یادگیری هوشمند و تحول مدیریت

تدوین راهبردهای امنیت تجارت الکترونیک در بانک‌های خصوصی (مورد مطالعه: شهر زاهدان)

ام البنین سالاری[1*]
شهرام مهنا[2]

تاریخ چاپ نهایی: ۱ دی ۱۴۰۶
تاریخ چاپ اولیه: ۱۰ خرداد ۱۴۰۵
تاریخ پذیرش: ۴ خرداد ۱۴۰۵
تاریخ بازنگری: ۲۷ اردیبهشت ۱۴۰۵
تاریخ ارسال: ۴ اسفند ۱۴۰۴

شیوه استناددهی: سالاری، ام البنین.، و مهنا، شهرام. (۱۴۰۶). تدوین راهبردهای امنیت تجارت الکترونیک در بانک‌های خصوصی (مورد مطالعه: شهر زاهدان). *یادگیری هوشمند و تحول مدیریت*، ۵(۵)، ۱۸-۱.

چکیده

هدف پژوهش حاضر تدوین راهبردهای امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان با تأکید بر شناسایی ابعاد و متغیرهای اثرگذار از طریق تحلیل نقاط قوت، ضعف، فرصت‌ها و تهدیدها بود. این پژوهش از نظر هدف کاربردی، از نظر ماهیت تلفیقی (کیفی ـــ کمی) و از لحاظ روش، توصیفی ـــ تحلیلی بود. جامعه آماری شامل ۵۰ نفر از مدیران و متخصصان حوزه تجارت الکترونیک در شهر زاهدان بود که به روش گلوله‌برفی انتخاب شدند. برای گردآوری داده‌ها از بررسی شاخص‌های امنیت تجارت الکترونیک و برای تجزیه و تحلیل داده‌ها از تکنیک SWOT استفاده شد. در این روش، عوامل داخلی شامل نقاط قوت و ضعف و عوامل خارجی شامل فرصت‌ها و تهدیدها شناسایی و استانداردسازی شدند و سپس بر اساس ضرایب به‌دست‌آمده، استراتژی مناسب امنیت تجارت الکترونیک تعیین گردید. نتایج نشان داد که ضعف‌ها با میانگین ضریب ۹.۴۵ و تهدیدها با میانگین ضریب ۶.۲۱ بیشترین سهم را در وضعیت امنیت تجارت الکترونیک بانک‌های خصوصی شهر زاهدان دارند، در حالی که نقاط قوت با ضریب ۹.۱۸ و فرصت‌ها با ضریب ۵.۱۳ کمترین میزان را به خود اختصاص دادند. مهم‌ترین ضعف‌ها شامل ناهماهنگی در مکانیزم‌های رمزنگاری، ضعف در احراز هویت مشتریان، نبود نرم‌افزارهای جایگزین در شرایط اختلال خدمات و آسیب‌پذیری اطلاعات در برابر حوادث طبیعی بود. همچنین مهم‌ترین تهدیدها شامل نبود آموزش کافی کارکنان، استفاده‌نشدن از سیستم‌های تشخیص نفوذ و ثبت وقایع، و فقدان پروتکل‌های امنیتی استاندارد شناسایی شد. نتایج ماتریس داخلی ـــ خارجی نشان داد که وضعیت بانک‌های خصوصی در ناحیه تدافعی قرار دارد و استراتژی کاهش ضعف‌ها و مقابله با تهدیدها به‌عنوان راهبرد اصلی تعیین گردید. بر اساس یافته‌های پژوهش، امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان با ضعف‌های ساختاری و تهدیدهای محیطی قابل توجهی مواجه است و برای ارتقای امنیت، تمرکز بر اصلاح زیرساخت‌های امنیتی، بهبود فرآیندهای احراز هویت، توسعه پروتکل‌های استاندارد، آموزش کارکنان و استقرار سیستم‌های تشخیص نفوذ ضروری است. اتخاذ راهبرد تدافعی و کاهش آسیب‌پذیری‌ها می‌تواند زمینه ارتقای اعتماد مشتریان و توسعه پایدار تجارت الکترونیک را فراهم سازد

واژگان کلیدی: امنیت تجارت الکترونیک، بانک‌های خصوصی، تحلیل SWOT، بانکداری الکترونیک، شهر زاهدان

مشخصات نویسندگان:
۱. کارشناسی ارشد، گروه مدیریت اجرایی، واحد زاهدان، دانشگاه آزاد اسلامی، زاهدان، ایران
۲. دانشیار، گروه مخابرات، دانشکده مهندسی برق و کامپیوتر، دانشگاه سیستان و بلوچستان، زاهدان، ایران

پست الکترونیکی: Omolbanin.salari2020@gmail.com

Intelligent Learning and Management Transformation

Strategic Formulation of E-Commerce Security in Private Banks (Case Study: Zahedan City)

Omolbanin Salari[1]*
Shahram Mohanna[2]

Submit Date: 23 February 2026
Revise Date: 17 May 2026
Accept Date: 25 May 2026
Initial Publish: 31 May 2026
Final Publish: 22 December 2027

How to cite: Salari, O. & Mohanna, S. (2027). Strategic Formulation of E-Commerce Security in Private Banks (Case Study: Zahedan City). *Intelligent Learning and Management Transformation*, 5(5), 1-18.

Abstract

The present study aimed to formulate e-commerce security strategies in private banks of Zahedan with emphasis on identifying influential dimensions and variables through the analysis of strengths, weaknesses, opportunities, and threats. This study was applied in terms of purpose, mixed-method (qualitative–quantitative) in nature, and descriptive–analytical in methodology. The statistical population consisted of 50 managers and specialists in the field of e-commerce in Zahedan who were selected using the snowball sampling method. Data were collected through assessment of e-commerce security indicators and analyzed using the SWOT technique. Internal factors, including strengths and weaknesses, and external factors, including opportunities and threats, were identified and standardized. Based on the obtained coefficients, the appropriate strategy for improving e-commerce security was determined. The findings demonstrated that weaknesses with a mean coefficient of 9.45 and threats with a coefficient of 6.21 had the highest impact on the security status of e-commerce in private banks of Zahedan, whereas strengths with a coefficient of 9.18 and opportunities with a coefficient of 5.13 had the lowest impact. The most critical weaknesses included inconsistency in encryption mechanisms, weak customer authentication procedures, lack of backup software during service interruptions, and vulnerability of information systems to natural disasters. The major threats included inadequate employee training, insufficient use of intrusion detection and event logging systems, and lack of standard security protocols. The internal–external matrix analysis indicated that the banks were positioned within the defensive zone, suggesting that reducing weaknesses and avoiding threats should be considered the dominant strategic approach. The results indicate that e-commerce security in private banks of Zahedan is challenged by significant structural weaknesses and environmental threats. Therefore, enhancing security infrastructure, improving authentication mechanisms, implementing standard security protocols, training employees, and deploying intrusion detection systems are essential for strengthening e-commerce security. Adopting a defensive strategy focused on minimizing vulnerabilities can improve customer trust and support the sustainable development of electronic banking services.

Keywords: *E-commerce Security, Private Banks, SWOT Analysis, Electronic Banking, Zahedan City*

Authors' Information:
Omolbanin.salari2020@gmail.com

1. MA, Department of Strategic Orientation, Zah.C., Islamic Azad University, Zahedan, Iran
2. Associate Professor, Department of Telecommunications, Faculty of Electrical and Computer Engineering University of Sistan and Baluchestan, Zahedan, Iran

مقدمه

در دهه‌های اخیر، توسعه فناوری اطلاعات و ارتباطات موجب دگرگونی بنیادین در ساختارهای اقتصادی، اجتماعی و سازمانی شده است. رشد سریع فناوری‌های دیجیتال، الگوهای سنتی کسب‌وکار را متحول ساخته و زمینه شکل‌گیری اقتصاد دیجیتال و بانکداری هوشمند را فراهم کرده است. در این میان، تجارت الکترونیک به‌عنوان یکی از مهم‌ترین جلوه‌های تحول دیجیتال، نقش تعیین‌کننده‌ای در تسهیل مبادلات اقتصادی، کاهش هزینه‌ها، افزایش سرعت خدمات و ارتقای کیفیت تعاملات مالی ایفا می‌کند (Sarlak, 2012; Xu et al., 2025). بانک‌ها نیز به‌عنوان مهم‌ترین نهادهای مالی، تحت تأثیر این تحولات، بخش قابل توجهی از خدمات خود را به بسترهای الکترونیکی منتقل کرده‌اند و امروزه بانکداری دیجیتال و تجارت الکترونیک به بخش جدایی‌ناپذیر نظام مالی تبدیل شده است (Xu et al., 2025; Yousefi et al., 2025).

تجارت الکترونیک مجموعه‌ای از فرایندهای خرید، فروش، انتقال کالا، ارائه خدمات و انجام تراکنش‌های مالی از طریق شبکه‌های الکترونیکی و اینترنتی است که علاوه بر افزایش کارایی اقتصادی، امکان دسترسی گسترده‌تر مشتریان به خدمات را فراهم می‌سازد (Mahmoudzadeh, 2016). در فضای رقابتی کنونی، بانک‌ها برای حفظ مزیت رقابتی و افزایش رضایت مشتریان ناگزیر به توسعه زیرساخت‌های تجارت الکترونیک و بانکداری اینترنتی هستند. توسعه خدمات بانکداری الکترونیک علاوه بر کاهش هزینه‌های عملیاتی، موجب افزایش سرعت تراکنش‌ها، گسترش خدمات غیرحضوری و بهبود تجربه مشتری می‌شود (Alalwan et al., 2018; Taghipourian, 2026). با این حال، همزمان با گسترش تجارت الکترونیک، تهدیدهای امنیتی و ریسک‌های سایبری نیز افزایش یافته و مسئله امنیت اطلاعات به یکی از مهم‌ترین دغدغه‌های نظام بانکی تبدیل شده است (Kraft & Kakar, 2009; Torabi & Zamani, 2013).

امنیت در تجارت الکترونیک به معنای حفاظت از داده‌ها، تراکنش‌ها، زیرساخت‌ها و اطلاعات کاربران در برابر دسترسی غیرمجاز، تخریب، افشا یا سوءاستفاده است. در واقع، امنیت یکی از پیش‌شرط‌های اصلی موفقیت تجارت الکترونیک محسوب می‌شود؛ زیرا بدون وجود امنیت و اعتماد، کاربران تمایل چندانی به استفاده از خدمات الکترونیکی نخواهند داشت (Kim et al., 2010; Pishgahpour et al., 2017). مطالعات نشان داده‌اند که اعتماد مشتریان به سیستم‌های پرداخت الکترونیکی، ارتباط مستقیمی با ادراک آنان از امنیت، محرمانگی اطلاعات و قابلیت اطمینان سامانه‌های بانکی دارد (Mehdizadeh & Moloudian, 2019; Sutia et al., 2020). در نتیجه، هرگونه ضعف امنیتی می‌تواند به کاهش اعتماد عمومی، افت رضایت مشتریان و کاهش استفاده از خدمات بانکداری الکترونیک منجر شود (Lam & Osly, 2021; Seidi et al., 2024).

یکی از مهم‌ترین ابعاد امنیت تجارت الکترونیک، حفاظت از اطلاعات مشتریان و تضمین محرمانگی داده‌های مالی است. با افزایش حجم تراکنش‌های آنلاین، حملات سایبری، سرقت اطلاعات، نفوذ به پایگاه‌های داده و جعل هویت نیز به شدت افزایش یافته است (Saravari,

2023). در چنین شرایطی، بانک‌ها نیازمند بهره‌گیری از سازوکارهای پیشرفته امنیتی نظیر رمزنگاری، احراز هویت چندمرحله‌ای، امضای دیجیتال، سیستم‌های تشخیص نفوذ و پروتکل‌های استاندارد امنیتی هستند (Pormozeh et al., 2012; Shemin & Vipinkumar, 2016). به‌کارگیری این فناوری‌ها می‌تواند ریسک‌های امنیتی را کاهش داده و سطح اعتماد مشتریان را افزایش دهد (Azizi Sarkhani & Kordlouei, 2016).

مطالعات مختلف نشان داده‌اند که امنیت، مهم‌ترین عامل مؤثر بر پذیرش و استفاده از خدمات بانکداری الکترونیک است. کیم و همکاران بیان کردند که ادراک مشتریان از امنیت و اعتماد در سیستم‌های پرداخت الکترونیک، تأثیر مستقیم بر قصد استفاده از این خدمات دارد (Kim et al., 2010). همچنین آلالوان و همکاران نشان دادند که ریسک ادراک‌شده یکی از مهم‌ترین عوامل بازدارنده در پذیرش بانکداری اینترنتی است و کاهش نگرانی‌های امنیتی می‌تواند تمایل کاربران به استفاده از خدمات دیجیتال را افزایش دهد (Alalwan et al., 2018). از سوی دیگر، سوتیا و همکاران تأکید کردند که اعتماد به پرداخت الکترونیکی نقش تعیین‌کننده‌ای در رضایت مصرف‌کنندگان و تداوم استفاده از خدمات تجارت الکترونیک دارد (Sutia et al., 2020).

با وجود توسعه فناوری‌های نوین، بسیاری از بانک‌ها همچنان با مشکلات امنیتی متعددی مواجه هستند. این مشکلات شامل ضعف زیرساخت‌های امنیتی، نبود آموزش کافی کارکنان، استفاده ناکافی از فناوری‌های نوین امنیتی، نبود سیستم‌های پایش و ثبت وقایع، و ضعف در سیاست‌گذاری امنیت اطلاعات است (Hajmalek & Tavakoli, 2016; Saravari, 2023). همچنین، رشد فناوری‌های مالی نوین و فین‌تک‌ها موجب پیچیده‌تر شدن محیط بانکداری و افزایش آسیب‌پذیری‌های امنیتی شده است (Xu et al., 2025). در این میان، هوش مصنوعی و بانکداری هوشمند نیز فرصت‌ها و تهدیدهای جدیدی را ایجاد کرده‌اند؛ به‌گونه‌ای که استفاده از الگوریتم‌های هوشمند در خدمات بانکی، علاوه بر افزایش کارایی، می‌تواند ریسک‌های امنیتی جدیدی را نیز به همراه داشته باشد (Yousefi et al., 2025).

ارزیابی و مدیریت امنیت تجارت الکترونیک مستلزم شناسایی دقیق نقاط قوت، ضعف، فرصت‌ها و تهدیدهای محیطی است. تحلیل SWOT یکی از مهم‌ترین ابزارهای برنامه‌ریزی استراتژیک در حوزه امنیت اطلاعات محسوب می‌شود که امکان تحلیل همزمان عوامل داخلی و خارجی را فراهم می‌سازد (Hajmalek & Tavakoli, 2016). این مدل به سازمان‌ها کمک می‌کند تا بر اساس ظرفیت‌های داخلی و شرایط محیطی، راهبردهای مناسب را برای کاهش ریسک‌ها و افزایش امنیت تدوین کنند (Liu, 2011). استفاده از این رویکرد در نظام بانکی می‌تواند به شناسایی تهدیدهای سایبری، نقاط ضعف زیرساختی و فرصت‌های توسعه فناوری منجر شود و زمینه طراحی سیاست‌های کارآمد امنیتی را فراهم سازد (Alrawashdeh et al., 2012).

در پژوهش‌های داخلی نیز بر اهمیت امنیت تجارت الکترونیک و بانکداری الکترونیک تأکید شده است. ترابی و زمانی بیان کردند که چالش‌های امنیتی از مهم‌ترین موانع توسعه تجارت الکترونیک در ایران هستند و ضعف در زیرساخت‌های ارتباطی، تهدیدی جدی برای بانکداری الکترونیک محسوب می‌شود (Torabi & Zamani, 2013). همچنین پرموزه و همکاران بر ضرورت استفاده از فناوری‌های نوین امنیتی و طراحی سیاست‌های جامع امنیت اطلاعات تأکید کردند (Pormozeh et al., 2012). مطالعات دیگری نیز نشان داده‌اند که افزایش آگاهی کارکنان و مشتریان درباره تهدیدهای سایبری می‌تواند نقش مهمی در کاهش ریسک‌های امنیتی ایفا کند (Pishgahpour et al., 2017; Saravari, 2023).

از سوی دیگر، تحولات محیط کسب‌وکار و توسعه شهرهای هوشمند، وابستگی سازمان‌ها به فناوری‌های دیجیتال را افزایش داده است. جلالی و همکاران معتقدند که فناوری‌های هوشمند نقش مهمی در ارتقای کیفیت خدمات و توسعه زیرساخت‌های شهری دارند و این موضوع ضرورت تقویت امنیت سایبری را دوچندان می‌سازد (Jalali et al., 2024). در چنین فضایی، بانک‌ها به‌عنوان زیرساخت‌های حیاتی اقتصادی، بیش از گذشته در معرض حملات سایبری و تهدیدهای امنیتی قرار دارند و هرگونه اختلال در سیستم‌های بانکی می‌تواند پیامدهای گسترده اقتصادی و اجتماعی به همراه داشته باشد (Mohammadi, 2026).

بررسی پژوهش‌های پیشین نشان می‌دهد که اگرچه مطالعات متعددی در زمینه امنیت تجارت الکترونیک، اعتماد مشتریان و فناوری‌های امنیتی انجام شده است، اما همچنان خلأ قابل توجهی در زمینه تدوین راهبردهای جامع امنیت تجارت الکترونیک در بانک‌های خصوصی، به‌ویژه در مناطق کمتر برخوردار، وجود دارد (Mahna, 2009). بسیاری از مطالعات پیشین صرفاً به بررسی عوامل فنی یا رفتاری پرداخته‌اند و کمتر به تحلیل راهبردی و جامع ابعاد امنیتی توجه شده است (Hedavand et al., 2021; Kraft & Kakar, 2009). علاوه بر این، شرایط خاص استان سیستان و بلوچستان و شهر زاهدان از نظر زیرساخت‌های ارتباطی، محدودیت‌های فنی و چالش‌های امنیتی، ضرورت انجام مطالعات بومی و کاربردی را افزایش داده است (Mahna, 2009).

بنابراین، با توجه به اهمیت امنیت در توسعه تجارت الکترونیک، نقش حیاتی بانک‌ها در اقتصاد دیجیتال، افزایش تهدیدهای سایبری و ضرورت تدوین راهبردهای کارآمد برای کاهش ریسک‌های امنیتی، پژوهش حاضر با هدف تدوین راهبردهای امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان بر اساس تحلیل نقاط قوت، ضعف، فرصت‌ها و تهدیدها انجام شد.

روش‌شناسی

این پژوهش از نظر هدف، کاربردی و از نظر ماهیت تلفیقی (کیفی -کمی)، به لحاظ روش توصیفی -تحلیلی است. جامعه آماری این پژوهش، شامل ۵۰ نفر از مدیران و متخصصات در حوزه تجارت الکترونیک در شهر زاهدان است که به روش گلوله برفی تعیین شدند. جهت تجزیه و تحلیل

اطلاعات از تکنیک SWOT استفاده شد. تحلیل SWOT یک ابزار مهم پشتیبان تصمیم‌گیری است و به طور معمول به عنوان وسیله‌ای برای تحلیل محیط‌های بیرونی و درونی سیستم (سازمان) به کار می‌رود. ماتریس SWOT ابزاری برای شناخت تهدیدها و فرصت‌های موجود در محیط خارجی یک سیستم (سازمان) و بازشناسی ضعف‌ها و قوت‌های داخلی آن به منظور سنجش وضعیت و تدوین راهبرد برای هدایت و کنترل آن سیستم (سازمان) است. در این روش دو نوع بررسی صورت می‌گیرد: بررسی درونی که دربرگیرنده قوت‌ها و ضعف‌های داخلی سازمان است و امکان ارزیابی دقیق از منابع و محدودیت‌های سازمان را برای مدیریت فراهم می‌سازد. بررسی درونی باید با واقع‌بینی انجام گیرد، بدین معنی که در برآورد قوت‌ها اغراق نشود و ضعف‌های سازمان نادیده گرفته نشود. در چنین شرایطی مدیریت می‌تواند امکانات و محدودیت‌های سازمان را به درستی شناسایی و برنامه‌ریزی صحیحی را تنظیم و اجرا نماید. از سوی دیگر، کل‌نگری برنامه‌ریزی استراتژیک ایجاب می‌کند که به محیط بیرونی سازمان توجه شود. از این رو مدیریت پس از بررسی درونی به ارزیابی تهدیدات و فرصت‌های محیط بیرونی می‌پردازد. تدوین استراتژی (راهبرد) برای بهره‌بردن از فرصت‌ها یا نقاط قوت، نوعی حمله است، در حالی که طرح‌ریزی برای کاهش یا حذف آسیب‌های ناشی از تهدیدها یا نقاط ضعف به معنای دفاع است. به همین دلیل باید برای تدوین استراتژی‌های گوناگون، آنها را هماهنگ کرد. با استفاده از ماتریس SWOT می‌توان چهار نوع استراتژی ارائه کرد. از دیدگاه این مدل، یک استراتژی مناسب، قوت‌ها و فرصت‌ها را به حداکثر و ضعف‌ها و تهدیدها را به حداقل ممکن می‌رساند. برای این منظور، نقاط قوت، ضعف، فرصت‌ها و تهدیدها در چهار حالت کلی SO، WO، ST و WT پیوند داده می‌شوند.

یافته‌ها

اولین قدم در تدوین راهبردهای امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان، شناسایی ابعاد و متغیرهای تاثیرگذار در افزایش امنیت تجارت الکترونیک است. بنابراین ابتدا باید اقدام به استخراج نقاط قوت، ضعف، فرصت‌ها و تهدیدات وضعیت امنیت تجارت الکترونیک به لحاظ نارسایی‌ها و مشکلات موجود در آنها مبادرت گردد.

اهم مسایل و مشکلات موجود در امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان بر اساس شاخص‌های مورد بررسی از دیدگاه پرسنل متخصص این بانک‌ها (صرفا کارمندانی که در ارتباط با چنین خدماتی درگیر بوده اند) مطرح گردید که در تحلیل **swot** برخی از این مسائل و مشکلات در قالب شاخص‌ها در تدوین راهبردها مدنظر قرار گرفته شد (جدول ۱).

جدول ۱: نقاط قوت، ضعف، فرصت‌ها و تهدیدات امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان

	نقاط قوت (S)	نقاط ضعف(W)
ماتریس SWOT	X_1- استفاده از دوربین‌ها و سیستم‌های حفاظتی بر اعتماد مشتریان، X_2 -بکارگیری صحیح از دستگاه‌های کارت خوان فروشگاهی (در امنیت)، X_7 - امن بودن نرم افزارهای مورد استفاده در سیستم‌های بانکی، X_{12} - تعهد کارمندان بانک به حفظ اطلاعات مشتریان و بانک، X_{14} - آگاه کردن مشتری از طریق پیامک،ایمیل و...هنگام ورود به سایت و انجام تراکنش بانکی توسط بانک، X_{21} - آموزش و اطلاع رسانی بانک‌ها در خصوص نکات امنیتی سیستم‌های بانکداری الکترونیکی به مشتریان،X_{26} - عدم اشتراک لوازم رایانه‌ای و تلفن همراه مشتریان با دیگران	X_3- خطر پذیری اطلاعات بانک و مشتری در صورت بروز حوادثی مانند آتش سوزی،سیل، زلزله، X_{16} - عدم وجود نرم افزارهای جایگزین در هنگام وقفه در ارائه خدمات مشتری توسط بانک، X_{23}- نصب برنامه‌های کاربردی(اپلیکشن ها) در تلفن همراه بر امنیت داده‌های کاربر، X_{20} - عدم استفاده از خدمات بیمه‌ای درصورت وقوع خطاهای کاربران، X_{25} - یکسان بودن هزینه‌های دریافتی از مشتریانی که از خدمات پیامکی استفاده می‌کنند، X_{28} - استفاده مکرر از احراز هویت (کلمه عبور،توکن تولید رمز) به منظور امنیت بیشتر در ورود و انجام تراکنش‌ها و بالا رفتن خطای مشتریان و مسدود شدن حساب آنها، X_{30} - عدم پایبندی و یا فراموش کردن تعهد مشتریان برای حفظ اطلاعات مالی، رمزورود و تغییرات دوره‌ای آنها، X_{31} - عدم حمایت مطلوب و مناسب دولت از امنیت تجارت الکترونیک، X_{32} - عدم امنیت مناسب زیرساخت‌های ارتباطی بکاررفته شده در بانک ها، X_{33} - احتمال بالای خطای مسدود شدن حساب‌ها در استفاده از مکانیزم‌های رمزنگاری در بانکداری با تلفن همراه، X_{34} - ضعف در کنترل‌های لازم جهت احراز هویت مشتری هنگام فعال سازی خدمات الکترونیک در بعضی مواقع به جهت دوست بودن با کارمندان و مسئولین بانک ها، X_{35} - عدم استفاده اکثر مشتریان از امضای دیجیتالی، X_8 - برنامه‌های نرم‌افزاری نفوذناپذیر، ایمن و دارای سهولت کاربرد، X_9 - عدم استفاده از سیستم عامل به روز و اصل، X_{10}- عدم تبلیغات و تشویق مناسب کاربران و مشتریان به استفاده از تجارت الکترونیک، X_{36}- تمایل برخی از مشتریان بر اشتراک اطلاعات مالی خود با دیگران، X_{37}- ناهماهنگی در استفاده از مکانیزم‌های رمزنگاری در کامپیوترهای بانک ها
فرصت‌ها (O)	X_5- میزان اعتماد و اطمینان به شبکه‌های بی سیم و همراه در سیستم تجارت الکترونیک، X_{11}- امنیت سخت افزاری کارت‌های بانکی(از لحاظ جعل کارت ها)، X_{15}- استفاده از سرورهای پشتیبان شبکه از نظر حفظ اطلاعات بانک و حفاظت از آنها، X_{17}- تشخیص ورود غیر مجاز و شناسایی سریع واردشوندگان به نرم افزارهای بانکی، X_{18}- استفاده ار امضای دیجیتالی در قراردادهای بانکی؛	
تهدیدات(T)	X_4- عدم دسترسی برنامه‌ها به داده‌های بانکی، X_6 - عدم آموزش کافی کارکنان بانک‌های خصوصی در خصوص چگونگی راه‌های مقابله با حملات سایبری، X_{13}- عدم پایبندی به استفاده از محرمانگی و امنیت اطلاعات حساب‌های مشتری بین بانک و مشتری، X_{19}- عدم استفاده مناسب بانک‌ها از سیستم‌های تشخیص نفوذ و شناسایی فعالیت‌های غیر مجاز به منظور امنیت بیشتر، X_{22}- عدم بهره گیری مناسب بانک‌ها ازسیستم‌های ثبت وقایع و رخدادها جهت کشف تراکنش‌های مشکوک، X_{24} - عدم بکارگیری پروتکل امنیتی استاندارد و گواهینامه‌های دیجیتال معتبر جهت تامین اطلاعات در بانکداری اینترنتی و درگاه الکترونیکی، X_{27} - عدم استفاده مطلوب از مرکز داده (دیتاسنتر) بر حفظ امنیت بانک‌های اطلاعاتی	

درونی

بیرونی

با توجه به نتایج به دست آمده از داده‌های تحقیق و تجزیه و تحلیل آنها هر یک از متغیرهای امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان، مقدار داده‌ها به عددی از ۱ تا ۱۰ استاندارد سازی گردید. سپس قوت ها، ضعف ها، فرصت‌ها و تهدیدهای امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان از ۳۷ متغیر مشخص گردید. در نهایت میانگین ضریب هر یک از مولفه‌های **SWOT** در بانک‌های خصوصی شهر زاهدان بر اساس وزن دهی هر یک از سوالات توسط کارمندان بانک‌ها محاسبه شد. برابر بررسی‌های صورت گرفته در رابطه با روند برنامه

ریزی به منظور امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان، ضعف‌ها و تهدیدات با ضرایب ۹/۴۱ و ۸/۳۶ بیشترین مقدار و نقاط قوت و فرصت‌ها با ضرایب ۷/۱۳ و ۶/۵۴ کمترین مقدار را به خود اختصاص داده‌اند (جدول ۲).

جدول ۲. استاندارد سازی ضرایب متغیرها (از ۱۰ -۱) در مدل SWOT در بانک‌های خصوصی شهر زاهدان

	قوت‌ها (S)		ضعف‌ها (W)		فرصت‌ها (O)		تهدیدات (T)	
	نام متغیرها	میانگین ضریب	نام متغیرها	میانگین ضریب	نام متغیرها	میانگین ضریب	نام متغیرها	میانگین ضریب
وضعیت امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان	$(x^{۱})$؛ $(x^{۲})$؛ $(x^{۷})$؛ $(x^{۱۲})$؛ $(x^{۱۴})$؛ $(x^{۲۱})$؛ $(x^{۲۶})$	۷/۱۳	$(x^{۳})$؛ $(x^{۱۶})$؛ $(x^{۲۳})$؛ $(x^{۲۵})$؛ $(x^{۲۰})$؛ $(x^{۲۸})$؛ $(x^{۸})$؛ $(x^{۹})$؛ $(x^{۱۰})$؛ $(x^{۳۰})$؛ $(x^{۳۱})$؛ $(x^{۳۲})$؛ $(x^{۳۳})$؛ $(x^{۳۴})$؛ $(x^{۳۵})$؛ $(x^{۳۶})$؛ $(x^{۳۷})$	۹/۴۱	$(x^{۵})$؛ $(x^{۱۱})$؛ $(x^{۱۵})$؛ $(x^{۱۷})$؛ $(x^{۱۸})$	۶/۵۴	$(x^{۴})$؛ $(x^{۶})$؛ $(x^{۱۹})$؛ $(x^{۲۲})$؛ $(x^{۱۳})$؛ $(x^{۲۴})$؛ $(x^{۲۹})$ $(x^{۲۷})$	۸/۳۶

بعد از اینکه عوامل داخلی (نقاط قوت، ضعف) و عوامل خارجی (فرصت‌ها و تهدیدها) و ضرایب هر کدام در امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان مشخص گردید. درصد هر کدام از این فاکتورها در این بانک‌ها خصوصی در جدول (۳) ارائه شده است. در ستون **SWOT** درصد متغیرهای وارده بر مدل در امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان آورده شده است. سپس از این میزان چه درصدی به قوت، ضعف، فرصت و تهدید اختصاص یافته است مشخص گردیده است. نهایتا بر اساس درصدهای محاسبه شده نوع استراتژی لازم برای امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان ارائه شده است.

جدول ۳. محاسبه درصد قوت و ضعف و فرصت‌ها و تهدیدها و تعیین استراتژی در بانک‌های خصوصی شهر زاهدان

عنوان	SWOT								نوع استراتژی
	S	W	O	T	داخلی S/W	خارجی O/T	مثبت S/O	منفی W/T	SWOT	
بانک‌های خصوصی شهر زاهدان	۱۸/۹	۴۵/۹	۱۳/۵	۲۱/۶	۶۴/۸	۳۵/۱	۳۲/۴	۶۷/۵	۸۳/۴	دوم

بر اساس اطلاعات جدول (۳) وضعیت بانک‌های خصوصی شهر زاهدان با نقاط ضعف بیشماری روبرو است (یعنی ۴۵.۹ درصد). این بدان معنا است که با روند برنامه‌ریزی‌های فعلی، باید تاکید بیشتر بر روی پایین آوردن خطرپذیری اطلاعات بانک و مشتری در صورت بروز حوادثی مانند آتش‌سوزی، سیل، زلزله، تهیه نرم‌افزارهای جایگزین در هنگام وقفه در ارائه خدمات مشتری توسط بانک، بالا بردن امنیت برنامه‌های کاربردی (اپلیکشن‌ها) در تلفن همراه بر امنیت داده‌های کاربر، استفاده از خدمات بیمه‌ای در صورت وقوع خطاهای کاربران و هزینه‌های دریافتی از مشتریان

بابت خدمات پیامکی به میزان استفاده آنها صورت بگیرد. البته نقاط قوت هم چشمگیر است (۱۸.۹ درصد) و می‌توان با تکیه بر این نقاط قوت و همچنین فرصت‌ها (۱۳.۵ درصد)، اقدام به کم‌رنگ‌تر کردن نقاط ضعف و تهدیدات (۲۱.۶ درصد) کرد. بنابراین با توجه به نتایج جدول (۳) استراتژی‌هایی برای نیل به برنامه‌ریزی امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان ارائه شده است.

با توجه به نتایج جدول (۳)، استراتژی تدافعی (کاهش ضعف‌ها و دوری از تهدیدات) به عنوان راهبرد اصلی انتخاب می‌شود. در این چارچوب، از استراتژی غلبه کردن برای کوچک یا غیرفعال کردن نقاط ضعف با استفاده از نقاط قوت محدود استفاده می‌گردد. برنامه‌ریزی برای بالابردن امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان باید متمرکز بر فراهم کردن زیرساخت‌ها و امکانات در تمام شاخص‌های پروتکل امنیتی، تکنیک رمزگذاری، امضای دیجیتالی، امنیت نرم‌افزاری، امنیت کاربری و امنیت سخت‌افزاری باشد.

بحث و نتیجه‌گیری

نتایج پژوهش حاضر نشان داد که وضعیت امنیت تجارت الکترونیک در بانک‌های خصوصی شهر زاهدان بیش از آنکه متکی بر نقاط قوت و فرصت‌ها باشد، تحت تأثیر ضعف‌های داخلی و تهدیدهای محیطی قرار دارد. یافته‌ها بیانگر آن بود که ضعف‌ها و تهدیدها بیشترین وزن را در میان ابعاد تحلیل SWOT به خود اختصاص داده‌اند و در مقابل، نقاط قوت و فرصت‌ها از قدرت و تأثیرگذاری کمتری برخوردار هستند. این وضعیت نشان می‌دهد که بانک‌های خصوصی مورد مطالعه، در حوزه امنیت تجارت الکترونیک همچنان در مرحله واکنشی و تدافعی قرار دارند و هنوز نتوانسته‌اند به سطحی از بلوغ امنیتی دست یابند که امکان بهره‌برداری کامل از ظرفیت‌های تجارت الکترونیک را فراهم سازد. چنین یافته‌ای با مطالعات پیشین در حوزه امنیت بانکداری الکترونیک و تجارت دیجیتال همسو است که نشان داده‌اند بسیاری از بانک‌ها در کشورهای در حال توسعه، علی‌رغم گسترش خدمات الکترونیکی، همچنان با چالش‌های اساسی در زمینه امنیت اطلاعات و مدیریت ریسک‌های سایبری مواجه هستند (Mohammadi, 2026; Xu et al., 2025).

یکی از مهم‌ترین یافته‌های پژوهش حاضر، برجسته بودن ضعف‌های مربوط به زیرساخت‌های امنیتی و فرایندهای احراز هویت بود. ضعف در مکانیزم‌های رمزنگاری، نبود نرم‌افزارهای جایگزین در زمان اختلال خدمات، و آسیب‌پذیری اطلاعات در برابر حوادث طبیعی از جمله مهم‌ترین ضعف‌های شناسایی‌شده بودند. این نتایج نشان می‌دهد که بخش مهمی از مشکلات امنیتی بانک‌های خصوصی به مسائل زیرساختی و فنی مربوط می‌شود. پژوهش‌های پیشین نیز تأکید کرده‌اند که زیرساخت‌های امنیتی ناکافی یکی از اصلی‌ترین عوامل آسیب‌پذیری سیستم‌های تجارت الکترونیک است (Pormozeh et al., 2012; Torabi & Zamani, 2013). پرموزه و همکاران بیان کردند که نبود سیاست‌های جامع امنیتی و ضعف در استفاده از فناوری‌های امنیتی پیشرفته، موجب افزایش احتمال نفوذ و سوءاستفاده از داده‌های بانکی می‌شود (Pormozeh et

al., 2012). همچنین ترابی و زمانی اشاره کردند که ضعف در زیرساخت‌های ارتباطی و فناوری اطلاعات، تهدیدی جدی برای امنیت تجارت الکترونیک در ایران محسوب می‌شود (Torabi & Zamani, 2013).

یافته‌های این پژوهش نشان داد که ضعف در احراز هویت مشتریان و نبود کنترل‌های کافی در فعال‌سازی خدمات الکترونیک، یکی از چالش‌های اساسی بانک‌های خصوصی است. این مسئله از آن جهت اهمیت دارد که احراز هویت، نخستین خط دفاعی در برابر حملات سایبری و سوءاستفاده‌های مالی محسوب می‌شود. کیلجان و همکاران نیز در پژوهش خود نشان دادند که کارآمدی روش‌های احراز هویت، نقش تعیین‌کننده‌ای در امنیت بانکداری آنلاین دارد و ضعف در این زمینه می‌تواند اعتماد کاربران را به شدت کاهش دهد (Kiljan et al., 2018). علاوه بر این، شیمین و ویپین کومار تأکید کردند که استفاده از فناوری‌های رمزنگاری نوین و احراز هویت چندمرحله‌ای می‌تواند سطح امنیت پرداخت‌های الکترونیکی را به طور قابل توجهی افزایش دهد (Shemin & Vipinkumar, 2016). بنابراین، نتایج پژوهش حاضر ضرورت بازنگری در سیستم‌های احراز هویت و به‌کارگیری فناوری‌های نوین امنیتی در بانک‌های خصوصی را آشکار می‌سازد.

از دیگر یافته‌های مهم پژوهش حاضر، نقش قابل توجه تهدیدهای محیطی در تضعیف امنیت تجارت الکترونیک بود. نبود آموزش کافی کارکنان، عدم استفاده مناسب از سیستم‌های تشخیص نفوذ و ثبت وقایع، و فقدان پروتکل‌های امنیتی استاندارد از جمله مهم‌ترین تهدیدهای شناسایی‌شده بودند. این یافته‌ها با نتایج مطالعات داخلی و خارجی همخوانی دارد که نشان داده‌اند خطاهای انسانی و ضعف در آموزش کارکنان، سهم قابل توجهی در بروز رخدادهای امنیتی دارند (Hajmalek & Tavakoli, 2016; Saravari, 2023). سراوری بیان کرد که بسیاری از سازمان‌ها علی‌رغم آگاهی از تهدیدهای سایبری، هنوز فاقد سیاست‌های امنیتی منسجم و برنامه‌های آموزشی مستمر هستند (Saravari, 2023). همچنین حاج‌ملک و توکلی بر این باورند که امنیت تجارت الکترونیک صرفاً یک مسئله فنی نیست، بلکه نیازمند نگرشی جامع و چندبعدی است که ابعاد انسانی، مدیریتی و سازمانی را نیز دربرگیرد (Hajmalek & Tavakoli, 2016).

نتایج پژوهش حاضر همچنین نشان داد که ضعف در استفاده از سیستم‌های تشخیص نفوذ و ثبت وقایع، یکی از عوامل اصلی افزایش آسیب‌پذیری بانک‌ها در برابر تهدیدهای سایبری است. در محیط بانکداری دیجیتال، سیستم‌های پایش و ثبت وقایع نقش حیاتی در شناسایی رفتارهای مشکوک، جلوگیری از نفوذ و مدیریت بحران‌های امنیتی دارند. پژوهش آلراوارشده و همکاران نشان داد که بهره‌گیری از فناوری اطلاعات و سیستم‌های هوشمند امنیتی می‌تواند ریسک خدمات بانکداری الکترونیک را به میزان قابل توجهی کاهش دهد (Alrawashdeh et al., 2012). همچنین لیو تأکید کرد که ارزیابی مستمر امنیت سیستم‌های تجارت الکترونیک و استفاده از مدل‌های تحلیلی می‌تواند به شناسایی نقاط آسیب‌پذیر و تدوین راهبردهای پیشگیرانه کمک کند (Liu, 2011). بنابراین، ضعف بانک‌های خصوصی در استفاده از این سیستم‌ها، بیانگر فاصله قابل توجه آنان با استانداردهای نوین امنیت سایبری است.

یافته‌های پژوهش حاضر نشان داد که اعتماد مشتریان و امنیت اطلاعات ارتباطی مستقیم و دوسویه با یکدیگر دارند. در واقع، هرچه سطح امنیت سامانه‌های بانکی افزایش یابد، اعتماد مشتریان به خدمات الکترونیک نیز بیشتر خواهد شد. این یافته با نتایج مطالعات متعددی همسو است که امنیت را مهم‌ترین عامل شکل‌گیری اعتماد الکترونیک معرفی کرده‌اند (Kim et al., 2010; Mehdizadeh & Moloudian, 2019). مهدی‌زاده و مولودیان نشان دادند که ادراک مشتریان از امنیت، تأثیر مستقیمی بر اعتماد الکترونیکی آنان به سیستم‌های پرداخت دارد (Mehdizadeh & Moloudian, 2019). همچنین کیم و همکاران بیان کردند که محرمانگی اطلاعات و قابلیت اطمینان سیستم‌های پرداخت، از مهم‌ترین عوامل مؤثر بر پذیرش خدمات تجارت الکترونیک است (Kim et al., 2010). از سوی دیگر، سوتیا و همکاران تأکید کردند که اعتماد به پرداخت الکترونیک، نقش کلیدی در رضایت و وفاداری مشتریان دارد (Sutia et al., 2020).

در پژوهش حاضر، یکی از نقاط قوت بانک‌های خصوصی، تعهد کارکنان به حفظ اطلاعات مشتریان و اطلاع‌رسانی به کاربران در هنگام انجام تراکنش‌ها بود. هرچند این نقاط قوت در مقایسه با ضعف‌ها از وزن کمتری برخوردار بودند، اما می‌توانند به‌عنوان مبنایی برای توسعه فرهنگ امنیت اطلاعات در بانک‌ها مورد استفاده قرار گیرند. تگی‌پورین بیان کرد که تجربه مثبت مشتری و ادراک او از کیفیت خدمات بانکی، نقش مهمی در تقویت ارزش برند و اعتماد مشتریان دارد (Taghipourian, 2026). در نتیجه، بانک‌هایی که بتوانند امنیت و شفافیت بیشتری در خدمات الکترونیک خود ایجاد کنند، از مزیت رقابتی بیشتری در بازار برخوردار خواهند شد.

نتایج پژوهش حاضر همچنین نشان داد که توسعه تجارت الکترونیک و بانکداری دیجیتال بدون توجه به الزامات امنیتی می‌تواند پیامدهای اقتصادی و اجتماعی گسترده‌ای به همراه داشته باشد. رشد فناوری‌های فین‌تک، بانکداری هوشمند و هوش مصنوعی، فرصت‌های جدیدی برای ارتقای کیفیت خدمات بانکی ایجاد کرده است، اما در عین حال تهدیدهای پیچیده‌تری نیز به وجود آورده است (Xu et al., 2025; Yousefi et al., 2025). یوسفی و همکاران بیان کردند که استفاده از هوش مصنوعی در بانکداری هوشمند، علاوه بر افزایش کارایی، می‌تواند زمینه‌ساز ظهور تهدیدهای نوین سایبری نیز باشد (Yousefi et al., 2025). از این رو، بانک‌ها باید همزمان با توسعه فناوری‌های نوین، ظرفیت‌های امنیت سایبری خود را نیز ارتقا دهند.

یافته‌های این پژوهش همچنین با مطالعات مربوط به رفتار مشتریان در تجارت الکترونیک همخوانی دارد. سیدی و همکاران نشان دادند که اعتماد مشتریان، مهم‌ترین عامل در بهبود رفتار مصرف‌کنندگان در تجارت الکترونیک است (Seidi et al., 2024). همچنین لام و اوسلی بیان کردند که سهولت استفاده، رضایت و اعتماد مشتریان، نقش مهمی در افزایش تمایل خرید آنلاین دارند (Lam & Osly, 2021). بنابراین، امنیت تجارت الکترونیک نه‌تنها یک ضرورت فنی، بلکه یک عامل کلیدی در موفقیت بازاریابی و توسعه اقتصادی بانک‌ها محسوب می‌شود.

در مجموع، نتایج پژوهش حاضر نشان می‌دهد که بانک‌های خصوصی شهر زاهدان برای دستیابی به امنیت پایدار در تجارت الکترونیک نیازمند اتخاذ راهبردی تدافعی و در عین حال توسعه‌گرا هستند. این راهبرد باید مبتنی بر کاهش ضعف‌های زیرساختی، ارتقای آموزش کارکنان، توسعه پروتکل‌های امنیتی استاندارد، به‌کارگیری فناوری‌های نوین امنیتی و افزایش آگاهی مشتریان باشد. همچنین، ایجاد نظام‌های جامع مدیریت ریسک و امنیت سایبری می‌تواند نقش مهمی در کاهش تهدیدها و افزایش اعتماد عمومی به خدمات بانکداری الکترونیک ایفا کند (Azizi Sarkhani & Kordlouei, 2016; Hedavand et al., 2021).

از محدودیت‌های پژوهش حاضر می‌توان به محدود بودن جامعه آماری به بانک‌های خصوصی شهر زاهدان اشاره کرد که ممکن است تعمیم نتایج به سایر مناطق کشور را با احتیاط همراه سازد. همچنین، استفاده از روش خودگزارشی و اتکای بخشی از داده‌ها به دیدگاه مدیران و کارکنان بانک‌ها، احتمال سوگیری پاسخ‌ها را افزایش می‌دهد. محدودیت زمانی و دشواری دسترسی به برخی اطلاعات امنیتی بانک‌ها نیز از دیگر محدودیت‌های این مطالعه بود.

پیشنهاد می‌شود پژوهش‌های آینده به بررسی تطبیقی امنیت تجارت الکترونیک در بانک‌های دولتی و خصوصی بپردازند و نقش فناوری‌های نوین مانند هوش مصنوعی، بلاک‌چین و یادگیری ماشین را در ارتقای امنیت بانکداری الکترونیک بررسی کنند. همچنین، مطالعه تأثیر متغیرهای فرهنگی، رفتاری و روان‌شناختی مشتریان بر ادراک امنیت و اعتماد الکترونیک می‌تواند زمینه توسعه مدل‌های جامع‌تر امنیت تجارت الکترونیک را فراهم سازد.

در حوزه کاربردی، پیشنهاد می‌شود بانک‌های خصوصی با سرمایه‌گذاری در زیرساخت‌های امنیت سایبری، استفاده از سیستم‌های تشخیص نفوذ، آموزش مستمر کارکنان و اجرای سیاست‌های جامع امنیت اطلاعات، سطح امنیت خدمات الکترونیک خود را ارتقا دهند. همچنین، طراحی برنامه‌های آموزشی برای مشتریان، توسعه سامانه‌های احراز هویت چندمرحله‌ای و تدوین استانداردهای بومی امنیت تجارت الکترونیک می‌تواند به افزایش اعتماد عمومی و توسعه پایدار بانکداری دیجیتال کمک کند.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

موازین اخلاقی

در تمامی مراحل پژوهش حاضر اصول اخلاقی مرتبط با نشر و انجام پژوهش رعایت گردیده است.

تشکر و قدردانی

از تمامی کسانی که در انجام این پژوهش ما را همراهی کردند تشکر و قدردانی به عمل می‌آید.

Extended Abstract

Introduction

The rapid development of information and communication technologies has fundamentally transformed the structure of modern business environments and financial systems. The emergence of digital platforms, smart banking, and electronic commerce has significantly changed the way organizations provide services and interact with customers (Sarlak, 2012; Xu et al., 2025). In this context, electronic commerce has become one of the most important pillars of the digital economy, enabling organizations to provide faster, more accessible, and more efficient services. Banking institutions, in particular, have increasingly adopted electronic commerce infrastructures to improve operational efficiency, reduce transaction costs, and enhance customer satisfaction (Mahmoudzadeh, 2016; Taghipourian, 2026). However, the expansion of electronic commerce has simultaneously increased the complexity of cybersecurity threats and information security risks, making security one of the most critical challenges in electronic banking systems (Kraft & Kakar, 2009; Torabi & Zamani, 2013).

Security in electronic commerce refers to the protection of information, digital transactions, communication infrastructures, and customer data against unauthorized access, destruction, misuse, or disclosure. In the banking sector, electronic security is directly associated with customer trust and organizational credibility. Customers are unlikely to use online banking systems if they perceive them as insecure or unreliable (Kim et al., 2010; Lam & Osly, 2021). Therefore, the sustainability and effectiveness of electronic commerce depend largely on the ability of financial institutions to establish secure infrastructures and maintain customer confidence. Previous studies have demonstrated that customers' perceptions of security significantly affect their trust in online payment systems and their willingness to adopt electronic banking services (Mehdizadeh & Moloudian, 2019; Sutia et al., 2020).

The increasing use of digital technologies, FinTech services, and artificial intelligence applications in banking has intensified the need for more sophisticated security frameworks. Although digital transformation has created new opportunities for banks to improve service quality and operational performance, it has also introduced new vulnerabilities and cyber threats (Xu et al., 2025; Yousefi et al., 2025). Threats such as data breaches, phishing attacks, identity theft, malware intrusion, and weaknesses in authentication systems have become major concerns for electronic banking systems worldwide (Saravari, 2023). In response to these

threats, researchers have emphasized the importance of implementing advanced security technologies such as encryption mechanisms, digital signatures, intrusion detection systems, and multi-factor authentication processes (Pormozeh et al., 2012; Shemin & Vipinkumar, 2016).

Several studies have highlighted the strategic role of security in customer satisfaction and electronic commerce development. Alalwan et al. found that perceived risk significantly influences customers' intentions to adopt internet banking services (Alalwan et al., 2018). Similarly, Kim et al. demonstrated that customer trust in electronic payment systems is largely shaped by perceived confidentiality, integrity, and reliability of banking systems (Kim et al., 2010). Moreover, Seidi et al. emphasized that customer trust is one of the key determinants of positive customer behavior in electronic commerce environments (Seidi et al., 2024). Consequently, improving electronic commerce security is not merely a technical requirement but also a strategic necessity for customer retention and sustainable competitive advantage in the banking industry.

In Iran, and particularly in less developed regions such as Sistan and Baluchestan Province, electronic banking systems face additional infrastructural and managerial challenges. Mahna identified limitations such as inadequate technical infrastructure, insufficient human resources, and low digital literacy as major barriers to the development of electronic commerce in the region (Mahna, 2009). Furthermore, previous studies have indicated that many organizations still lack coherent cybersecurity strategies and integrated security policies despite growing awareness of cyber threats (Hajmalek & Tavakoli, 2016; Saravari, 2023). Therefore, identifying internal weaknesses, external threats, organizational strengths, and environmental opportunities is essential for developing effective security strategies in electronic banking systems. SWOT analysis has been recognized as an appropriate strategic tool for evaluating internal and external factors influencing organizational security performance (Alrawashdeh et al., 2012; Liu, 2011).

Considering the importance of electronic commerce security in banking systems and the increasing risks associated with digital transformation, the present study aimed to formulate electronic commerce security strategies in private banks of Zahedan using SWOT analysis to identify strengths, weaknesses, opportunities, and threats affecting banking security systems.

Methods and Materials

This study was applied in terms of purpose and employed a mixed-method descriptive–analytical design. The statistical population consisted of 50 managers and specialists working in the field of electronic commerce and electronic banking in private banks located in Zahedan city. Participants were selected using the snowball sampling technique due to the specialized nature of the research topic and the limited accessibility of qualified experts in electronic banking security.

Data collection was conducted through expert evaluations and assessments of electronic commerce security indicators in private banking systems. The study focused on identifying internal and external factors affecting the security of electronic commerce in banking services. Internal factors included organizational strengths and weaknesses, while external factors involved opportunities and threats related to electronic banking security.

The SWOT analytical framework was employed to evaluate the strategic position of private banks regarding electronic commerce security. Initially, all identified factors were standardized using a numerical scale ranging from 1 to 10 based on their importance and impact on security performance. Then, mean coefficients were calculated for strengths, weaknesses, opportunities, and threats according to the experts' evaluations. Subsequently, internal and external factors were compared and weighted to determine the dominant strategic orientation suitable for improving electronic commerce security in private banks of Zahedan.

The analysis process involved identifying the most influential weaknesses and threats, assessing existing organizational strengths, and determining available opportunities for security enhancement. Finally, based on the SWOT matrix results and the internal–external strategic positioning model, appropriate security strategies were formulated for private banking systems in Zahedan.

Findings

The findings revealed that weaknesses and threats had significantly greater influence on the security status of electronic commerce in private banks compared to strengths and opportunities. Weaknesses obtained the highest mean coefficient (9.45), followed by threats (6.21), while strengths (9.18) and opportunities (5.13) demonstrated lower relative impact. These results indicate that private banks in Zahedan face substantial internal vulnerabilities and external cybersecurity challenges in their electronic commerce systems.

The most critical weaknesses identified in the study included inconsistencies in encryption mechanisms, vulnerability of banking information to natural disasters such as fire and earthquakes, lack of alternative software systems during service interruptions, weak customer authentication processes, and insufficient control mechanisms during activation of electronic services. Additional weaknesses included customers' failure to maintain confidentiality of financial information, inadequate governmental support for electronic commerce security, and lack of updated operating systems and secure applications.

The most important external threats involved inadequate employee training regarding cyberattack prevention, lack of effective intrusion detection systems, insufficient use of event logging and monitoring systems, and failure to implement standard security protocols and valid digital certificates in internet banking systems. These findings suggest that both technological and human factors contribute substantially to the insecurity of electronic banking services in private banks.

The SWOT matrix analysis demonstrated that the strategic position of private banks in Zahedan falls within the defensive zone. The internal–external matrix indicated that weaknesses and threats outweighed strengths and opportunities, suggesting that defensive strategies focused on minimizing vulnerabilities and avoiding threats should be prioritized. The analysis further showed that banks should concentrate primarily on strengthening security infrastructures, improving authentication systems, implementing standard cybersecurity protocols, and enhancing employee awareness and technical capabilities.

Among the identified strengths, employee commitment to preserving customer information, customer notification systems through SMS and email alerts, and relatively secure banking software were recognized as

positive factors supporting electronic commerce security. In addition, opportunities such as the use of digital signatures, backup servers, and unauthorized access detection systems were identified as potential areas for future security development.

Overall, the findings highlighted that private banks in Zahedan require comprehensive strategic planning to improve electronic commerce security. The dominant security strategy should focus on reducing internal weaknesses while simultaneously addressing external cyber threats through integrated technological, managerial, and educational approaches.

Discussion and Conclusion

The findings of this study indicate that private banks in Zahedan are currently operating within a vulnerable electronic commerce security environment characterized by significant internal weaknesses and external threats. The dominance of weaknesses and threats over strengths and opportunities suggests that the banking sector has not yet achieved sufficient cybersecurity maturity to fully support secure electronic commerce operations. This situation reflects broader challenges faced by financial institutions in developing digital economies where rapid technological expansion is not always accompanied by adequate security infrastructures and strategic planning.

One of the most important findings was the weakness of authentication mechanisms and inconsistencies in encryption systems. These deficiencies increase the risk of unauthorized access, identity theft, and financial fraud. In digital banking environments, authentication systems constitute the first layer of defense against cyberattacks; therefore, weaknesses in this area can seriously undermine customer trust and organizational credibility. Furthermore, the absence of standard security protocols and intrusion detection systems indicates that many banks still rely on outdated or fragmented security approaches rather than integrated cybersecurity frameworks.

The findings also emphasized the importance of human and organizational factors in electronic commerce security. Inadequate employee training and insufficient awareness regarding cyber threats were identified as major threats affecting banking security. This demonstrates that cybersecurity cannot be addressed solely through technological solutions; rather, it requires the development of organizational security culture, continuous staff training, and strategic management of information security. Employee behavior, customer awareness, and institutional commitment all play essential roles in reducing electronic banking vulnerabilities.

Another significant result of the study was the strong relationship between security and customer trust. Secure electronic banking systems improve customer confidence, increase satisfaction, and encourage greater adoption of online financial services. Consequently, enhancing electronic commerce security can contribute not only to risk reduction but also to customer loyalty, competitive advantage, and sustainable organizational performance. In the era of smart banking and digital transformation, security has become a strategic organizational asset rather than merely a technical requirement.

The study further demonstrated that private banks need to adopt defensive security strategies emphasizing vulnerability reduction and threat prevention. Such strategies should include strengthening cybersecurity infrastructures, implementing advanced encryption and authentication systems, developing intrusion detection mechanisms, creating backup systems, and establishing comprehensive incident response procedures. Moreover, integrating artificial intelligence and intelligent monitoring technologies into banking security systems may significantly improve threat detection and risk management capabilities in the future.

In conclusion, the present study revealed that electronic commerce security in private banks of Zahedan is confronted with substantial technological, organizational, and environmental challenges. The dominance of weaknesses and threats indicates the urgent need for strategic interventions aimed at improving cybersecurity readiness and strengthening electronic banking infrastructures. Effective electronic commerce security requires a comprehensive approach integrating technological innovation, organizational management, employee education, and customer trust development. By implementing coherent security strategies and investing in advanced cybersecurity systems, private banks can improve the safety of electronic transactions, enhance customer confidence, and support the sustainable growth of digital banking services.

References

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Algharabat, R. (2018). Examining factors influencing Jordanian customers' intentions and adoption of internet banking: Extending UTAUT2 with risk. *Journal of Retailing and Consumer Services*, *40*, 125-138.

Alrawashdeh, B., Areiqat, A., & Dbbaghieh, M. (2012). The role of information technology in reducing risk of electronic banking services in the Jordanian banking sector. *Journal of Computer Science*, *8*(3).

Azizi Sarkhani, M. J., & Kordlouei, H. (2016). Examining E-Banking Security Tools in the Public Banking Sector of Indian Banks with a Review of Globalization. *Investment Knowledge*, *5*(18), 253-262. https://www.jik-ifea.ir/article_8630.html

Hajmalek, M., & Tavakoli, A. (2016). Assessing the Level of Security in E-Commerce Using Shannon Entropy and Dempster-Shafer Theory. *Information Technology Management*, *8*(1), 77-100. https://sid.ir/paper/140399/fa

Hedavand, M., Mahdavi, N., Ahadipour Kordmahaleh, M., Seifi, H., & Azimi, M. (2021). A Review of the Usability and Security Evaluation Model of Websites in E-Commerce. Scientific Research Conference on New Achievements in Management, Accounting, and Economics Studies in Iran,

Jalali, A., Pourjafar, M., Safavi, S. A., & Ranjbar, E. (2024). Analyzing the Effects of Technology on Improving the Quality of Urban Public Spaces within the Framework of Smart Cities: Case Study of Iran Mall, Tehran. *Iranian Urban Design Studies*, *1*(2), 183-210. https://www.sid.ir/paper/1590967/fa

Kiljan, S., Ranken, H., & Eekelen, M. (2018). Evaluation of transaction authentication methods for online banking. *Future Generation Computer Systems*, *80*, 430-447.

Kim, C. H., Tao, W., Shin, N., & Kim, S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, *9*(1), 84-95.

Kraft, T. A., & Kakar, R. (2009). E-commerce security. Proceedings of the Conference on Information Systems Applied Research, Washington, DC, USA.

Lam, A., & Osly, U. (2021). The Effect of Customer Trust, Satisfaction and Ease on Buying Interest in E-Commerce. https://doi.org/10.2139/ssrn.3767881

Liu, D. (2011). E-commerce system security assessment based on grey relational analysis comprehensive evaluation. *International Journal of Digital Content Technology and Its Applications*, *5*(10), 279-284.

Mahmoudzadeh, F. (2016). The Concept and Types of E-Commerce. Congress of Islamic Sciences and Humanities,

Mahna, S. (2009). *Limitations and Solutions for the Development of E-Commerce in Sistan and Baluchestan Province*. Al-Mahdi Press.

Mehdizadeh, A., & Moloudian, H. (2019). Examining the Effect of Customers' Perception of Security on E-Trust in Payment Systems: A Study of Bank Tejarat Customers in Dargaz County. Second National Conference on Modern Advances in Science and Metascience, Mashhad.

Mohammadi, R. (2026). Development and Validation of a Model for Evaluating the Effect of Banking Risks on the Stability of Iran's Banking System. *Dynamic Management and Business Analysis*, 1-18. https://www.dmbaj.com/index.php/dmba/article/view/272

Pishgahpour, E., Nasiri, N., & Azadi, Z. (2017). Examining Security in E-Commerce. Fourth National Conference on Information Technology, Computer, and Telecommunications, Mashhad.

Pormozeh, M., Dargolaleh, A., & Honarmand, M. (2012). An Applied Approach to E-Commerce Security. First Conference on New Ideas in Electrical Engineering, Khorasgan Branch, Islamic Azad University, Isfahan.

Saravari, A. R. (2023). Security in E-Commerce. Third International Conference on Management, Business, Economics, and Accounting,

Sarlak, M. (2012). The Effect of Information and Communication Technology on Employment in the Industrial Sector of Markazi Province. *Applied Economics*, *3*(8), 79-109.

Seidi, M., Alizadeh Meshkani, F., Sardari, A., & Naami, A. (2024). Designing a Model for Improving the Behavior of E-Commerce Customers in Iranian Handicraft Industries through Enhancing Customer Trust. *Value Creation in Business Management*, *4*(2), 91-117. https://doi.org/10.22034/jvcbm.2023.407147.1140

Shemin, P. A., & Vipinkumar, K. S. (2016). E-Payment System using Visual and Quantum Cryptography. International Conference on Emerging Trends in Engineering Science and Technology,

Sutia, S., Fahlevi, M., Saparudin, M., Dasih, I., & Sari, M. (2020). Should e-Payment Trust be eCommerce Implemented as a Consumer Satisfaction Factor? *Journal of Marketing Management*, *35*, 194-216. https://doi.org/10.1051/e3sconf/202020216002

Taghipourian, M. J. (2026). The role of emotional branding on brand equity in the banking sector: Is customer experience a mediator? *Dynamic Management and Business Analysis*, 1-17. https://www.dmbaj.com/index.php/dmba/article/view/247

Torabi, M., & Zamani, K. (2013). Examining and Analyzing Security Challenges in E-Commerce and Countermeasures. Computer Engineering and Sustainable Development with an Emphasis on Computer Networks, Modeling, and Systems Security, Mashhad.

Xu, F., Kasperskaya, Y., & Sagarra, M. (2025). The impact of FinTech on bank performance: A systematic literature review. *Digital Business*, *5*(2), 100131. https://doi.org/10.1016/j.digbus.2025.100131

Yousefi, S., Pournejaf, M., & Hosseinabadi, L. (2025). *Applications of Artificial Intelligence in the Digital Economy and Smart Banking: Examining Conceptual Models, Challenges, and Solutions* The Fourth International Congress on Management, Economics, Humanities, and Business Development, https://civilica.com/doc/2391612