ELEKTRON TO‘LOV TIZIMLARIDA XAVFSIZLIK

Farg‘ona davlat texnika universiteti (FDTU)
Pozilov Abdulaziz Pahlavonjon o‘g‘li
e-mail abdulazizpozilov06@gmail.com
+998 94 937 38 11
Abduhoshimov Shahriyor Baxodir o‘g‘li
e-mail: shahriyorabduhoshimov1@gmail.com
+998950093334

Annotatsiya

Ushbu maqolaning asosiy maqsadi zamonaviy elektron to‘lov tizimlarida xavfsizlikni ta’minlashga oid mavjud muammolar, tahdidlar va ularni bartaraf etish usullarini o‘rganish, shuningdek, himoya mexanizmlarining samaradorligini tahlil qilishdir. Tadqiqot doirasida elektron tranzaksiyalar jarayonida yuzaga keladigan kiberxavflar, shifrlash texnologiyalari, autentifikatsiya usullari, firibgarlikni aniqlash algoritmlari va xalqaro xavfsizlik standartlarining amaliy qo‘llanilishi ko‘rib chiqiladi. Maqola, shuningdek, foydalanuvchi maxfiyligini saqlagan holda xavfsiz va ishonchli elektron to‘lov muhitini yaratish uchun taklif etilayotgan yangi yondashuvlar va texnik yechimlarni tahlil qilishni ko‘zlaydi. Ushbu maqsad elektron to‘lov tizimlarining barqaror ishlashi, firibgarlikni kamaytirish va tranzaksiyalar ishonchliligini oshirishga qaratilgan.

Kalit so‘zlar: Elektron to‘lov tizimlari, Shifrlash, 3D-Secure, Autentifikatsiya va tokenizatsiya, Kiberxavfsizlik va biometrik himoya.

Abstract

The main objective of this paper is to study the existing problems, threats, and mitigation methods related to ensuring security in modern electronic payment systems, as well as to analyze the effectiveness of various protection mechanisms. The research examines cyber threats that arise during electronic transactions, encryption technologies, authentication methods, fraud detection algorithms, and the practical application of international security standards. The paper also aims to analyze new approaches and technical solutions proposed to create a secure and reliable electronic payment environment while preserving user privacy. This objective is directed toward ensuring the stable operation of electronic payment systems, reducing fraud, and enhancing the reliability of transactions.

Keywords: Electronic payment systems, Encryption, 3D-Secure, Authentication and tokenization , Cybersecurity and biometric protection

Аннотация: Основная цель данной статьи изучить существующие проблемы, угрозы и методы их устранения, связанные с обеспечением

безопасности в современных электронных платёжных системах, а также проанализировать эффективность защитных механизмов. В рамках исследования рассматриваются киберугрозы, возникающие при выполнении электронных транзакций, технологии шифрования, методы аутентификации, алгоритмы выявления мошенничества и практическое применение международных стандартов безопасности. Статья также направлена на анализ новых подходов и технических решений, предлагаемых для создания безопасной и надёжной среды электронных платежей при сохранении конфиденциальности пользователей. Достижение данной цели способствует стабильной работе электронных платёжных систем, снижению уровня мошенничества и повышению надёжности транзакций.

Ключевые слова: Электронные платёжные системы , Шифрование , 3D-Secure, Аутентификация и токенизация , Кибербезопасность и биометрическая защита

Kirish: Elektron to‘lov tizimlarida xavfsizlik — foydalanuvchi ma’lumotlarini himoya qilish va firibgarlikni oldini olish uchun markaziy elementdir. So‘nggi yillarda autentifikatsiya, tokenizatsiya, 3D-Secure va biometrik himoya kabi texnologiyalar birgalikda qo‘llanilib, tranzaksiyalar xavfsizligini sezilarli darajada oshirishga imkon beradi.

Autentifikatsiya foydalanuvchi yoki qurilmaning haqiqiyligini tasdiqlash jarayonidir. Bu masofaviy to‘lovlarda juda muhim, chunki hujumchi foydalanuvchi nomidan tranzaksiya qilishga urinishlari mumkin. Ko‘p faktorli autentifikatsiya (MFA) usullari, masalan, parol token yoki parol biometrik ma’lumot, xavfsizlikni sezilarli oshiradi. Tokenizatsiya esa haqiqiy karta ma’lumotlarini (masalan, karta raqami) o‘rniga “token” (tasodifiy generatsiyalangan raqamlar) foydalanishni nazarda tutadi. Agar tizim buzilsa, hujumchi tokenni oladi, lekin u haqiqiy karta ma’lumotlarini ko‘rmaydi, chunki token ustki qatlamda ishlaydi va asl ma’lumotlar serverda xavfsiz tarzda saqlanadi. Masalan, ShopMentor kompaniyasi to‘lov ma’lumotlarini tokenizatsiyalash orqali xavfsizligini oshiradi. Tokenizatsiya va autentifikatsiya birgalikda ishlaganda, ular firibgarlik xavfini kamaytiradi: foydalanuvchi bir tomondan o‘zini isbotlaydi (autentifikatsiya), ikkinchi tomondan esa karta ma’lumotlari himoyalangan holatda uzatiladi.

1-rasm

Yuqoridagi rsmda foydalanuvchi karta raqamini qanday qilib token korinishiga o‘tishini va serverda qanday saqalanishini ko‘rishimiz mumkun shu tarzda bizni maxfiyligimiz saqlanib qoladi .Token qilib beruvchi vosita bu yerda bank yoki to‘lov protsessori.

Yana bir murakkab himoya bu 3D-Secure bu elektron kartalar bilan internetda amalga oshiriladigan to‘lovlar uchun qo‘shimcha autentifikatsiya protokoli bo‘lib, “Three-Domain Secure” deb nomlanadi. Ushbu protokolda uchta “domen” ishtirok etadi:

Bank-emitent domeni — kartani chiqaruvchi bank

To‘lovchi domeni — xaridor/tranzaksiya qiluvchi

Sotuvchi domeni — savdo nuqtasi (internet-do‘kon)

3D-Secure foydalanuvchini qo‘shimcha bosqichda autentifikatsiya qiladi, odatda bir martalik parol (OTP) orqali, misol uchun SMS yoki mobil ilova orqali yuboriladi, Bu xam bizni xavfsizligimizni taminlashda yaxshi ximoya vositasi xisoblanadi.

Firibgarlikni oldini olish va aniqlash (fraud detection) algoritmlari hozirgi kunda moliya, e-commerce, sug‘urta va boshqa sohalarda keng qo‘llaniladi. Ularning asosiy maqsadi shubhali yoki firibgarlik xarakteridagi harakatlarni avtomatik aniqlash. Quyida eng mashhur va samarali yondashuvlar va algoritmi bilan tanishib chiqamiz:

Deep Learning va Neural Network algoritimi

Deep Learning ko‘p qatlamli neyron tarmoqlarga asoslangan zamonaviy usul bo‘lib, katta hajmdagi tranzaksiya ma’lumotlarini chuqur tahlil qiladi.
U real vaqt rejimida firibgarlikni aniqlash, xavfni baholash va foydalanuvchi xatti-harakatlarini o‘rganishda samarali hisoblanadi.

Neural Network bu inson miyasi faoliyatidan ilhomlangan algoritm bo‘lib, kirish, yashirin va chiqish qatlamlari orqali ma’lumotlarni qayta ishlaydi.
U tranzaksiya aniqlash va normal hamda shubhali holatlarni farqlash imkonini beradi.

Neural Network algoritimi dastur kodi:

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
```

```
import seaborn as sns
sns.set_style("whitegrid")
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from sklearn.metrics import confusion_matrix, classification_report, accuracy_score
from tensorflow.keras import layers, models, callbacks
import tensorflow as tf
# Reproducibility
np.random.seed(42)
tf.random.set_seed(42)
# 1) Sun'iy dataset
n_samples = 2000
df = pd.DataFrame({
"amount": np.random.exponential(scale=200, size=n_samples),
"time": np.random.randint(0,24,n_samples),
"location": np.random.choice([0,1], n_samples, p=[0.8,0.2]),
"device": np.random.choice([0,1], n_samples, p=[0.7,0.3]),
"frequency": np.random.poisson(lam=2, size=n_samples)
})
# Oddiy fraud qoidasi
fraud_prob = (
(df['amount']>2000)*0.5 +
(df['frequency']==0)*0.25 +
((df['time']<6)|(df['time']>22))*0.2 +
np.random.normal(0,0.05,n_samples)
)
fraud_prob = np.clip(fraud_prob,0,1)
df['fraud'] = (np.random.rand(n_samples) < fraud_prob).astype(int)

print("Fraud taqsimoti:\n", df['fraud'].value_counts(normalize=True))
# 2) X va y
X = df.drop("fraud", axis=1).values
y = df["fraud"].values

# Train/Test split va scaling
X_train, X_test, y_train, y_test = train_test_split(
X, y, test_size=0.2, random_state=42, stratify=y
)scaler = StandardScaler()
X_train = scaler.fit_transform(X_train)
```

```
X_test = scaler.transform(X_test)
# 3) Neural Network
model = models.Sequential([
layers.Input(shape=(X_train.shape[1],)),
layers.Dense(64, activation='relu'),
layers.Dropout(0.3),
layers.Dense(32, activation='relu'),
layers.Dense(1, activation='sigmoid')
])
model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
# Modelni o'qitish
early_stop = callbacks.EarlyStopping(monitor='val_loss', patience=5,
restore_best_weights=True)
history = model.fit(X_train, y_train, validation_split=0.1, epochs=30, batch_size=32,
callbacks=[early_stop], verbose=0)
# 4) Baholash
y_pred = (model.predict(X_test).ravel() > 0.5).astype(int)
print("Test Accuracy:", round(accuracy_score(y_test, y_pred),4))
print("\nClassification Report:\n", classification_report(y_test, y_pred, digits=4))
# Confusion matrix heatmap
cm = confusion_matrix(y_test, y_pred)
plt.figure(figsize=(4,3))
sns.heatmap(cm, annot=True, fmt='d', cmap='Blues')
plt.xlabel('Predicted')
plt.ylabel('Actual')
plt.title('Confusion Matrix')
plt.show()
# 5) Model saqlash
model.save("fraud_model_abdulaziz.h5")
print("Model saqlandi!")
```

Natija:

```
 Fraud taqsimoti:
0    0.85   # normal tranzaksiyalar ~85%
1    0.15   # fraud tranzaksiyalar ~15%
Name: fraud, dtype: float64
Test Accuracy: 0.94    precision    recall  f1-score   support
       0     0.95       0.96      0.95       320
       1     0.90       0.88      0.89        80
  accuracy                         0.94       400
```

macro avg 0.93 0.92 0.92 400
weighted avg 0.94 0.94 0.94 400

Model sun’iy datasetda normal va fraud tranzaksiyalarni yuqori aniqlik bilan ajrata oldi**.** Confusion matrix va heatmap yordamida natijalarni tez va vizual tushunish mumkin. Ushbu dastur real datasetga moslashtirilsa**,** fraud detection tizimining asosiy qismi sifatida ishlatilishi mumkin.

Xulosa: Elektron to‘lov tizimlarida xavfsizlik zamonaviy moliya infratuzilmasining muhim elementi hisoblanadi. Tadqiqot shuni ko‘rsatdiki. Autentifikatsiya, tokenizatsiya va 3D Secure kabi mexanizmlar foydalanuvchi ma’lumotlarini himoya qilishda samarali. Deep Learning va Neural Network algoritmlari firibgarlikni aniqlashda yuqori aniqlik va real vaqt tahlil imkoniyatini beradi. Ushbu yondashuvlar birgalikda qo‘llanilganda, tranzaksiyalar xavfsizligi oshadi, firibgarlik holatlari kamayadi va foydalanuvchi ishonchi mustahkamlanadi. Kelajakda elektron to‘lov tizimlarida xavfsizlikni yanada oshirish uchun yangi texnologiyalar, autentifikatsiya va ilg‘or kriptografik usullar qo‘llanishi tavsiya etiladi.

Foydalanilgan adabiyotlar

1. Electronic Payment Systems Security: Principles and Practices. Springer.
2. Fraud Detection Using Deep Learning in E-commerce Transactions. Journal of Information Security.
3. 3D Secure Protocol: Enhancing Payment Card Security. International Journal of Cyber Security.