Security Standards

Related to the transmission and storage of video and data.

1. Data Encryption

1.1. Encryption in Transit

1.1.1. Use secure protocols like **TLS (Transport Layer Security) 1.2, or higher** to encrypt video and data during transmission over networks. This ensures data cannot be intercepted and read by unauthorized parties.

1.1.2. For video streaming, **SRTP (Secure Real-time Transport Protocol)** or **HTTPS** should be used for securing real-time communication.

1.2. Encryption at Rest

1.2.1. Store sensitive video and data using strong encryption algorithms like **AES (Advanced Encryption Standard)** with a key length of at least **256 bits**.

1.2.2. Implement proper key management practices, ensuring that encryption keys are stored separately and protected.

2. Authentication and Access Control

2.1. Strong Authentication

2.1.1. Implement **multi-factor authentication (MFA)** for accessing video storage and transmission systems.

2.2. Access Control

2.2.1. Use the **principle of least privilege** to limit access to video and data only to users or systems that require it.

2.2.2. Enforce role-based access control (RBAC) or attribute-based access control (ABAC) to ensure that different users or systems have appropriate access permissions.

2.2.3. Audit access logs to track who has accessed the video and data, and ensure compliance with internal security policies.

3. Data Integrity and Validation

3.1. Hashing and Integrity Checks

3.1.1. Use cryptographic hash functions (e.g., **SHA-256**) to verify the integrity of video and data during transmission. This ensures that the content has not been tampered with in transit.

3.1.2. Implement **digital signatures** for video and data files to confirm their authenticity and integrity.

3.2. Data Validation

3.2.1. Perform data validation to prevent injection attacks (e.g., SQL injections) when interacting with video or data storage systems.

3.2.2. Ensure that only valid data formats are accepted (e.g., video codecs, resolutions) to prevent exploitation of vulnerabilities in data handling.

4. Video Streaming and Storage Security

4.1. Secure Video Streaming

4.1.1. Use **HLS (HTTP Live Streaming)** or **DASH (Dynamic Adaptive Streaming over HTTP)** with **DRM (Digital Rights Management)** or encryption to secure live video streaming.

4.1.2. Implement **watermarking** to prevent unauthorized redistribution of video content.

4.1.3. Consider using **token-based access control** to authenticate users and prevent unauthorized access to live streams.

4.2. Video Storage Security

4.2.1. Store videos in secure environments such as encrypted cloud storage or on-premises storage systems that are physically protected.

4.2.2. Implement real-time replication of data.

4.2.3. Implement backup and disaster recovery mechanisms for video storage, ensuring the availability and recovery of data in case of failure.

4.2.4. Ensure proper network segmentation, firewall rules, and intrusion detection/prevention systems (IDS/IPS) to secure storage infrastructure.

5. Compliance and Legal Requirements

5.1. Data Privacy Regulations

5.1.1. Personally identifiable information, including student images, is not collected by the system ex. via scanning.

5.1.2. Implement measures to safeguard personally identifiable information (PII) when handling video data that may contain sensitive content.

6. Monitoring and Incident Response

6.1. Logging and Monitoring

6.1.1. Implement continuous monitoring of systems handling video and data, including access logs, transaction logs, and error logs.

6.1.2. Use **SIEM (Security Information and Event Management)** systems to detect and respond to security incidents.

6.2. Incident Response Plan

6.2.1. Develop and maintain an incident response plan that includes procedures for identifying, mitigating, and recovering from security incidents related to video and data breaches.

7. Network Security

7.1. Secure Transmission Networks

7.1.1. Ensure the use of **VPNs (Virtual Private Networks)** or **MPLS (Multiprotocol Label Switching)** for transmitting sensitive video and data across public or untrusted networks.

7.1.2. Utilize **firewalls** and **intrusion prevention systems (IPS)** to protect video and data transmission paths.

7.2. Network Segmentation

7.2.1. Isolate video and data networks from other IT networks, especially if they contain sensitive content. This reduces the potential attack surface.

8. Software and Firmware Security

8.1. Path Management

8.1.1. Regularly update all software, firmware, and applications involved in the processing and storage of video and data to mitigate vulnerabilities.

8.2. Vulnerability Testing

8.2.1. Conduct regular vulnerability assessments, penetration testing, and code reviews to identify and mitigate potential threats.

9. User Training and Awareness

9.1. Security Awareness Training

9.1.1. Provide regular training to all users (including developers, administrators, and end-users) on security best practices related to video and data transmission and storage, such as avoiding phishing attacks, proper password management, and recognizing security threats.

By implementing these standards and practices, organizations can establish a secure framework for handling video and data, ensuring the protection of sensitive content and compliance with regulatory requirements.