**Topic 5. Multimedia Product Service Platform (e.g., Netflix, Spotify)**

**Application Scenarios:**

**1. Gaps:** Identify security vulnerabilities and gaps in the existing security mechanisms of multimedia product service platforms like Netflix or Spotify.

**2. Reliable Arguments for the Gaps:** Provide evidence-based arguments that support the existence of identified security vulnerabilities and gaps, with reference to real-world examples and case studies.

**3. Motivations:** Emphasize the critical motivation behind securing these platforms, considering the vast amounts of user data, payment information, and intellectual property they handle.

**4. Desired Functional and Security Features:**

• Strong data protection and confidentiality.

• Secure user authentication and authorization.

• Data integrity and authenticity assurance.

• Protection against various cyber threats like piracy and unauthorized access.

**5. Related Stakeholders:** Identify stakeholders such as content providers, users, regulatory bodies, and the platform's administrators.

**Determine Specific Algorithms:**

**• Chaotic-based Stream Cipher:**

• Known for its unpredictability and encryption efficiency.

• Suitable for secure multimedia content streaming.

• Applicable for ensuring data confidentiality in multimedia platforms.

**• AES (Advanced Encryption Standard):**

• Widely recognized symmetric encryption algorithm.

• Ensures data confidentiality and security.

• Ideal for encrypting and decrypting stored content.

**Solutions:**

**Solution Architecture:**

• Implement a hybrid cryptographic system using Chaotic-based Stream Cipher and AES.

• The components include encryption/decryption modules, key management, user authentication, and access control mechanisms.

**Detail of Functional Features:**

**• Encryption and Decryption:**

• Chaotic-based Stream Cipher for real-time data streaming.

• AES for data at rest and during transmission.

**• User Authentication and Authorization:**

• Secure user login and session management.

• Role-based access control for content distribution.

**Detail of Security Features:**

**• Confidentiality:**

• Strong encryption mechanisms to protect the confidentiality of multimedia content.

**• Authentication:**

• Secure user authentication processes to verify the identities of users and prevent unauthorized access.

**• Integrity:**

• Ensure data integrity to prevent tampering or modification of multimedia content.

**Implementation and Testing:**

**Tools or Libraries Recommendation:**

• Use programming languages like Python, Java, or C++ for implementation.

• Utilize cryptographic libraries like PyCryptodome for Chaotic-based.

Stream Cipher and existing AES libraries.

• Conduct testing using platforms such as Jupyter Notebook for code development.

**Experimental Scenarios:**

• Simulate real-time streaming of multimedia content.

• Test the AES encryption for data at rest.

**Testing Goals and Conducts:**

• Goal: Ensure that the hybrid encryption system effectively secures multimedia content and prevents unauthorized access.

• Conduct:

• Real-time streaming tests to assess the performance of Chaotic-based Stream Cipher.

• Data integrity tests for AES-encrypted content at rest.

**Deployment:**

• Deploy the hybrid encryption system in a controlled environment to assess its real-world performance and security.

References:

• Cite academic papers, textbooks, and research articles on Chaotic-based Stream Ciphers,

AES, and multimedia platform security.

**Assessment Rubric:**

**1. Quality of Research (15%):** How well the student has identified and justified gaps in the multimedia platform's security.

**2. Algorithm Selection (10%):** Appropriateness and justification for choosing Chaotic-based Stream Cipher and AES.

**3. Solution Architecture (15%):** The clarity and effectiveness of the hybrid cryptographic system's design.

**4. Functional Features (20%):** The effectiveness of the encryption, authentication, and authorization features.

**5. Security Features (20%):** How well the student has addressed confidentiality, authentication, and integrity concerns.

**6. Implementation and Testing (10%):** The effectiveness of the tesing process and its alignment with the proposed solution.

**7. Presentation and Documentation (10%):** Clarity, organization, and quality of presentation materials and project documentation.