**Preventive Measures**

**Strong Authentication:** Implement strong, complex passwords and consider multi-factor authentication (MFA) for all EC2 instances to resist brute force attacks.

**Security Groups and Network ACLs**: Configure security groups and network access control lists (ACLs) to restrict inbound and outbound traffic to only necessary ports and IP addresses.

**Intrusion Detection and Prevention Systems** : Deploy IDPS solutions to detect and prevent unauthorized access and reconnaissance activities.

**Patch Management**: Regularly update and patch operating systems and applications to fix vulnerabilities that could be exploited by attackers.

**SSH Key Pairs**: Use SSH key pairs for authentication instead of passwords where possible, particularly for SSH access.

**Logging and Monitoring**: Enable detailed logging and continuous monitoring of network traffic and system activities to detect and respond to suspicious activities promptly.

**Incident Response Plan**: Develop and maintain an incident response plan to quickly and effectively address security incidents.

**User Education and Awareness**: Train users on security best practices, phishing awareness, and the importance of using strong, unique passwords.

**Rate Limiting**: Implement rate limiting on login attempts to prevent brute force attacks.

**Disable Unused Services**: Turn off unnecessary services and ports on EC2 instances to reduce the attack surface.