ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 12, Issue 12, December 2022 Impact Factor 8.059 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

Comparative Study of Online Payment Security Protocols

Mr. M.S. Gaikwad
B.Sc IT Department
College of Computer Science and Multimedia,
SataraParisar, Aurangabad (Sambhajinagar)

Abstract:

The rapid expansion of online shopping, mobile commerce, and digital banking has turned secure payment systems into a critical requirement for individuals, businesses, and financial institutions. As cyber threats continue to evolve, protecting sensitive payment data such as card numbers, authentication codes, and personal credentials has become a central challenge for both service providers and users. Over the past two decades, a variety of security protocols and frameworks have been designed to reduce risks and build trust in electronic transactions. This paper presents a detailed comparative analysis of major online payment security mechanisms, including Secure Sockets Layer/Transport Layer Security (SSL/TLS), Europay–Mastercard–Visa (EMV) chip technology, 3-D Secure authentication, Secure Electronic Transaction (SET), OAuth-based authorization, and tokenization strategies. The study evaluates these protocols using technical, operational, and user-oriented criteria such as confidentiality, integrity, authentication strength, ease of deployment, scalability, and user convenience. The findings show that each protocol offers distinctive benefits while also facing specific limitations. SSL/TLS remains essential for protecting data in transit but cannot prevent fraud originating from compromised endpoints. EMV provides strong safeguards for card-present payments but is less effective for card-not-present environments. 3-D Secure and tokenization strengthen online authentication and reduce the exposure of card details, though they introduce additional processing steps. OAuth enables secure delegated authorization in modern app-based and API-driven payment systems. Based on these observations, the paper recommends a layered security strategy that integrates multiple protocols to achieve robust protection, maintain user trust, and adapt to emerging technological and regulatory challenges in the digital payment ecosystem.

Keywords:

Online payments, SSL/TLS, EMV, 3-D Secure, SET, OAuth, tokenization, payment security, comparative study etc.

Introduction:

Online payments form the backbone of today's e-commerce and digital banking world. Millions of people now shop, transfer money, and pay bills on the internet every day, making speed and convenience a normal part of financial life. However, this growth in online activity has also created new opportunities for fraud, theft, and large-scale data breaches. Hackers target payment systems

to steal card details, intercept transactions, or misuse personal information, which makes security one of the most critical challenges in digital finance.

To deal with these threats, a variety of security systems and protocols have been introduced over the years. Each one is designed to protect a different part of the payment process. Some technologies, such as Secure Sockets Layer and its successor Transport Layer Security (SSL/TLS), focus on creating a safe channel between the user and the payment server. By encrypting data during transmission, SSL/TLS prevents outsiders from reading or altering information while it travels across networks.

Other solutions provide protection beyond the communication channel. Europay–Mastercard–Visa (EMV) chip technology adds dynamic cryptography to physical card payments, making it extremely difficult to clone a card. For online transactions, 3-D Secure introduces an extra step where the cardholder's identity is verified through a password, one-time code, or biometric confirmation. More recent approaches such as tokenization replace actual card numbers with randomly generated tokens, reducing the risk of stolen data. OAuth, widely used in mobile apps and API-based systems, allows secure authorization without revealing a user's full credentials.

Together, these tools form a layered defense that balances strong security with the speed and convenience consumers expect. Understanding how these systems work and how they complement each other is essential for building safe and trustworthy online payment environments.

Objectives:

1. To explain the most widely used online payment security protocols.
2. To evaluate these protocols using technical and practical criteria.
3. To highlight their strengths and weaknesses in real-world use.
4. To suggest effective ways to combine them for maximum security.

Literature Review:

Payment security has evolved significantly in response to emerging cyber threats. Early protocols, such as Secure Electronic Transaction (SET), provided strong encryption for electronic payments but were too complex for widespread adoption (Chaum et al.). Secure Sockets Layer and Transport Layer Security (SSL/TLS) later became the standard for protecting data during online transactions; however, these protocols only secure the communication channel and do not prevent all forms of fraud (Rescorla 12). Europay–Mastercard–Visa (EMV) chip technology greatly reduced counterfeit card fraud in physical transactions by using dynamic cryptographic methods (EMVCo 5). For online payments, 3-D Secure was introduced to authenticate cardholders, and subsequent versions enhanced transaction speed and improved user experience (EMVCo, "3-D Secure Specification"). More recent innovations, such as tokenization and OAuth, aim to safeguard card information in mobile and app-based transactions by limiting the exposure of sensitive data and enabling secure delegated authorization (Hardt 8; PCI Security Standards Council 14). Regulatory

frameworks, including the Payment Card Industry Data Security Standard (PCI DSS) and Strong Customer Authentication (SCA), provide additional guidance for implementing these protocols effectively, ensuring that merchants and financial institutions maintain a high level of security compliance (European Banking Authority 22).

Overview of Security Protocols:

SSL/TLS:

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are protocols designed to protect data exchanged between a user's device and a website. They encrypt sensitive information such as login credentials, credit card details, and personal data to ensure that attackers cannot intercept or read the information while it travels across the network. SSL/TLS also provides integrity by detecting if data is modified during transmission and allows the client to authenticate the server's identity through digital certificates. SSL/TLS only secures the communication channel. It cannot protect against threats originating from a compromised user device, malware, or attacks targeting the website's backend systems and databases. Proper configuration and regular updates are important to prevent vulnerabilities like weak cipher suites or certificate mismanagement.

EMV:

EMV (Europay–Mastercard–Visa) technology uses a small embedded chip on credit and debit cards to enhance payment security. The chip generates a unique cryptographic code for each transaction, which prevents fraud from cloned or counterfeit cards. EMV also supports PIN-based authentication, adding another layer of protection. This system is highly effective for in-store, card-present transactions because it ensures that stolen card data cannot be reused easily. However, EMV provides limited protection for online or card-not-present (CNP) transactions, which remain vulnerable to phishing, stolen credentials, and other forms of cyber fraud.

3-D Secure:

3-D Secure is a protocol that adds an additional authentication step for online payments, allowing the card issuer to verify the cardholder's identity before approving a transaction. This verification include a password, a one-time passcode sent via SMS or email, or biometric confirmation such as a fingerprint or facial scan. Newer, risk-based versions of 3-D Secure evaluate the transaction's risk and decide whether to request additional authentication, reducing delays for low-risk transactions. This helps protect against unauthorized card use in online shopping while balancing security with user convenience.

Secure Electronic Transaction (SET):

SET was an early protocol designed to secure online credit card transactions using encryption and digital signatures. It ensured confidentiality, integrity, and non-repudiation, meaning neither the cardholder nor the merchant could deny the transaction. SET failed to gain widespread adoption because it required complex public key infrastructure (PKI) management, including issuing and validating digital certificates, which was costly and difficult for merchants and banks to implement.

OAuth and Tokenization:

OAuth is a widely used authorization framework that allows apps and websites to access resources on behalf of a user without exposing the user's actual credentials. Tokenization complements this by replacing sensitive card data with randomly generated tokens. These tokens is safely stored or transmitted during transactions, reducing the risk of exposing real card numbers. OAuth and tokenization are essential in mobile wallets, API-based payment systems, and app-driven commerce, providing both security and usability for modern digital payments.

Regulatory Mechanisms:

Standards such as the Payment Card Industry Data Security Standard (PCI DSS) and regulations like Strong Customer Authentication (SCA) provide guidelines for secure payment processing. PCI DSS sets requirements for storing, transmitting, and processing cardholder data, while SCA mandates multi-factor authentication for certain online transactions. Compliance with these standards helps organizations reduce the risk of data breaches, protect consumer information, and maintain trust in digital payment systems.

Evaluation Method:

To understand how well different online payment protocols perform, we evaluated them using three main sets of criteria: **Security**, **Operational Factors**, and **User Experience**. This approach allows a comprehensive comparison of technical effectiveness, practical deployment considerations, and the overall impact on end-users and businesses as given in the below image:

ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 12, Issue 12, December 2022 Impact Factor 8.059 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

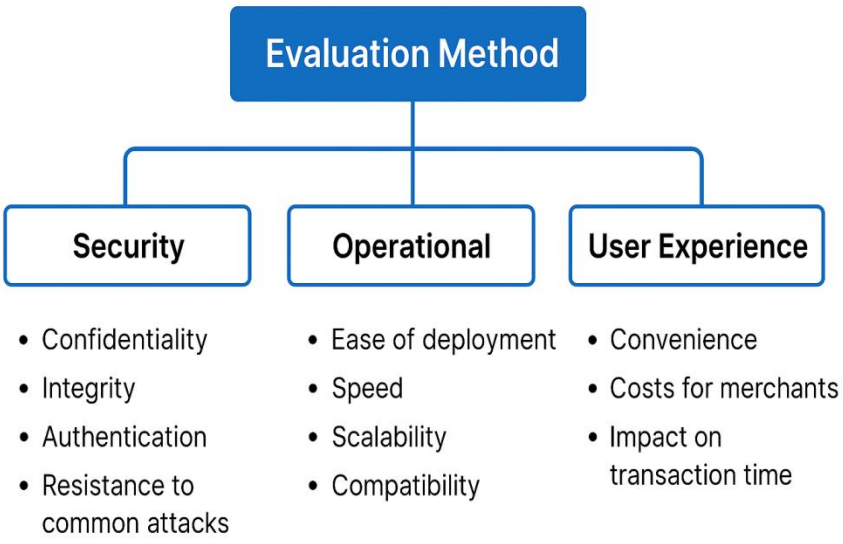

Image 1: Evaluation Method

The image 1 shows the Evaluation method as:

1. Security:

Security measures determine how well a protocol protects sensitive payment data and prevents fraud. This set of criteria includes:

- **Confidentiality:** Ensures that sensitive information, such as card numbers and personal data, remains private and inaccessible to unauthorized parties. Protocols like SSL/TLS encrypt data in transit, while tokenization replaces sensitive card data with secure tokens.
- **Integrity:** Protects data from being altered during transmission or processing. For example, EMV generates unique cryptographic codes for each transaction, ensuring that transaction data cannot be tampered with.
- **Authentication:** Confirms the identities of all parties involved in a transaction. 3-D Secure, OAuth, and EMV all provide mechanisms to authenticate the user, merchant, or issuing bank.
- **Resistance to common attacks:** Measures a protocol's ability to prevent threats such as man-in-the-middle attacks, phishing, replay attacks, and card cloning. Each protocol has strengths against specific attack types.

2. Operational Factors

Operational criteria focus on the practical implementation and management of the protocol. These include:

- **Ease of deployment:** How simple it is for merchants, banks, and app developers to integrate the protocol into existing systems. Protocols with simpler setup, like SSL/TLS, are easier to deploy than complex systems like SET.
- **Speed:** The effect of the protocol on transaction processing time. Some methods, such as risk-based 3-D Secure, balance security and speed to reduce checkout delays.
- **Scalability:** The ability of the protocol to handle large volumes of transactions without performance degradation. Tokenized payment systems and OAuth are designed to scale efficiently in mobile and API-based environments.
- **Compatibility:** Ensures the protocol works across different devices, platforms, and payment networks, which is essential for seamless digital commerce.

3. User Experience

User experience criteria evaluate the impact of the security protocols on consumers and merchants. This set includes:

- **Convenience:** Measures how easily users complete transactions. Protocols requiring multiple steps, like early versions of 3-D Secure, may reduce convenience, while tokenization and OAuth offer smoother experiences.
- **Costs for merchants:** Some protocols require additional infrastructure, such as EMV-enabled terminals or PKI for SET, which increases operational costs.
- **Impact on transaction time:** Evaluates whether the protocol slows down the checkout process, potentially causing cart abandonment or user dissatisfaction. Risk-based authentications methods help minimize delays while maintaining security.

Key Findings:

Protocol	Security	Ease of Use	Deployment	Remarks
SSL/TLS	High for data in transit	Very easy	Widely deployed	Essential but limited to channel protection
EMV	High for physical payments	Easy for users	Requires hardware	Best for in-store transactions
3-D Secure	Strong for online	Moderate friction	Medium	Good for card-not-present payments
SET	Strong but outdated	High friction	Low adoption	Too complex for widespread use
OAuth	Strong if well implemented	Easy for app users	Medium	Ideal for mobile and API systems

Tokenization	High	Very easy	Medium	Protects stored card data effectively

Each protocol serves a specific purpose. SSL/TLS is necessary for safe communication but cannot stop fraud if a database is hacked. EMV protects against card cloning in stores but offers little help online. 3-D Secure adds strong authentication for online shopping but can cause delays if poorly implemented. OAuth and tokenization are well suited for mobile apps and reduce the exposure of sensitive card data. Older systems such as SET provided excellent cryptography but were too complicated for mass use.

Recommendations:

- Use multiple protocols together to build strong protection.
- Keep software and certificates updated to avoid weak points.
- Replace stored card numbers with tokens to limit data theft.
- Apply risk-based checks so that extra verification is used only when needed.
- Protect key assets such as token servers and encryption keys with strict access control.
- Prepare for future threats such as quantum computing by planning upgrades to stronger encryption.

Conclusion:

Online payment security requires a comprehensive, layered approach to effectively protect sensitive financial data and maintain user trust. SSL/TLS encryption safeguards communication between the user and the payment server, ensuring that data transmitted over the internet remains confidential and tamper-proof. EMV (Europay, Mastercard, and Visa) standards enhance security for card-present transactions by using chip-based authentication, making it difficult for counterfeit cards to be used. 3-D Secure adds an additional layer of verification for online transactions, often requiring the cardholder to enter a password or a one-time code, which helps prevent unauthorized purchases. Tokenization further reduces the risk of card data theft by replacing actual card numbers with randomly generated tokens, so sensitive information is never stored or transmitted in its original form. Merchants and financial institutions create a balanced and robust security strategy that minimizes fraud while maintaining a seamless and convenient user experience for customers.

References:

Chaum, David, et al. *Secure Electronic Transaction Specification*. 1997.

EMVCo. *EMV Integrated Circuit Card Specifications*. EMVCo, 2020.

EMVCo. *3-D Secure Specification*. EMVCo, 2021.

Hardt, Dick. "The OAuth 2.0 Authorization Framework." *IETF RFC 6749*, 2012.

PCI Security Standards Council. *PCI DSS: Payment Card Industry Data Security Standard*, Version 4.0, 2022.

Rescorla, Eric. *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley, 2001.

European Banking Authority. *Guidelines on Strong Customer Authentication and Secure Communication*, EBA/GL/2017/17, 2017.