2026
SOCIAL CHALLENGES, SHARED FUTURES:
INNOVATION FOR EQUITY AND DEVELOPMENT
NEXT SCIENTISTS CONFERENCES
Published Date: 31 JANUARY 2026

ENSURING DATA PRIVACY IN ELECTRONIC PAYMENT SYSTEMS THROUGH STRIDE-BASED THREAT MODELING AND MULTI-FACTOR AUTHENTICATION

Agzamova Mohinabonu
PhD, Assoc. Professor, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan, Uzbekistan

Nuruddinova Adiba
PhD, Deputy director, Social Policy Laboratory under the National Agency for Social Protection, Uzbekistan

ABSTRACT

Electronic payment systems process large volumes of sensitive financial and personal data, making them attractive targets for cyberattacks. Ensuring data privacy in such systems requires systematic identification and mitigation of security threats across complex, distributed architectures. While cryptographic and regulatory controls are widely applied, existing studies often address threats in isolation and lack an integrated, system-level threat modeling framework tailored to modern payment infrastructures. This paper addresses this gap by proposing a structured threat modeling approach for electronic payment systems based on the STRIDE methodology, combined with privacy-preserving authentication mechanisms.

The proposed framework models payment system components using data flow diagrams and systematically classifies threats related to identity spoofing, data tampering, repudiation, information disclosure, denial of service, and privilege escalation. For each threat category, corresponding technical and organizational countermeasures are mapped to system assets and aligned with contemporary security standards. Additionally, the paper examines the role of multi-factor authentication, including biometric-based mechanisms, as a risk mitigation strategy within the threat model.

Rather than reporting experimental performance metrics, the study provides a methodological evaluation demonstrating how STRIDE enables comprehensive coverage of privacy risks and supports consistent risk prioritization. The main contribution is a reproducible, architecture-aware threat modeling framework that enhances privacy protection in electronic payment systems and can be adapted to evolving threat landscapes.

KEYWORDS: Electronic payment systems; data privacy; threat modeling; STRIDE; cybersecurity; authentication.

INTRODUCTION

The pursuit of technological advancement has always been a driving force in many scientific domains, and facial expression and attributes recognition is no exception. Over recent years, this field has undergone significant evolution, particularly in harnessing the power of multi-task learning strategies and lightweight neural networks. By synergizing these strategies, we aim to address the longstanding challenges of computational efficiency and deliver robust performance. Electronic payment systems have become a foundational component of the global digital economy, supporting financial transactions across e-commerce, mobile banking, and peer-to-peer platforms [1]. These systems routinely process sensitive data, including personal identifiers, authentication credentials, and payment instrument information. Consequently, breaches affecting payment infrastructures can result in financial loss, identity theft, regulatory penalties, and erosion of user trust.

Existing security approaches in payment systems primarily focus on cryptographic protection, compliance with standards such as PCI DSS, and post-incident monitoring. While these measures are necessary, they are insufficient on their own to address privacy risks arising from complex interactions between system components, third-party services, and users. Many studies concentrate on individual attack vectors—such as data leakage or authentication failures—without providing a holistic method for identifying and managing threats throughout the system lifecycle.

Threat modeling offers a structured mechanism for proactively identifying security and privacy risks during system design and evolution. However, its application in electronic payment systems remains fragmented, and comparative analyses of threat modeling methodologies highlight inconsistencies in scope, granularity, and practical applicability [2].

This study addresses this gap by applying the STRIDE threat modeling methodology to electronic payment systems, with a specific focus on protecting data privacy. The objectives and contributions of this paper are as follows:

- To develop a system-level threat model for electronic payment systems using STRIDE.
- To identify privacy-relevant threats across core payment components and data flows.
- To map identified threats to concrete mitigation strategies aligned with current security practices.
- To demonstrate how multi-factor and biometric authentication mechanisms can be integrated into the threat model to reduce privacy risks.

2. Study Area/Data

This research does not rely on a specific geographic study area or empirical transaction dataset. Instead, it focuses on a conceptual yet realistic electronic payment system architecture representative of contemporary payment platforms. The modeled system includes authentication services, API gateways, billing services, databases, transaction logs, and integrations with external payment service providers [3-4].

The analysis is architecture-centric and methodology-driven, making it applicable across different regulatory jurisdictions and deployment contexts. No real user data or transaction records are used, ensuring that the study remains focused on privacy-preserving design rather than data analysis.

3. Methodology

3.1 Threat Modeling Approach

The proposed methodology is based on STRIDE, a widely adopted threat classification framework that categorizes threats into six classes: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE was selected due to its systematic structure, compatibility with data flow diagrams, and suitability for complex software systems [5]. The STRIDE methodology enables systematic classification of threats affecting payment system components, as illustrated in Figure 1.

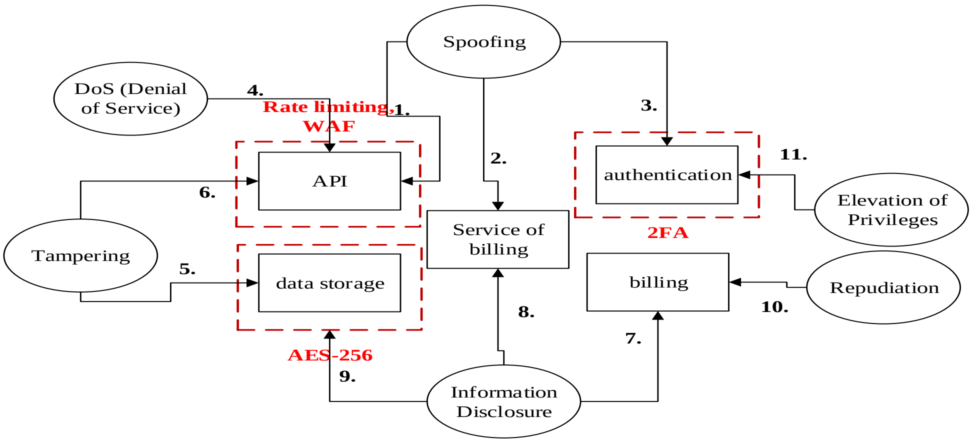


Figure 1. STRIDE threat categories and their impact on electronic payment systems

The modeling process consists of the following steps:

1. Identification of critical assets, including user credentials, transaction data, payment instruments, and audit logs.
2. Construction of data flow diagrams representing interactions between system components.
3. Classification of potential threats for each component and data flow using STRIDE.
4. Assessment of privacy impact based on the likelihood and potential consequences of each threat.
5. Definition of mitigation strategies corresponding to identified threats.

The analyzed payment system architecture and data flows between core components are presented in Figure 2.

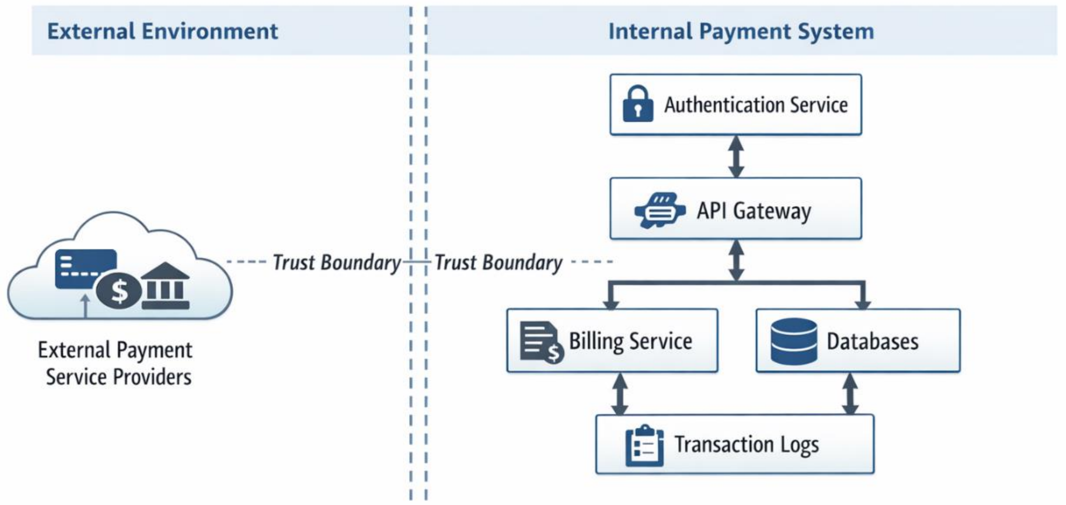


Figure 2. High-level architecture of an electronic payment system with trust boundaries

3.2 Data Preprocessing

As the study is design-oriented, preprocessing is limited to abstraction and normalization of system components. Functional elements are grouped into logical services, and data flows are categorized based on sensitivity levels. This abstraction enables consistent threat classification without exposing implementation-specific details [6].

3.3 Models and Algorithms

No predictive or classification models are trained in this study. Instead, the “model” refers to the threat model constructed using STRIDE principles. Authentication mechanisms, including cryptographic verification and biometric authentication, are analyzed conceptually as control mechanisms rather than algorithmic implementations.

3.4 Feature Selection

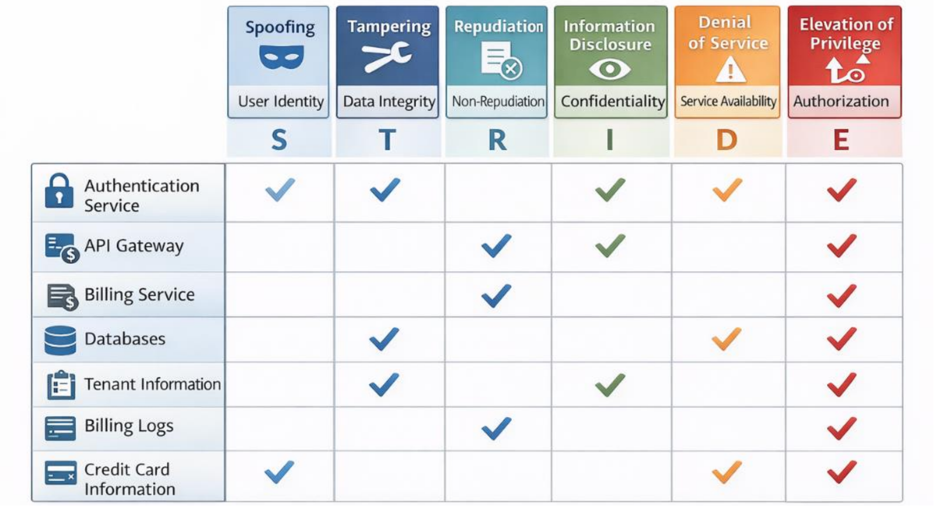
Relevant features in the threat model include asset sensitivity, trust boundaries, authentication mechanisms, and access privileges. These features guide the identification of privacy-related threats and the prioritization of mitigation measures [7].

3.5 Validation Strategy

Validation is performed qualitatively through consistency checks against established security standards and prior threat modeling studies. The completeness of threat coverage and the logical alignment between threats and mitigations serve as the primary evaluation criteria.

4. Results

The application of the STRIDE methodology resulted in a comprehensive classification of threats affecting electronic payment systems. Information disclosure and spoofing emerged as the most critical categories with respect to data privacy, particularly in authentication services, API gateways, and data storage components [8]. The distribution of identified threats across system components is summarized in Figure 3, highlighting the prevalence of information disclosure and spoofing risks.



	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	User Identity	Data Integrity	Non-Repudiation	Confidentiality	Service Availability	Authorization
	S	T	R	I	D	E
Authentication Service	✓	✓		✓	✓	✓
API Gateway			✓	✓		✓
Billing Service			✓			✓
Databases		✓			✓	✓
Tenant Information		✓		✓		✓
Billing Logs			✓			✓
Credit Card Information	✓				✓	✓

Figure 3. Mapping of STRIDE threat categories to payment system assets

The analysis shows that privacy risks are not confined to data storage but are distributed across authentication workflows, inter-service communication, and logging mechanisms. The structured mapping between threats and countermeasures demonstrates that STRIDE supports systematic risk identification without requiring empirical attack data [9].

Tables summarizing threat categories, affected assets, and mitigation strategies are used to illustrate coverage across the system architecture. These tables highlight alignment with widely recognized security controls, including encryption, access control, audit logging, and multi-factor authentication.

5. Discussion

The results indicate that STRIDE provides a practical and extensible framework for addressing privacy risks in electronic payment systems. Compared with more complex methodologies, STRIDE offers a balance between analytical rigor and usability, making it suitable for both design and operational contexts. From a privacy perspective, the most critical threat paths are illustrated in Figure 4.

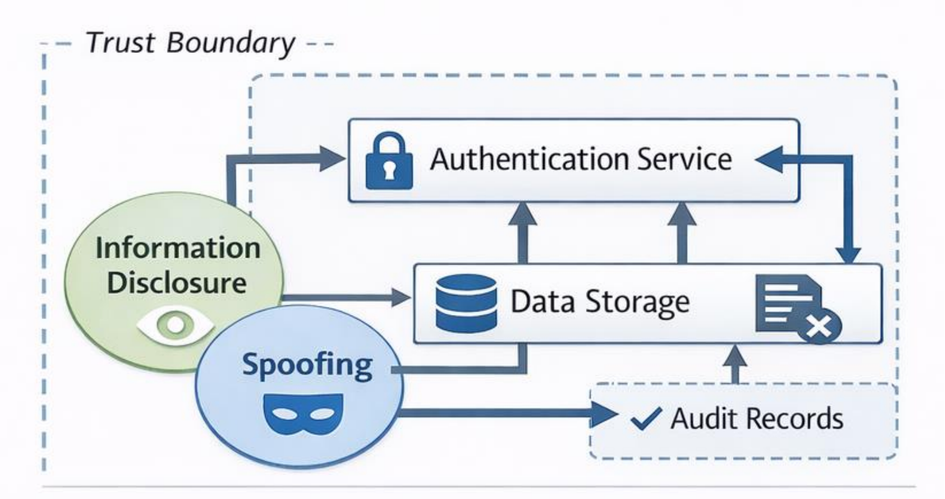


Figure 4. Privacy-focused threat model for electronic payment systems

A key strength of the proposed approach is its architecture-aware perspective, which captures privacy threats arising from component interactions rather than isolated vulnerabilities. The integration of multi-factor authentication, including biometric factors, further strengthens protection against identity-related threats.

However, the study is limited by its qualitative nature and absence of empirical validation. While this aligns with the goal of threat modeling, future work could complement the framework with quantitative risk assessment or simulation-based evaluation[11].

6. Conclusion

This paper presented a structured approach to ensuring data privacy in electronic payment systems through STRIDE-based threat modeling. By systematically identifying threats across system components and mapping them to targeted mitigation strategies, the proposed framework addresses privacy risks at an architectural level.

The findings demonstrate that STRIDE enables comprehensive coverage of privacy-relevant threats and supports the integration of advanced authentication mechanisms. Practically, the framework can guide system designers and security engineers in embedding privacy protections early in the development lifecycle.

Future research will focus on extending the model with quantitative risk metrics, evaluating its applicability to real-world payment platforms, and integrating adaptive threat intelligence to address emerging attack vectors.

References

1. Mohinabonu A. et al. E-payment Systems Security Solutions Using Facial Authentication Based on Artificial Neural Networks //World Conference Intelligent System for Industrial Automation. – Cham : Springer Nature Switzerland, 2022. – С. 139-148.
2. Агзамова М. ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АУТЕНТИФИКАЦИИ ЛИЦА В ПЛАТЕЖНЫХ СИСТЕМАХ //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 4. – С. 148-157.
3. Агзамова М. ОБУЧЕНИЕ И НАСТРОЙКА НЕЙРОННОЙ СЕТИ НА БАЗЕ ПОДГОТОВЛЕННЫХ ДАННЫХ ДЛЯ МОДУЛЯ ОБНАРУЖЕНИЯ ЛИЦ //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 4. – С. 158-164.
4. Mohinabonu A. ADVANCED FACE DETECTION USING RESNET AND FPN ARCHITECTURES WITH FOCAL LOSS FOR ENHANCED ACCURACY //Next Scientists Conferences. – 2024. – С. 48-51.
5. Mohinabonu A. Contrastive convolution in face recognition: advancements in accuracy //Next Scientists Conferences. – 2023. – С. 3-5.
6. Mohinabonu A. Emotion recognition through advanced neural architectures: a comprehensive analysis //International Scientific and Current Research Conferences. – 2023. – С. 29-31.
7. Mohinabonu A. ENHANCING FACIAL RECOGNITION THROUGH CONTRASTIVE CONVOLUTION: A COMPREHENSIVE METHODOLOGY //The American Journal of Engineering and Technology. – 2023. – Т. 5. – №. 11. – С. 105-114.
8. Agzamova M. ANALYSIS OF ISSUES RELATED TO BIOMETRIC AUTHENTICATION IN PAYMENT //Science and innovation. – 2024. – Т. 3. – №. A10. – С. 209-214.
9. Agzamova M. ENHANCING FACIAL EXPRESSION AND ATTRIBUTES RECOGNITION: AN EXPLORATION OF MULTI-TASK LEARNING WITHIN LIGHTWEIGHT NEURAL NETWORKS //Science and innovation. – 2023. – Т. 2. – №. A11. – С. 177-184.
10. Agzamova M. Development of a software module implementing a proposed facial biometric authentication algorithm and evaluation of solution effectiveness //Science and innovation. – 2023. – Т. 2. – №. A7. – С. 51-57.
11. Nuriddinov Azizbek, Agzamova Mokhinabonu . IMPROVING THE AUTHENTIFICATION MECHANISM BASED ON NEURAL NETWORKS IN PAYMENT SYSTEMS. 2(11)2025., doi:https://doi.org/10.61663/252tuitmct11