**Case Study ID: 2320030487**

**1. Title : Analyzing the Role of OSI Layers in Ensuring Secure Online Payments**

**2. Introduction**

* **Overview** : The OSI model is very essential in establishing security frameworks for communication in online payments. All of the layers in the OSI model contribute towards security in terms of transferring data, encrypting files, and error detection and secured authentication of users.
* **Objective** : To analyze how each OSI layer contributes to the overall security of online payments and to propose methods for further strengthening payment system protocols.

**3. Background**

* **Organization/System /Description** : An e-commerce platform facilitating online transactions using third-party payment gateways such as PayPal
* **Current Network Setup :**
* **Application Layer:** HTTPS-enabled payment pages**.**
* **Transport Layer:** TLS for secure data transmission. Responsible for giving the sequencenumbers in order divides into packets and sequence into order
* **Network Layer:** Firewalls and IP monitoring. Responsible to direct packets in the shortest path
* **Data Link and Physical Layers:** Secured with VLANs and encrypted wireless communications. Transforms into frames and detect the errors

**4. Problem Statement**

* **Challenges Faced :**
* Vulnerability to man-in-the-middle (MITM) attacks at the Transport Layer.
* Lack of proper security monitoring at the Network Layer.
* Poor encryption protocols for payment information being transferred.

**5. Proposed Solutions**

* **Approach :**
* Upgrade the security solutions at every OSI layer based on encryption, authentication, and anomaly detection techniques.
* **Technologies/Protocols Used :**
* Advanced Web Application Firewalls (WAF), Secure Cookies.
* Transport Layer: Upgraded TLS (version 1.3).
* Network Layer: Intrusion Prevention Systems (IPS).
* Data Link Layer: MAC Address Filtering.

**6. Implementation**

* **Process :**

Conduct security audit to reveal the vulnerabilities on every OSI layer.

Implement new security protocols and tools

Test system integrity post-upgrade**.**

* I**mplementation :**

Installation of advanced encryption tool, like AES-256.  
use advanced monitoring tool for detecting real-time threats

* **Timeline :**

Phase 1: Security audit for 1 month  
Phase 2: Updating of protocols takes 2 months  
Phase 3: Testing and deployment will take 1 month

**7. Results and Analysis**

* **Outcomes :**

Improved end-to-end encryption for payment data.

Enhanced network monitoring to detect threats early.

Reduction in MITM attacks and unauthorized access attempts.

* **Analysis :**

Security measures significantly reduced the system’s vulnerabilities, particularly at the Application, Transport, and Network layers.

**8. Security Integration**

* **Security Measures** : Implementation of zero-trust architecture.
* Two-factor authentication (2FA) for users.
* Regular penetration testing to ensure ongoing security.

**9. Conclusion**

* **Summary**  : The OSI model's layered approach is crucial to securing online payment systems. With the reduction of vulnerabilities and deployment of updated protocols, secure communication and data protection can be ensured.
* **Recommendations :**
* Use AI-driven tools for threat detection.
* Educate users about online security practices.

**10. References :**

Research papers on OSI security frameworks.

**Citations : Reference Research papers**

* **Dierks, T., & Rescorla, E. (2008).**
* **Fielding, R. T., & Reschke, J. (2014).**

**NAME: G.Geetha**

**ID-NUMBER:2320030487**

**SECTION-NO:1**