सबसे पहले यह decide किया जाता है कि किन events को audit करना है (जैसे login attempts, file access)।
2. System उन events की logs collect करता रहता है।
3. Administrator या auditor उन logs को periodically review करता है।
4. अगर कोई suspicious activity मिलती है, तो उस पर आगे investigation की जाती है।

3.3.2 Features

- यह पता लगाने में मदद करता है कि किसने, कब, कौन सा resource access किया।
- Compliance requirements (जैसे company policies, government regulations) को पूरा करने में मदद करता है।
- Unauthorized access attempts और policy violations को पकड़ने में useful होता है।
- Regular auditing से system में मौजूद weaknesses (कमजोरियों) को समय रहते पहचाना जा सकता है।
- Audit reports management को यह समझने में मदद करती हैं कि security policies effective हैं या नहीं।

Advantages

- Security policies को properly enforce करने में मदद करता है।
- Accountability बढ़ती है, क्योंकि हर action track होती है।
- Fraud aur misuse को detect करने में मदद करता है।
- Regulatory aur legal compliance को साबित करने के लिए proof provide करता है।

Disadvantages

- बहुत detailed auditing से system की performance थोड़ी slow हो सकती है।
- Audit data को manage करने के लिए extra resources चाहिए होते हैं।
- Skilled auditors की ज़रूरत होती है, जो हर organization के पास आसानी से उपलब्ध नहीं होते।
- अगर auditing सही तरीके से plan न की जाए, तो important events भी miss हो सकती हैं।

Example: किसी bank में employees किन-किन customer accounts को access कर रहे हैं, इसे audit करके यह ensure किया जाता है कि कोई भी employee बिना वजह किसी account की details न देखे।

3.4 File System Protection

> **File System Protection** वह security feature है जो files और folders को unauthorized access, modification, या deletion से बचाता है, ताकि सिर्फ authorized users ही उन्हें access कर सकें।

3.4.1 File System Protection के तरीके (Methods)

Method	Description
Permissions (Read, Write, Execute)	हर file/folder पर यह set किया जाता है कि कौन उसे read, write, या execute कर सकता है
Access Control List (ACL)	यह detailed list होती है जो बताती है कि कौन से specific users या groups को किस file पर कौन सी permission है
Encryption	Files को encrypt करके रखा जाता है, ताकि बिना सही key के कोई भी उन्हें पढ़ न सके
Ownership	हर file का एक owner होता है, जो यह decide कर सकता है कि बाकी लोगों को कौन सी permissions देनी हैं

3.4.2 Features

- Data को accidental या intentional नुकसान से बचाता है।
- अलग-अलग users को अलग-अलग level की access permissions दी जा सकती हैं।

- Sensitive files को unauthorized लोगों की पहुँच से दूर रखता है।
- File-level और folder-level, दोनों तरह की protection लागू की जा सकती है।
- Deleted files को भी कुछ समय तक recover करने की facility (जैसे Recycle Bin) कई file systems देते हैं।

Advantages

- Important data unauthorized access से सुरक्षित रहता है।
- अलग-अलग users के लिए customized access control possible है।
- Encryption की वजह से data चोरी होने पर भी वह पढ़ा नहीं जा सकता।
- Accidental modification या deletion का खतरा काफी हद तक कम हो जाता है।

Disadvantages

- Permissions को गलत तरीके से set करने पर authorized users भी access खो सकते हैं।
- Complex permission structures manage करना मुश्किल हो सकता है।
- Encryption/decryption की वजह से file access करने में थोड़ा extra time लग सकता है।
- अगर encryption key खो जाए, तो data permanently access करना मुश्किल हो सकता है।

Example: Windows में किसी folder पर right-click करके "Properties → Security" में जाकर यह set किया जा सकता है कि कौन सा user उस folder को सिर्फ read कर सकता है और कौन उसे edit भी कर सकता है।

3.5 User Privileges

> **User Privileges** वह rights (अधिकार) होते हैं जो किसी user को system में दिए जाते हैं, यह decide करने के लिए कि वह user कौन-कौन से resources को access कर सकता है और क्या-क्या actions perform कर सकता है।

3.5.1 Types of User Privileges

User Type	Privileges
Administrator (Root/Superuser)	पूरे system पर full control होता है — software install/uninstall करना, settings बदलना, दूसरे users को manage करना
Standard User	Limited privileges होती हैं — अपनी files access कर सकता है, लेकिन system-wide settings नहीं बदल सकता
Guest User	सबसे कम privileges होती हैं — सिर्फ basic tasks कर सकता है, कोई permanent changes नहीं कर सकता

3.5.2 Principle of Least Privilege

> यह एक important security principle है, जिसके according हर user को सिर्फ **उतनी ही privileges** दी जानी चाहिए जितनी उसे अपना काम करने के लिए ज़रूरी हैं — न कम, न ज़्यादा।

- इससे अगर किसी user का account compromise (hack) भी हो जाए, तो attacker को सीमित नुकसान ही पहुँचा पाएगा।
- यह accidental changes या misuse के risk को भी कम करता है।

3.5.3 Features

- हर user को उसके role के according अलग privileges दी जाती हैं (Role-Based Access Control)।
- Administrator किसी भी समय किसी user की privileges को बदल सकता है।
- Privileges को समय-समय पर review करके यह check किया जा सकता है कि कहीं किसी को ज़रूरत से ज़्यादा access तो नहीं मिली हुई।
- User privileges के according ही system यह decide करता है कि कौन सी files, folders, या settings किसे दिखेंगी।

Advantages

- Unauthorized या accidental system changes से सुरक्षा मिलती है।
- हर user को सिर्फ ज़रूरी access मिलने से overall system security बढ़ती है।
- अगर कोई account compromise हो जाए, तो attacker का नुकसान सीमित रहता है।
- अलग-अलग departments/roles के लिए access को आसानी से customize किया जा सकता है।

Disadvantages

- Privileges को manage करना, especially बड़े organizations में, समय लेने वाला काम हो सकता है।
- गलत privilege setting से authorized users को भी ज़रूरी access न मिलने की समस्या हो सकती है।
- बार-बार permission requests से काम की speed धीमी हो सकती है।
- Privileges की regular review न होने पर पुराने/अनावश्यक access rights बने रह सकते हैं।

> **Example:** किसी company में एक normal employee सिर्फ अपने department के software use कर सकता है, लेकिन IT administrator को पूरे network के servers और systems को manage करने की privilege होती है।

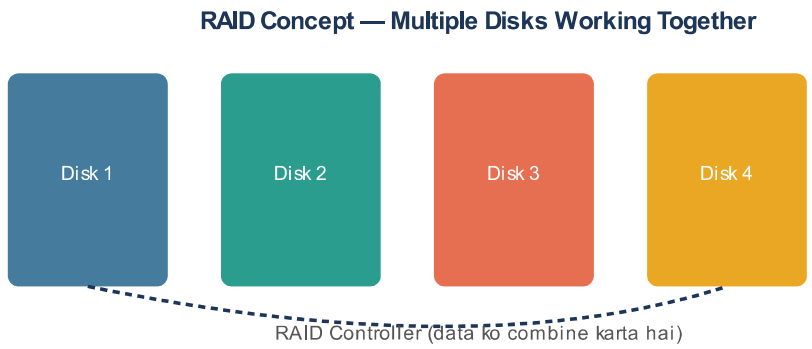
3.6 RAID Options

> **RAID (Redundant Array of Independent Disks)** एक technology है जिसमें कई hard disks को आपस में combine करके एक single logical unit बनाया जाता है, ताकि data की **redundancy (backup)** बढ़े और **performance** भी बेहतर हो।

3.6.1 Types of RAID

RAID Level	Description
RAID 0 (Striping)	Data को कई disks में बाँटकर (stripe करके) store किया जाता है, जिससे speed तो बढ़ती है लेकिन कोई redundancy (backup) नहीं होती — अगर एक disk fail हो जाए तो पूरा data चला जाता है
RAID 1 (Mirroring)	Data की exact copy दूसरी disk में भी store की जाती है, जिससे अगर एक disk fail हो जाए तो data दूसरी disk से मिल जाता है
RAID 5 (Striping with Parity)	Data को stripe करके parity information के साथ store किया जाता है, जिससे किसी एक disk के fail होने पर भी data recover हो सकता है
RAID 6	RAID 5 जैसा ही है, लेकिन double parity use होती है, जिससे एक साथ दो disks fail होने पर भी data सुरक्षित रहता है

RAID 10 (1+0)	RAID 1 aur RAID 0 का combination है — यह अच्छी speed भी देता है और अच्छी redundancy भी



चित्र 3.6.1 — RAID में कई physical disks मिलकर एक logical unit की तरह काम करते हैं, जिससे data redundancy और performance दोनों बेहतर होते हैं।

3.6.2 Features

- Data की redundancy बढ़ती है, यानी एक disk के fail होने पर भी data सुरक्षित रहता है (RAID के type के according)।
- Multiple disks पर एक साथ read/write होने से data access की speed बढ़ जाती है।
- अलग-अलग needs (speed या safety) के according सही RAID level choose किया जा सकता है।

Advantages

- Disk fail होने पर भी data loss की संभावना कम हो जाती है (RAID 1, 5, 6, 10 में)।
- Read/write performance improve होती है।

Disadvantages

- Multiple disks की वजह से hardware cost बढ़ जाती है।
- RAID 0 में redundancy बिल्कुल नहीं होती, इसलिए एक disk fail होने पर पूरा data चला जाता है।

> **Example:** Servers और data centers में RAID 5 या RAID 10 का इस्तेमाल आम तौर पर किया जाता है, ताकि disk fail होने पर भी company का data सुरक्षित रहे और business बिना रुके चलता रहे।

3.7 Anti-Virus Software

> **Anti-Virus Software** एक ऐसा program है जो computer system में मौजूद viruses, malware, worms, trojans जैसे harmful software को detect करता है, उन्हें block करता है, और ज़रूरत पड़ने पर system से remove भी कर देता है।

3.7.1 Types of Anti-Virus Detection

Type	Description
Signature-based Detection	पहले से known viruses के unique "signatures" (patterns) की database से match करके उन्हें पहचानता है
Heuristic-based Detection	Files के behavior और structure को analyze करके यह पता लगाता है कि क्या यह कोई नया, unknown virus हो सकता है
Cloud-based Detection	Cloud पर मौजूद बड़ी database का उपयोग करके real-time में नए threats को पहचानता है
Behavior-based Detection	किसी program के run होने के दौरान उसकी suspicious activities (जैसे बिना अनुमति के files बदलना) को monitor करता है

3.7.2 Working Process

1. Anti-virus software system की files aur programs को **scan** करता है।
2. हर file को known virus signatures की database से **compare** किया जाता है।
3. अगर कोई match मिलता है, तो उस file को **quarantine** (अलग करना) कर दिया जाता है, ताकि वह बाकी system को नुकसान न पहुँचाए।
4. User की अनुमति से infected file को **delete/clean** कर दिया जाता है।
5. Anti-virus regularly अपनी virus definition database को **update** करता रहता है, ताकि नए threats से भी बचा जा सके।

3.7.3 Features

- Real-time protection देता है, यानी नई files को download या open करते ही उन्हें scan कर लेता है।
- Scheduled scans set किए जा सकते हैं, ताकि पूरा system periodically check होता रहे।
- Firewall aur email scanning जैसे additional security features भी अक्सर साथ में आते हैं।

Advantages

- System को viruses और malware से सुरक्षित रखता है।
- Real-time monitoring से threats को पहले ही रोक देता है, नुकसान होने से पहले।

Disadvantages

- System के resources (RAM, CPU) थोड़ा ज़्यादा use करता है, जिससे system slow हो सकता है।
- अगर virus definitions update न हों, तो नए (latest) viruses को detect नहीं कर पाता।

Example: Windows Defender, Quick Heal, और Norton जैसे anti-virus software आम तौर पर personal computers और laptops में इस्तेमाल किए जाते हैं,

> ताकि internet से download की गई files या email attachments से आने वाले viruses से बचाव हो सके।