Proposing a Cybersecurity Model for Electronic Banking Using a Grounded Theory Approach

Hossein Babaee[1], Mansoureh Aligholi[2]*, Daryoush Gholamzadeh[3], Mohammadreza Radfar[4]

1.Department of Information Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
2.Department of Business Administration, Central Tehran Branch, Islamic Azad University, Tehran, Iran (Corresponding author).
3.Department of Public Administration, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
4.Department of Financial Management and Accounting, South Tehran Branch, Islamic Azad University, Tehran, Iran.
*** Corresponding author email address**: aligholi@iauctb.ac.ir

Received: 2024-11-02 **Reviewed:** 2024-12-05 **Revised:** 2025-01-01 **Accepted:** 2025-02-03 **Published:** 2025-06-30

Abstract

The present study was conducted using a qualitative approach, and the research method was fundamental in terms of its objective. The analysis of this study was carried out using Grounded Theory. The statistical population included experts in electronic banking and cybersecurity from Bank Mellat, cybersecurity specialists from the Ministry of Petroleum, and academic experts. The study was conducted based on the perspectives of 15 experts from these domains. The data collection tool consisted of semi-structured interviews with semi-open-ended questions. Among the identified factors, axial coding was performed, and based on this, a linear relationship was established among the research categories, including core categories, causal conditions, contextual conditions, intervening conditions, strategies, and outcomes, leading to the development of a qualitative research model. The results of this study demonstrated that developing a cybersecurity model for electronic banking is essential, particularly in response to the increasing cybersecurity threats. Since cyber threats against the banking system undermine public trust in governance and pose a threat to national security, utilizing advanced technologies such as blockchain and machine learning, alongside user behavior analysis and organizational culture, can enhance security and increase customer trust in electronic banking services.

Keywords: *Cybersecurity, Electronic Banking, Advanced Technologies*

How to cite this article:
Babaee H , Aligholi M, Gholamzadeh D, Radfar M. (2025). Proposing a Cybersecurity Model for Electronic Banking Using a Grounded Theory Approach. Management Strategies and Engineering Sciences, 7(2), 71-82.

1. Introduction

Traditional banks are filled with conventional financial mechanisms and are under significant pressure to minimize costs sustainably. Given the high demand for tailored product portfolios and the availability of complex communication mechanisms, as well as advanced transactions, new types of companies known as financial technology services (FinTech) have emerged [1]. The financial sector has evolved over time due to technological advancements. However, over the past decade, technology-driven innovations in finance have significantly increased consumer access to various services, including payments, lending, insurance, savings, and investments [2]. Traditional banks, after collaborating with FinTech companies, become more vulnerable to cyber intrusions [3, 4].

As more services move online and data becomes widespread, data security has become a significant challenge for banks. With the increasing penetration of online banking services, companies can collect vast amounts of customer and visitor data, which are analyzed to generate insights into consumer purchasing patterns and strategies for acquisition and retention. If FinTech companies and traditional banks collaborate to mitigate cybersecurity risks, achieving profitability will be much more feasible. However, previous research on cybersecurity in this context is scarce [5-7].

A study by Aldahidhavi et al. (2020) on the impact of FinTech variables on cybersecurity showed that there are complementary relationships between independent variables in this sector. The study also demonstrated that cyberattacks have led to substantial efforts by professionals and researchers to introduce intelligent technologies such as artificial intelligence and other analytical tools to predict and counteract cyberattacks before they occur. In their research on cybersecurity fortification, they emphasized the link between cyberspace and physical systems [8]. Similarly, Najaf et al. (2020) highlighted that due to the increasing cyberattacks in electronic banking environments, enhanced monitoring and supervision are essential to reduce the vulnerability of the electronic banking ecosystem [1].

The rapid growth of digital transformation in the banking sector has significantly increased the potential attack surface for cyber threats. This transformation has exposed organizations to a higher level of cyber threat activities, as an increasing number of businesses adopt digital banking solutions [9]. In response to these developments, cyberattacks continue to evolve and expand, with malicious actors refining their techniques to outpace security teams. Understanding the nature of cyber threats and associated risks is essential, as financial leaders must acknowledge that attackers will inevitably exploit vulnerabilities. This awareness should drive improvements in service design, risk management, and workforce training, highlighting the necessity of comprehending the changing cyber threat landscape that financial institutions face [8, 10, 11]. Cyberattacks targeting fintech companies have surged in recent years [10]. While such attacks have existed since the late 2000s, the financial technology industry has seen a marked increase in cyber threats since 2017 [12]. The primary issue is that with the recent expansion and enhanced capabilities of financial and banking services, substantial risks have emerged, and these services are now frequently subjected to severe cyberattacks. Financial institutions remain among the most vulnerable entities to these threats, necessitating continuous oversight of banking operations and regulatory mechanisms to address the risks associated with electronic banking transformation [8]. Persistent cyberattacks result in the theft of valuable and sensitive data, hacking attempts, insider threats, ransomware, and phishing campaigns targeting banks. This has created a critical dilemma, casting doubt on the viability of partnerships between traditional banks and fintech firms [1]. Although many cyberattacks have limited impact and affect only a few individuals, several large-scale financial sector breaches over the past decade have had significant short- and long-term consequences [11]. These large-scale attacks have impacted a wide range of financial services, including retail payments, health insurance, investment services, consumer credit, and credit reporting. Every segment of the financial industry remains a potential target for such large-scale attacks [13]. Both regulatory authorities and customers have expressed concerns regarding data security. The widespread adoption of digital banking technologies has increased both the penetration and scale of cyberattacks, posing a significant threat to customer data security and privacy across digital banking channels. Regulatory awareness of cybersecurity risks may prompt policymakers to reconsider the balance between efficiency and security in financial services [14]. Moreover, securing customer data in digital financial channels often incurs costs that exceed those of providing digital financial services themselves, potentially affecting operational efficiency and profitability for digital financial service providers. This presents a major challenge for regulators [15]. The existence of robust consumer protection frameworks tailored to digital financial services is crucial in fostering trust and confidence among customers

[16]. Additionally, financial and banking reforms can enhance the delivery of secure, innovative, and user-friendly digital financial services [17]. Given these factors, implementing effective cybersecurity programs in banking has become more critical than ever [18].

Adedoyin et al. (2024) examined cybersecurity risks in online banking and the application of preventive strategies. Their study explored various cybersecurity dimensions in the banking industry, focusing on the increasing use of online banking and the simultaneous rise in cybercrime. The study sought to clarify the current cybersecurity landscape, evaluate the effectiveness of existing frameworks, and propose strategic enhancements to strengthen digital defenses [19]. Mehenaj Jerin (2024) investigated emerging cybersecurity threats in the banking sector, identifying vulnerabilities and proposing legal solutions. The study underscored the complexity and rapid growth of these threats, emphasizing the necessity of continuously updating cybersecurity regulations. It also highlighted the importance of raising awareness within banks and fostering international collaborations to effectively combat these threats [5]. Selvaraj (2021) explored the role of artificial intelligence (AI) in cybersecurity, particularly in detecting and preventing financial fraud. His study provided an in-depth analysis of cybersecurity tools, applications, challenges, and regulatory considerations affecting cybersecurity performance [20]. Aldahidhavi et al. (2020) analyzed the impact of fintech variables on cybersecurity, measuring their influence as a dependent variable. Their findings indicated that cyberattacks have driven significant efforts by experts and researchers to introduce intelligent technologies such as AI and other analytical tools to anticipate and counteract cyber threats before they materialize [8]. Najaf et al. (2020) conceptualized cybersecurity risks in fintech firms and banks, revealing that the cybersecurity risks faced by fintech firms negatively affect their partnering banks. Cybersecurity risks not only result in substantial financial losses but also erode investor trust in both fintech firms and their partner financial institutions. Their findings demonstrated that all fintech and banking partnerships are exposed to cyber threats, prompting regulatory authorities to reconsider fintech safety frameworks [1]. Vojdani et al. (2024) investigated the impact of data privacy and security in electronic banking on customer loyalty, with a focus on reliability. As electronic banking systems provide significant economic advantages, such as cost reduction, profitability enhancement, improved service quality, and expanded banking operations, many financial institutions have adopted digital banking models. The study applied structural equation modeling and confirmed its hypotheses with a 95% confidence level, affirming the role of data security in fostering customer loyalty [21]. Mousavi et al. (2024) examined the influence of security measures in electronic payment systems on customer trust and perceived security. Their study used a correlational and applied research design, analyzing responses from 118 customers of Bank Melli using structural equation modeling. The results indicated that transaction processes, security statements, and technical safeguards significantly influenced perceived security and trust, subsequently affecting customer engagement with electronic banking [22]. Parnak et al. (2023) investigated the relationship between perceived security and customer trust in NFC-mobile banking systems, revealing that security mediates the relationship between objective security measures and system usage. However, trust was found to mediate the relationship between technical safeguards and transaction processes, while its mediating effect between security statements and electronic payment adoption was insignificant [23]. Tahmasebi et al. (2021) proposed a strategic collaboration framework between private banks and fintech firms in Iran. Their findings indicated that environmental uncertainties facilitate strategic collaboration, wherein fintech opportunity assessment, customer digital behavior, demand analysis, fintech awareness, competitive market conditions, Islamic financial regulations, and business valuation serve as causal conditions. Additionally, internal factors within private banking systems function as intervening conditions. This strategic collaboration yields financial, procedural, operational, and relational benefits for both parties [24].

The primary challenge in the present study, considering the vulnerability of digital data frameworks—including risks of attacks, theft, fraud by hackers, and other cybercriminal activities—underscores the critical role of cybersecurity in electronic banking. This issue necessitates a practical approach to developing strategies to address cybersecurity concerns, representing a major research gap. A review of the literature on electronic banking indicates that despite the importance of cybersecurity in electronic banking programs, limited studies have been conducted in this area.

Most existing research has focused primarily on the potential risks that collaborations between banks and FinTech firms pose for banks. Few studies have investigated FinTech variables and their impact on cybersecurity, and no comprehensive model has been proposed that considers all key variables in this domain. Based on the literature review, there is a lack of studies dedicated to developing a model specifically for cybersecurity in electronic banking.

Existing research has either neglected to present a model for electronic banking entirely—focusing solely on cybersecurity risks and cyber threats in FinTech—or, if a model was proposed, it examined electronic banking from perspectives other than cybersecurity. Therefore, a theoretical gap exists in the research, highlighting the need for a developed model that can assess electronic banking from a cybersecurity perspective.

Considering the discussions above, the primary research question of this study is: "What is the developed cybersecurity model for electronic banking?"

2. Methodology

This study was conducted using a qualitative approach. From the perspective of its objective, the research method was fundamental. In terms of execution, it was a descriptive and correlational research method. The present study was analyzed qualitatively using Grounded Theory. The statistical population consisted of experts in electronic banking and cybersecurity at Bank Mellat, cybersecurity experts at the Ministry of Petroleum, and academic experts. The sample size, or the number of interviewees, depended on reaching the level of theoretical saturation, and purposeful sampling was employed. The data collection tool comprised semi-structured interviews with semi-open-ended questions, based on the Grounded Theory approach. The interview process involved determining the type of interview, designing the interview protocol, recording the interviews, coding the interviews, identifying, summarizing, and refining indicators, screening and refining indicators, and compiling the final list of indicators.

The Grounded Theory theorist selects a category during the open coding phase and places it at the center of the process under investigation as the “central phenomenon,” then links other categories to it. These other categories include “causal conditions,” “contextual and intervening conditions,” and “outcomes.” This phase involves creating a diagram known as the “coding paradigm,” which reveals the relationships among causal conditions, strategies, contextual and intervening conditions, and outcomes. For qualitative content analysis in this study, ATLAS TI software was used.

3. Findings and Results

This section is dedicated to analyzing the data and explaining how the qualitative and quantitative methods were implemented. The qualitative portion of this study was carried out based on the opinions of 15 experts. Of these individuals, 13 were male and 2 were female. In the end, 4 participants had between 10 to 15 years of work experience, and 11 participants had over 15 years of work experience.

To develop Grounded Theory, there are five analytical steps (not necessarily sequential) during which nine actions are followed: (1) designing the research plan, (2) data collection, (3) data organization, (4) data analysis, and (5) comparison with the literature.

In open coding, the data obtained from the interviews were first carefully examined and analyzed. Subsequently, the conceptualization process took place, and data that were similar in meaning were labeled with appropriate names. Code labeling was done based on the interviews, and the researcher attempted to adhere, as necessary, to the respondents’ insights in order to avoid any potential and unintended bias as much as possible. Throughout all coding processes, the researcher remained committed to theoretical sensitivity, which is one of the principles of Grounded Theory research, to enhance the richness of the study.

Sample codes and relevant interviews are presented below:

Table 1. Identified Codes Based on Interviews

Open Code	Interview
Blockchain	“Blockchain, as a distributed and immutable ledger, can enhance the transparency and security of transactions in electronic banking systems. Due to its decentralized structure, altering or tampering with data is extremely difficult, which significantly increases the level of security. Moreover, using blockchain in authentication processes and smart contracts can prevent cyberattacks.”
Machine Learning	“Machine learning algorithms assist in analyzing big data to identify suspicious and unusual patterns, improving the prediction of cyberattacks. Additionally, machine learning can be effective in detecting financial fraud, reducing security risks, and enhancing decision-making processes in electronic banking.”
Internet of Things (IoT)	“IoT devices enable banks to receive more information from their users and provide better services. However, these devices can also create new vulnerabilities for cyberattacks. Security in IoT for electronic banking means protecting all devices and their connections to prevent cyber threats.”
Cloud Computing	“Using cloud services for storing and processing banking data can improve the flexibility and efficiency of banking systems. Nevertheless, securing cloud data entails new challenges. The security model must include robust protocols like data encryption and access management to protect users’ sensitive information.”

Artificial Intelligence	"In cybersecurity, artificial intelligence is a powerful tool for detecting advanced threats and responding rapidly to attacks. AI-driven systems can continuously monitor network activities and prevent identified attacks. Moreover, AI can optimize security solutions and automate security processes."
High Volume of Data	"Electronic banking manages a vast volume of transactions and sensitive financial information daily. An increase in data volume implies a need for powerful infrastructures to store, process, and transfer these data. Security in this large volume of data is challenging because, as volume grows, so does the risk of data breaches and cyberattacks. Employing technologies such as AI and cloud computing can help manage huge datasets and prevent unauthorized access."
Data Complexity	"Data in electronic banking are not only extensive in volume but also complex in structure and interconnections. This data includes financial transactions, users' personal information, and system data, each requiring protection from different angles. Implementing a security model capable of handling these complexities necessitates using advanced technologies like blockchain and machine learning, which can analyze complex data and predict threats."
Data Management	"Data management refers to how data are stored, accessed, and protected in electronic banking. Establishing robust frameworks for permission and access management, data encryption, and monitoring systems can prevent potential breaches and unauthorized access to sensitive data. Employing blockchain to ensure transparency and immutability of data is also effective in this regard."
Data Updates	"In electronic banking, data updates involve continuously updating systems, databases, and security infrastructures. Timely updates to data and security protocols can reduce vulnerabilities and prevent exploitation of security flaws. Artificial intelligence can be used to identify weaknesses and suggest necessary updates."
Cyberattacks	"Cyber threats such as DDoS attacks, phishing, and hacking of banking systems are very common in electronic banking. A security model must be able to detect and prevent such attacks. The use of machine learning and AI algorithms can help predict and identify threats, while blockchain and strong encryption can prevent unauthorized access and data alteration."
Robotic Attacks	"Robotic attacks refer to those carried out by bots or automated software. Such attacks often involve automating phishing processes, performing fraudulent transactions, or attempting to infiltrate banking systems. To combat these attacks, using advanced security systems and Intrusion Detection Systems (IDS) can be effective. Additionally, implementing security measures like CAPTCHA can block bots from accessing systems."
DDoS Attacks	"This type of attack targets a bank's servers with massive illegitimate traffic so that the system becomes unable to respond to legitimate requests. DDoS attacks can disable online banking systems and reduce customer trust. Countermeasures include load balancing solutions, advanced firewalls, and threat detection and response systems."
User Behavior Identification	"Identifying user behavior involves analyzing how users interact with the electronic banking system. This process helps detect normal and abnormal patterns. Information gathered from this analysis can be used to identify suspicious behaviors or cyberattacks. Machine learning techniques can help identify and predict abnormal behaviors."
Advanced Analysis of User Access Patterns	"This process involves in-depth analysis of the patterns in users' access to banking information and services. By leveraging advanced algorithms and machine learning, common and uncommon access patterns can be recognized. Such data can aid in detecting potential attacks and misuse, and it can also prevent financial fraud."
Suspicious Behavior Detection	"Suspicious behaviors may include repeated login attempts, unusual changes in transaction patterns, or access from abnormal locations. Using analytical tools and machine learning allows for identifying such behaviors and alerting security personnel to take preventative actions."
Updating User Biometric Information	"This process involves maintaining and updating biometric data such as fingerprints, facial recognition, and iris scans. Regular updates are vital to ensure accuracy and reliability. Changes in a user's physical condition, like injuries or appearance changes, can affect the performance of biometric systems. Consequently, continuous updates can prevent identity misuse and unauthorized access."
Identity Matching in Unauthorized Access	"Identity matching systems must be capable of identifying and rejecting unauthorized attempts. Employing multiple layers of authentication, such as two-factor authentication (2FA), and AI-based systems to detect suspicious patterns can aid in this process."
Information Security Awareness	"Establishing a strong security culture among employees and customers can help prevent cyberattacks and reduce risks. Ongoing education on cybersecurity and threat recognition can improve individuals' understanding and security measures."
Instability of the Digital Business Culture	"Given rapid changes in technology and consumer behavior, banks must have the flexibility and capability to adapt to new conditions. Such instability can create cybersecurity challenges, as attackers may exploit newly emerging weaknesses. Therefore, a security model must be able to forecast and respond to these changes and include strategies to deal with new threats."
Mass Behaviors	"Mass behaviors refer to the behavioral patterns of users within a large community or group, which can have positive or negative impacts on cybersecurity. For instance, if most users are optimistic about using new technologies such as electronic banking, the adoption rate may be high. However, if widespread fear and concern exist regarding information security, it may reduce usage of these services and increase vulnerabilities. Understanding mass behaviors can help cybersecurity model designers propose appropriate solutions to boost public trust."
Lack of Knowledge in Digital Business	"A lack of awareness about secure methods for using electronic banking services can put users at risk of cyber threats. Training and enhancing user knowledge about cybersecurity and digital commerce are essential to prevent misuse and increase people's confidence in electronic services."
Prevalence of Traditional Mindsets in Society	"Societies that remain traditionally committed to old, non-digital methods may resist new changes. Such traditionalism can hinder the adoption of new technologies, particularly electronic banking. In this situation, successfully implementing cybersecurity models requires changing societal attitudes and culture, as well as clearly communicating the benefits of digital banking."
Perceived Risk	"Perceived risk refers to individuals' sense of security threats associated with using electronic banking services. If users believe these services are risky, they may avoid adopting them. Therefore, managing perceived risk through education and awareness, providing transparent information on system security, and improving security protocols can help increase user trust."
Society's Slow Progress Toward Trust	"This component points to the gradual acceptance of new digital systems in many societies. Delays can result from previous negative experiences, lack of awareness, or an insufficient understanding of these systems. To expedite this process, banks and financial service providers must maintain effective communication with customers and reinforce trust through continuous advertising and training."

Local Regulations	“Local regulations refer to rules and laws that apply specifically to a particular country or geographic region. These regulations may address privacy requirements, data protection, and legal liabilities for security breaches. Banks must ensure that their security systems and operational methods comply with these regulations. Compliance with local regulations not only minimizes legal risks but also increases customer trust.”
International Laws	“International laws encompass agreements and standards ratified by international organizations and various countries. These may include cybersecurity agreements, anti-money laundering laws, and data protection regulations. Banks and financial institutions operating internationally must be aware of and comply with these regulations to avoid legal and economic complications.”
Banking and Local Regulations	“These regulations refer to rules specifically designed for the banking industry, usually enforced by financial regulatory bodies. They may include requirements for customer authentication, risk management, and cybersecurity obligations. Adhering to these regulations is vital for banks and contributes to creating a secure environment for financial transactions.”
Internal Policies	“Internal policies refer to the internal guidelines and operational procedures of a bank or financial institution focused on managing security risks and protecting sensitive information. These policies may involve incident response processes, employee training programs, and crisis management strategies. Having strong internal policies can facilitate compliance with external and local regulations.”
Regulatory and Governmental Policies	“These policies comprise legal and regulatory frameworks established by governments and regulatory authorities to protect financial and banking systems. They may include oversight of banking activities, security audits, and reporting requirements. Effective implementation of these policies increases security in electronic banking and maintains public trust in financial systems.”
Level of Awareness	“The level of awareness pertains to the amount of information and knowledge that users and staff have regarding security threats and methods for safeguarding information. Improving awareness helps users recognize potential risks and avoid unsafe behaviors. Regular training and informational programs can heighten awareness of best cybersecurity practices and threat mitigation strategies.”
Security Culture	“Security culture refers to the shared attitudes, beliefs, and behaviors in an organization or community about cybersecurity. A strong security culture fosters a secure environment and supports proper information security practices. This culture includes a commitment to following security policies, sharing information about threats, and encouraging continuous improvement in security processes.”
Safety Training Status	“Safety training status pertains to the quality and extent of security training provided to staff and users. Effective training should be conducted regularly and contain current content aligned with new threats. Such training can help identify suspicious behaviors, counter cyberattacks, and adhere to best security practices.”
Infrastructure Quality	“Infrastructure quality refers to the condition and capabilities of information technology and security systems in banks and financial institutions. High-quality infrastructure must protect sensitive data and information against cyberattacks. It includes secure networks, robust servers, encryption systems, and advanced technologies for threat detection and response. Infrastructure quality directly impacts an organization’s security capabilities.”
Technology Updates	“Technology updates involve keeping systems, software, and security protocols current to combat emerging threats. Security technologies must be continuously reviewed and updated to utilize the latest developments in cybersecurity. Regular software patches, installing security fixes, and hardware upgrades are among the measures that can boost security and reduce vulnerabilities.”

Axial coding is the second stage of data analysis in Grounded Theory in this study. The goal of this phase is to establish relationships among the categories generated during open coding. It is termed “axial” coding because the coding revolves around one research category, namely the ‘cybersecurity model in electronic banking.’ This category was chosen as the central category and placed at the center of the model because its traces and influence can be clearly observed in most of the data and interviewee quotations. Therefore, it can be situated at the center of the model, and other categories can be linked to it. In this study, Strauss and Corbin’s paradigmatic model was used for axial coding. This model assists the theorist in forming a comprehensive understanding of the theoretical process. The components of the paradigmatic model for axial coding are the central category, causal conditions, the prevailing context or environment, intervening conditions, strategies, and outcomes.

Table 2. Secondary (Axial) Coding

No.	Axial Coding	Open Coding	No.	Axial Coding	Open Coding
1	New and Advanced Technologies	- Blockchain - Machine Learning - Internet of Things (IoT) - Cloud Computing - Artificial Intelligence	12	Advanced Security Procedure	- Advanced Threat Management Platforms - Optimization and Automation of Security Processes - Authentication and Encryption in IoT Devices - IoT Device Management
2	Data Status	- High Volume of Data - Data Complexity - Data Management - Data Updates	13	Security Protocols and Standards	- Adhering to Security Standards and Protocols - Communication and Encryption Protocols - Authentication and Access Standards

					- Security Standards for Applications and Systems - Security Management and Threat Response
3	Cyber Threats	- Cyberattacks - Robotic Attacks - DDoS Attacks	14	Risk Management and Crisis Response	- Risk Management Methods and Processes - Risk Management Preparedness - Crisis Response to Combat Cyberattacks
4	User Behavior	- User Behavior Identification - Advanced Analysis of User Access Patterns - Suspicious Behavior Detection - Updating User Biometric Information - Identity Matching in Unauthorized Access	15	Data Protection	- Privacy - Data Integrity - Authentication - Access Control - Encryption - Transaction Approval
5	Attitudinal Factors	- Information Security Awareness - Instability of the Digital Business Culture - Mass Behaviors - Lack of Knowledge in Digital Business - Prevalence of Traditional Mindsets in Society - Perceived Risk - Society’s Slow Progress Toward Trust	16	Training and Awareness	- Employee Training in Information Security - Threat Prevention Training - User Information Campaigns - Training on Personal Data Protection Methods
6	Laws and Regulations	- Local Regulations - International Laws - Banking and Local Regulations - Internal Policies - Regulatory and Governmental Policies	17	Vulnerability Management	- Vulnerability Scanning and Assessment - Preventing Potential Damages - Rectifying Vulnerabilities - Updates and Patching
7	Organizational Culture	- Level of Awareness - Security Culture - Safety Training Status	18	Monitoring and Reporting	- Continuous Network Traffic Monitoring - Tracking Suspicious Activities - Reporting and Analysis
8	Technological Infrastructure	- Infrastructure Quality - Technology Updates - Technology Localization - Technology Standardization - Technology Adaptation - Technology Maintenance	19	Data Processing System	- Identifying Common Patterns - Data Mining - Security Algorithm Design - Big Data Analysis
9	Banking Industry	- Financial Regulations - Bank Internal Environment - Banking Industry Conditions - International Financial Regulations - Personalization - Bank Structure - Interbank Relations - Bank Tiers - Flexibility in the Banking Industry - Banking Industry Focus - Bank’s Position in Society - Industry Updates - Industry Hierarchy - Public vs. Private Ownership Status - Bank Reputation - Bank Position in the Stock Market	20	Backup and Recovery	- Creating Regular Backups - Disaster Recovery - Specialized Backup Team - Regular Data Sharing

10	Digital Economy	- Driver of Open Architecture - Open Data Policies - Digital Literacy - Data-Based Experimental Policy-Making - Cybersecurity - Reliable Digital Identity - Reliable Digital Data Hubs - Public Infrastructure for the Digital Economy	21	Employing Modern Techniques	- Biometric Authentication - Voice User Recognition - Synchronous Encryption - Homomorphic Encryption - Transparent Blockchain Transactions - Blockchain Smart Contracts - Cloud-Based Data Encryption - Role-Based Access Control
11	Protective and Security System	- Firewall - Intrusion Detection Systems - Event Management Systems	22	Customer Satisfaction	- Customer Satisfaction - Improving Customer Perception - Increasing Customer Loyalty - Growing Customer Base - Customer Education - Positive Customer Experience - Building Customer Trust
			23	Information Security	- Reducing Data Theft - Decreasing Exposure of Confidential Information - Decreasing Monetary Theft
			24	Cost Management	- Lowering Customer Reimbursement - Decreasing Damage Compensation - Reducing Regulatory Penalties - Cutting Security Protocol Costs
			25	Economic Efficiency	- Boosting Investments - Increasing Economic Activity - Enhancing Profitability

The main phase of data-based analysis is selective coding, where the researcher develops a theory based on the results of open and axial coding. In this section, the underlying causes and reasons for the formation of these conditions are discussed as theoretical memos, containing the analyst's reflections and thoughts concerning the research conditions.

Table 3. Grounded Theory Analysis (Causal, Contextual, and Intervening Conditions, Strategies, and Outcomes)

Selective Coding	Axial Coding
Causal Conditions	- New and Advanced Technologies - Data Status - Cyber Threats - User Behavior - Attitudinal Factors
Contextual Conditions	- Laws and Regulations - Organizational Culture - Technological Infrastructure - Banking Industry - Digital Economy
Intervening Conditions	- Protective and Security System - Security Protocols and Standards - Risk Management and Crisis Response
Strategies	- Data Protection - Training and Awareness - Vulnerability Management - Monitoring and Reporting - Data Processing System - Backup and Recovery - Employing Modern Techniques
Outcomes	- Customer Satisfaction - Information Security - Cost Management - Economic Efficiency

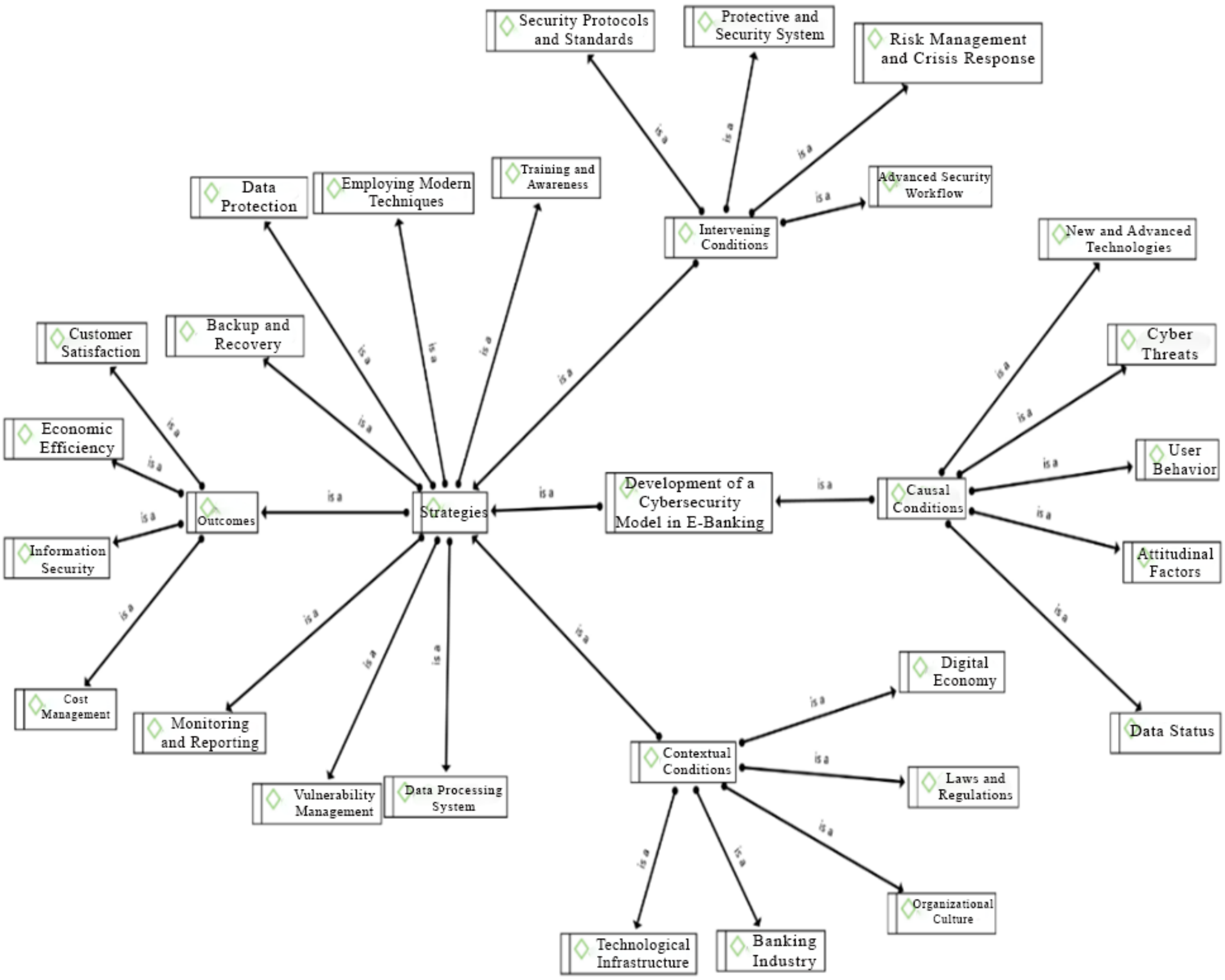

Figure 1. Paradigmatic Model of the Study (Cybersecurity Model in Electronic Banking)

4. Discussion and Conclusion

This study was conducted with the aim of developing a cybersecurity model for electronic banking. These findings align with the prior [5-7, 10, 11, 13, 14, 17, 19, 21, 22, 25-35]. The dimensions and components of this model are elaborated upon, and the interpretation of the study's findings is presented in a continuous and summarized manner. The results cover various dimensions, including causal conditions, contextual conditions, intervening conditions, strategies, and outcomes.

Causal conditions refer to factors that directly affect cybersecurity. These include new and advanced technologies such as blockchain, machine learning, the Internet of Things (IoT), cloud computing, and artificial intelligence, which are recognized as tools to enhance security and data management in electronic banking. These technologies contribute to threat detection and the improvement of security processes [36]. The volume and complexity of data, along with the need for data management and updates, are major challenges in cybersecurity [6]. These factors can increase vulnerabilities and cyber threats [7]. Cyberattacks, robotic attacks, and DDoS attacks are significant threats that jeopardize information security in electronic banking [34]. User behavior, including user behavior identification, analysis of access patterns, and updating biometric information, is a crucial factor that can enhance security [29]. Attitudinal factors, such as information security awareness, instability in the digital business culture, and a lack of digital knowledge, influence user behavior and, consequently, cybersecurity [25].

Contextual conditions refer to environmental factors influencing banking and cybersecurity. These include laws and regulations, where local and international laws, banking regulations, and supervisory policies serve as frameworks for implementing security measures [28]. Organizational culture, including the level of awareness and security culture within organizations, plays a crucial role in strengthening or weakening cybersecurity. Safety training and employee awareness of cyber threats are essential components of this culture [30]. The quality of technological infrastructure, technological updates, and standardization of technology directly impact cybersecurity [27]. The banking industry, including its regulatory environment, financial regulations, and interbank relations, significantly influences cybersecurity [26]. The digital economy, driven by open data policies, reliable digital identities, and public infrastructure for digital transactions, plays a fundamental role in cybersecurity improvements [35].

Intervening conditions are factors that can affect the implementation and effectiveness of cybersecurity models. Protective and security systems, including firewalls, intrusion detection systems, and event management systems, are essential tools for mitigating cyber threats [36]. Advanced security procedures, such as advanced threat management platforms, security process automation, and IoT device management, can improve cybersecurity effectiveness (Edmas et al., 2024). Security protocols and standards, particularly compliance with globally recognized frameworks such as PCI-DSS and ISO/IEC 27001, strengthen information security practices [37]. Risk management and crisis response involve the development of risk management methodologies, preparedness for cyberattacks, and crisis response plans, all of which are critical for ensuring cybersecurity resilience [31].

Strategies refer to actions that enhance cybersecurity. Data protection measures, including privacy safeguards, data integrity verification, authentication mechanisms, and access control, are vital for mitigating security risks [32]. Training and awareness initiatives, including employee education in cybersecurity, proactive threat prevention, and user awareness campaigns, contribute to reducing vulnerabilities [35, 38]. Vulnerability management entails regular vulnerability scanning, risk mitigation strategies, and the implementation of security patches and system updates [37]. Monitoring and reporting, involving continuous surveillance of network traffic and tracking of suspicious activities, help detect and respond to cyber threats effectively [31]. Backup and recovery measures, such as routine data backups and disaster recovery plans, are essential for minimizing the impact of cyber incidents [13].

The outcomes of cybersecurity in electronic banking refer to the results and impacts of implementing security models. Increased customer satisfaction, improved public perception of banking services, and enhanced customer loyalty are significant positive outcomes of cybersecurity efforts [33]. Strengthened information security, including reduced instances of data theft, lower exposure of confidential information, and minimized financial fraud, contributes to the overall trust in digital banking [39]. Cost management improvements, such as reduced expenditures on security protocols and minimized regulatory penalties, are direct benefits of enhanced cybersecurity frameworks [25]. Economic efficiency gains, including increased investments, expansion of digital economic activities, and improved profitability, further illustrate the benefits of a robust cybersecurity model [36].

Despite its significance and contributions, this research encountered several limitations. Rapid technological advancements present a challenge, as cybersecurity technologies evolve quickly, necessitating continuous updates to research findings. Cultural and social diversity also plays a role, as varying user perceptions and behaviors toward cybersecurity can lead to different research outcomes, highlighting the need for further investigation in diverse contexts. Additionally, restricted access to certain banking and financial data in some cases affected the precision and comprehensiveness of the research results.

Based on the findings of this study, several recommendations are proposed. Banks, particularly Bank Mellat, should invest more in emerging technologies such as blockchain, machine learning, and artificial intelligence, as these technologies contribute to cyber threat detection and enhanced data security. Employee training and awareness programs should be prioritized, with regular training sessions and practical workshops to educate banking staff on cyber threats and preventive measures. Strengthening security infrastructure should be an ongoing priority, with a focus on upgrading firewalls, intrusion detection systems, and other cybersecurity tools. Banks should adhere to internationally recognized security protocols and standards such as PCI-DSS and ISO/IEC 27001 to enhance security measures and minimize vulnerabilities. Furthermore, effective risk management and crisis response strategies should be implemented, including the development of comprehensive crisis response plans to counteract cyberattacks and mitigate security breaches.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] K. Najaf, C. Schinckus, M. I. Mostafiz, and R. Najaf, "Conceptualising cybersecurity risk of fintech firms and banks sustainability," 2020. [Online]. Available: https://shura.shu.ac.uk/id/eprint/27504.

[2] Y. Kim, Y. J. Park, J. Choi, and J. Yeon, "An empirical study on the adoption of "Fintech" service: Focused on mobile payment services," *Advanced Science and Technology Letters*, vol. 114, no. 26, pp. 136-140, 2015, doi: 10.14257/astl.2015.114.26.

[3] Y. Creado and V. Ramteke, "Active cyber defence strategies and techniques for banks and financial institutions," *Journal of Financial Crime*, vol. 27, no. 3, pp. 771-780, 2020, doi: 10.1108/JFC-01-2020-0008.

[4] F. J. Egloff, "Public attribution of cyber intrusions," *Journal of Cybersecurity*, vol. 6, no. 1, p. tyaa012, 2020, doi: 10.1093/cybsec/tyaa012.

[5] M. Mehenaj Jerin, "Emerging cyber security threats in the banking sector: Loopholes and solutions in the eye of law," *International Journal of Law*, vol. 10, no. 3, pp. 214-219, 2024.

[6] F. Rajabpour and H. Alizadeh, "Investigating the impact of environmental factors on the adoption of social media among small and medium enterprises during the Covid-19 crisis," in *The 6th National Conference and the 3rd International Conference on New Patterns of Business Management in Unstable Conditions*, 2024, pp. 1-13. [Online]. Available: https://civilica.com/doc/2098684/.

[7] O. Reis, J. S. Oliha, F. Osasona, and O. C. Obi, "Cybersecurity dynamics in Nigerian banking: trends and strategies review," *Computer Science & IT Research Journal*, vol. 5, no. 2, pp. 336-364, 2024, doi: 10.51594/csitrj.v5i2.761.

[8] H. M. K. Aldahidhavi, J. Z. S. Abdulreza, M. Sebai, and S. A. Harjan, "An efficient model for financial risks assessment based on artificial neural networks," *Journal of Southwest Jiaotong University*, vol. 55, no. 3, 2020, doi: 10.35741/issn.0258-2724.55.3.8.

[9] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital transformation: An overview of the current state of the art of research," *Sage Open*, vol. 11, no. 3, p. 21582440211047576, 2021, doi: 10.1177/21582440211047576.

[10] H. Alizadeh, K. Alba, and A. Rahdari, "Assessing of the development and sustainability of SMEs based on industry acceptance 4.0," in *1st National Conference on Modern Applied Research in Business and Industrial Development (ARBI2024)*, 2024, pp. 1-16. [Online]. Available: https://civilica.com/doc/2037846.

[11] H. Alizadeh and M. Foroughi, "A Strategic SWOT Analysis of Leading Electronics Companies based on Artificial Intelligence," *International Journal of Business Management and Entrepreneurship (IJBME)*, vol. 2, no. 2, pp. 1-16, 2023.

[12] D. Sadlakowski and A. Sobieraj, "The development of the FinTech industry in the Visegrad group countries," *World Scientific News*, vol. 85, pp. 20-28, 2017.

[13] M. S. Kabir and M. N. Alam, "IoT, Big Data and AI Applications in the Law Enforcement and Legal System: A Review," *International Research Journal of Engineering and Technology (IRJET)*, vol. 10, no. 05, pp. 1777-1789, 2023.

[14] C. Van Voorhis, W. Hatcher, T. Kalat, Y. Wang, and E. Hammad, "Towards an Automated Cybersecurity Risk Assessment of Next Generation Emergency Communication Networks-NG911," in *2024 IEEE World Forum on Public Safety Technology (WFPST)*, 2024, pp. 175-181, doi: 10.1109/WFPST58552.2024.00042.

[15] A. Mehrani, H. Alizadeh, and A. Rasouli, "Evaluation of the Role of Artificial Intelligence Tools in the Development of Financial Services and Marketing," *Journal of Technology in Entrepreneurship and Strategic Management*, vol. 1, no. 1, pp. 71-82, 2022.

[16] D. P. Widodo, T. Y. R. Syah, and D. A. Negoro, "Digital Channel and Customer Satisfaction on Financial Services," *Journal of Multidisciplinary Academic*, vol. 4, no. 3, pp. 159-163, 2020. [Online]. Available: https://www.kemalapublisher.com/index.php/JoMA/article/view/461.

[17] A. A. Shaikh, R. Glavee-Geo, H. Karjaluoto, and R. E. Hinson, "Mobile money as a driver of digital financial inclusion," *Technological Forecasting and Social Change*, vol. 186, p. 122158, 2023, doi: 10.1016/j.techfore.2022.122158.

[18] L. Tristan and P. Thng, "Outsourcing life cycle model for financial services in the fintech era," 2021. [Online]. Available: https://ink.library.smu.edu.sg/sis_research/6116/.

[19] O. Adedoyin Tolulope, O. Chinwe Chinazo, O. Onyeka Chrisanctus, and U. Chinonye Esther, "Cybersecurity risks in online banking: A detailed review and preventive strategies application," *World Journal of Advanced Research and Reviews*, vol. 21, no. 3, pp. 625-643, 2024, doi: 10.30574/wjarr.2024.21.3.0707.

[20] N. Selvaraj, "The essence of cybersecurity through fintech 3.5 in preventing and detecting financial fraud: a literature review," *Electronic Journal of Business and Management*, vol. 6, no. 2, pp. 18-29, 2021.

[21] B. Vojdani, "Investigating the Impact of Privacy and Security of Electronic Banking Services on Customer Loyalty with Emphasis on Reliability," in *1st International Conference on Management, Industrial Engineering, Accounting, and Economics in Humanities*, 2024. [Online]. Available: https://civilica.com/doc/2025680.

[22] S. A. Mousavi, "Investigating the Impact of Objective Security Dimensions of Electronic Payment Systems on Customers' Perception of Security and Trust (Case Study: Branches of Bank Melli in Kohgiluyeh and Boyer-Ahmad Province)," 2024. [Online]. Available: https://civilica.com/doc/1976050.

[23] A. Parnak, A. Gazari Neishabouri, and B. Seraj, "The Relationship Between Perceived Security and Customer Trust in the NFC-Mobile-Based Electronic Banking System," in *5th*

International Conference on Interdisciplinary Studies in Management and Engineering, 2022, pp. 674-691.

[24] D. Tahmasebi Aghbolaghi, M. Soltani, M. Shahbazi, and A. Ozaei, "Providing a Strategic Cooperation Framework Between the Private Banking System and FinTechs in Iran," *Technology Development Management*, vol. 9, no. 1, pp. 41-66, 2021.

[25] S. Goering, A. Beck, N. Dorfman, S. Schwarzwalder, and N. Wohns, "Privacy protections in and across contexts: why we need more than contextual integrity," *AJOB Neuroscience*, vol. 15, no. 2, pp. 149-151, 2024, doi: 10.1080/21507740.2024.2326932.

[26] R. Evren and S. Milson, "The Cyber Threat Landscape: Understanding and Mitigating Risks," 2024.

[27] S. Anwaar, "Harnessing Large Language Models in Banking: Banking Innovation with Operational and Security Risks," *World Journal of Advanced Engineering Technology and Sciences,* vol. 13, no. 1, 2024, doi: 10.30574/wjaets.2024.13.1.0426.

[28] N. Afrashteh, A. Mohammadi, A. Ahangari, and A. Asur, "Examining the Challenges and Solutions of Cybersecurity in Today's World," in *2nd International Conference on Management Research, Education, and Training in Education*, Tehran, 2024. [Online]. Available: https://civilica.com/doc/2039579.

[29] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications,* vol. 2, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.

[30] M. Shekarzehi, B. Hosseinbar, M. Hosseinbar, and A.-K. Arbabanahouk, "The Role of Cybersecurity in IT Education," in *15th International Conference on Management and Humanities Research in Iran, Tehran, Management and Humanities Research Conference in Iran*, 2023, vol. 15, 15 ed., pp. 775-780. [Online]. Available: https://civilica.com/doc/2013859.

[31] L. R. Sharma, S. Bidari, D. Bidari, S. Neupane, and R. Sapkota, "Exploring the mixed methods research design: types, purposes, strengths, challenges, and criticisms," *Glob Acad J Linguist Lit,* vol. 5, 2023.

[32] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon,* vol. 9, no. 3, 2023, doi: 10.1016/j.heliyon.2023.e14234.

[33] I. Negahdar, B. Pourghahramani, and J. Beigi, "Situational Prevention Approaches in Iran's Criminal Policy Towards Cybersecurity Violations in Light of International Documents," *Public Policy,* vol. 9, no. 2, pp. 97-114, 2023. [Online]. Available: https://civilica.com/doc/1654075.

[34] M. Kumar, "An overview of cyber security in the digital banking sector," *East Asian Journal of Multidisciplinary Research,* vol. 2, no. 1, pp. 43-52, 2023, doi: 10.55927/eajmr.v2i1.1671.

[35] S. Ahmadi, "Strategies for Developing the Digital Economy in Iran," *Economic Security Scientific Monthly,* vol. 11, no. 4, pp. 4-16, 2023. [Online]. Available: https://civilica.com/doc/1717234.

[36] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Transactions on Industrial Informatics,* vol. 17, no. 1, pp. 3-19, 2020, doi: 10.1109/TII.2020.2998479.

[37] A. Mazandarani, M.-T. Kheirabadi, and A. Bazazi, "A Lightweight Location-Aware Authentication Protocol for the Internet of Things," *Scientific Journal of Soft Computing and Information Technology,* vol. 12, no. 4, pp. 12-22, 2021. [Online]. Available: https://civilica.com/doc/1447733.

[38] M. Golparvar and K. Parsakia, "Building Resilience: Psychological Approaches to Prevent Burnout in Health Professionals," *KMAN Counseling & Psychology Nexus,* vol. 1, no. 1, pp. 159-166, 01/10 2023, doi: 10.61838/kman.psychnexus.1.1.18.

[39] H. Kaviani and N. Mirsepasi, "Designing an Organizational Capability Model in Cybersecurity," *Basij Strategic Studies,* vol. 24, no. 92, pp. 121-151, 2021. [Online]. Available: https://civilica.com/doc/1472913.