TASK-4

PASSWORD SECURITY & AUTHENTICATION ANALYSIS

1. Introduction:

Password security is an essential part of information security. Most online systems rely on passwords to authenticate users. If passwords are weak or improperly stored, attackers can gain unauthorized access. This report analyzes password storage methods, common attacks, authentication weaknesses, and secure authentication practices.

2. Password Storage Methods:

Modern systems do not store passwords in plain text. Instead, passwords are stored using **hashing algorithms**. Hashing converts a password into a fixed-length unreadable string. Even if the database is compromised, attackers cannot directly retrieve the original password.

3Hashing vs Encryption

Hashing

- One-way process
- Cannot be reversed
- Used for password storage

Encryption

- Two-way process
- Can be decrypted using a key
- Used for files and sensitive data

Diagram Explanation:

Password → Hash Function → Hash Value(Stored)

Encryption diagram:

Data → Encryption → Cipher Text → Decryption → Original Data

4. Types of Password Hash Algorithms

Algorithm	Security Level
MD5	Weak
SHA-1	Weak

Algorithm	Security Level
SHA-256	Moderate
bcrypt	Strong
Argon2	Very Strong

Older algorithms like MD5 and SHA-1 are vulnerable to fast cracking. Modern systems use bcrypt or Argon2 because they include salting and slow hashing.

5. Password Attacks

Dictionary Attack
Attackers use a predefined list of common passwords.
Brute Force Attack
Attackers try every possible combination until the correct password is found.

Diagram Explanation:
Attacker → Wordlist → Hash Matching → Password Found

6. Weak Password Analysis

Weak passwords fail because:

- They are short
- They use common words
- They lack symbols and numbers

Example of weak password:

password123

Example of strong password:

P@ssW0rd!9#Qz

7. Multi-Factor Authentication (MFA)

MFA adds additional security layers beyond passwords.

Factors:

1. Something you know – Password
2. Something you have – OTP / Mobile
3. Something you are – Fingerprint / Face ID

Diagram Explanation:

User → Password → OTP → Access Granted

8. Recommendations for Strong Authentication

- Use bcrypt or Argon2
- Apply password salting

- Enforce minimum password length
- Enable Multi-Factor Authentication
- Lock accounts after multiple failed attempts
- Educate users on password security

9. Conclusion

Weak passwords and outdated hashing algorithms pose serious security risks. Implementing strong hashing techniques, enforcing password policies, and enabling multi-factor authentication significantly improves system security.