# Cyber Fraud in Bangladesh's Digital Financial Ecosystem: Tracing Responsibility across Banks, Mobile Financial Services and End Users

**Niloy Saha[1], Samia Kashem Juhi[2], MD Nizam Uddin[3], MD Sezadur Rahman[4*]**

**[1]Daffodil International University**

**[2]Shanto-Mariam University of Creative Technology**

**[3]Nanjing University of Posts and Telecommunications**

**[4]University of Eastern Finland**

**DOI: https://dx.doi.org/10.51244/IJRSI.2025.12110086**

**Received: 19 November 2025; Accepted: 28 November 2025; Published: 09 December 2025**

## ABSTRACT

Bangladesh's rapidly expanding digital financial ecosystem—driven by mobile financial services (MFS), online banking and fintech innovation—has transformed economic participation and inclusion. Yet, this digital boom has also triggered an alarming rise in cyber fraud, exposing structural weaknesses in how responsibility is shared across institutions and users. Using the 2025 Standard Chartered Bank (SCB) OTP scam as a focal case, this paper examines cyber fraud not as an isolated technical or user-level issue, but as a systemic failure within a distributed network of accountability. It analyzes how gaps in authentication protocols, inadequate coordination between banks and telecom operators, and insufficient user awareness collectively enable exploitation. Drawing on publicly available data, regulatory frameworks and incident reports, the study proposes a multi-actor responsibility model to map how trust and accountability should be shared among banks, MFS providers, regulators and end users. The findings highlight the urgent need for integrated cyber governance—one that bridges institutional silos, enforces shared liability, and builds digital resilience across Bangladesh's evolving financial landscape.

**Index Terms:** Cyber fraud, digital financial ecosystem, multi- actor accountability, systemic vulnerabilities, OTP scam, user-centered security.

## INTRODUCTION

Within the last decade Bangladesh has become as one of the fastest growing digital economy in South Asia. With the launch of it's first Mobile Financial Services (MFS) in 2011, the country has witnessed an extraordinary digital finance boom, by a decade exceeding 100 million registered users[1]. Bangladeshi MFS platforms such as bKash, Nagad and Rocket have become integral to everyday life—powering over BDT 1.4 trillion in domestic remittances in 2022 alone [2]. More than 40% of small and medium size enterprises (SMEs) now distribute salary and wage through MFS platforms. This illustrates how deeply these platforms are woven into Bangladesh's national economy[3].

This rapid digital transformation has also drawn cyber criminal's attention. Among millions of these users, many are elderly or with limited digital literacy that enter the digital financial system. They often become prime targets for scams exploiting through social engineering, SIM swapping and one- time-password (OTP) interception[4]. The most recent 2025 Standard Chartered Bank (SCB) OTP scam, which affected hundreds of users through coordinated network manipulation, brings the systemic vulnerabilities within this ecosystem into perspective. Despite continuous improvements in encryption, authentication and fraud detection, incidents continue to rise. These coordinated attacks breaks user trust and exposes the weaknesses that lies in institutional coordination.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

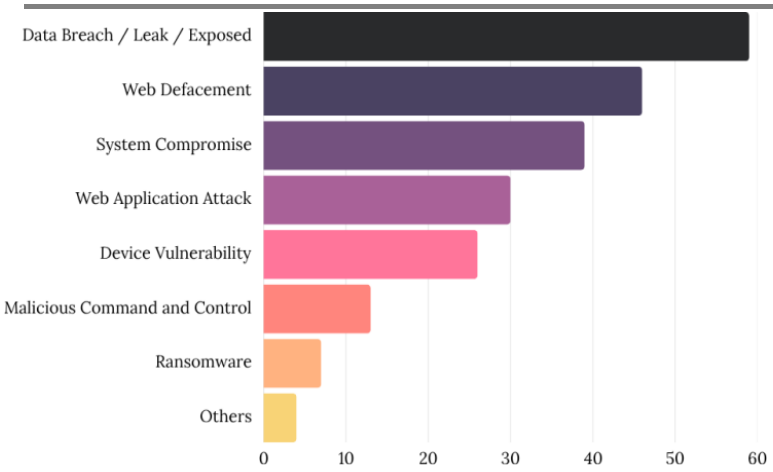


Figure 1. Distribution of reported cyber incidents by attack types [14]

Most existing studies and policy responses frame cyber fraud either as a technological failure (insufficient encryption, weak KYC systems) or as a user-level mistake (lack of awareness, negligence). This binary framing overlooks the inter- dependent nature of Bangladesh's digital-finance infrastructure where banks, MFS providers, telecom operators, regulators and users operate within a shared trust architecture. Failures in one node across authentication protocols, network security or consumer education—can cascade across the entire system.

This paper argues that cyber fraud in Bangladesh's digital financial ecosystem is fundamentally a systemic failure of distributed responsibility. It examines how fragmented account- ability among banks, telecom operators, regulators and users has enabled financial exploitation. The paper introduces a multi-actor responsibility model to clarify the shared obligations of these stakeholders and offers policy recommendations for building a more resilient, accountable, and user-secure digital finance environment.

## Related Work

The popularization of digital financial services has been a defining feature of emerging economies over the past decade, re- shaping the accessibility, speed and scale of financial transactions. In Bangladesh, Mobile Financial Services (MFS) and on- line banking platforms have similarly transformed the financial landscape, enabling millions to participate in formal finance [5]. The global literature agrees that such rapid digitization often introduces new vulnerabilities. Scholars have documented how fintech expansion, when coupled with insufficient cybersecurity governance, increases susceptibility to fraud, phishing and ac- count takeovers [6].

Several studies examine the behavioral aspects of cyber fraud. A study done on sub-Saharan Africa note that low dig- ital literacy, particularly among elderly or rural users significantly increases exposure to scams [7]. Researches have ob- served Similar pattern in Bangladesh's MFS adoption where users with limited knowledge of authentication protocols are disproportionately affected by OTP interception and SIM swap- ping attacks [8]. These insights underscore the importance of understanding fraud not merely as a technical failure but as a human-technology interaction problem.

The institutional perspective of financial cyber security is equally well documented. Research shows that fragmented governance and unclear lines of accountability exacerbate fraud risks. For example, in the Indian and Kenyan contexts, overlap- ping regulatory mandates between central banks, telecom regulators and MFS providers often lead to delayed responses and inconsistent enforcement [9] [10]. In Bangladesh, the literature indicates a similar challenge: regulatory oversight is distributed among the Bangladesh Bank, the Bangladesh Telecommunication Regulatory Commission (BTRC) and the Digital Security Agency. While each institution has formal responsibilities, there is scant evidence of coordinated, multi-stakeholder frame- works to address systemic vulnerabilities.

Several studies focus on technical fraud-mitigation strategies, including multi-factor authentication, transaction monitoring and machine learning–based anomaly detection. Research consistently highlights their limited effectiveness when institutional coordination is weak or user awareness is low [11]. Cybersecurity failures often

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

occur not because of a single actor's negligence but due to misalignment among interdependent ac- tors. Despite its relevance Bangladesh's digital-finance sector still tends to treat cyber fraud as an issue of either individual or organizational failure. High-profile fraud cases, including ATM heists, phishing attacks and OTP scams, are often cited in re- ports and media, but academic literature rarely provides system- level analyses of these incidents. The 2025 Standard Chartered

Bank (SCB) OTP scam exemplifies the kind of interdependent vulnerability that distributed-responsibility frameworks can illuminate. Such failures involve banks, telecom operators and regulatory oversight, compounded by user susceptibility.

In sum, the existing literature provides robust evidence of the growth of digital finance, patterns of cyber fraud and the socio-technical vulnerabilities of users. It also demonstrates that fragmented governance and insufficient coordination among institutions significantly exacerbate these risks. However, there is a clear gap in applying a systemic, distributed- responsibility perspective to Bangladesh's digital financial ecosystem. This gap justifies the present study, which integrates behavioral, technical, and institutional analyses to pro- pose a framework for multi-actor accountability in preventing and mitigating cyber fraud.

# METHODOLOGY

This study employs a qualitative and interpretive approach to investigate how cyber fraud emerges from systemic weaknesses across interdependent actors in Bangladesh's digital financial ecosystem. The SCB 2025 OTP scam was chosen as a focal case because it revealed cross-sector vulnerabilities and institutional fragmentation among banks, mobile financial service (MFS) providers, telecom operators, and regulators.

Data were drawn from secondary sources, including verified news articles, regulatory communications, and user testimonies. The incident first surfaced on social media platforms such as LinkedIn and Facebook, where victims shared their experiences of unauthorized withdrawals and their struggles to receive assistance from banks and telecom operators. These early posts were later substantiated by mainstream news coverage that provided detailed accounts and official responses.

The collected materials were analyzed thematically, identifying how technical, institutional, and user-level vulnerabilities interacted to enable systemic failure. While the study does not rely on confidential banking data or forensic audits, this interpretive approach captures the multi-actor dynamics that under- lie cyber fraud in Bangladesh's fintech ecosystem, forming the analytical basis for the subsequent case study.

CASE STUDY: THE SCB 2025 OTP SCAM

## Background of the SCB OTP Scam

The 2025 Standard Chartered Bank (SCB) OTP scam, though not the most shocking indecent, emerged as one of the most talked cyber fraud incidents in Bangladesh's recent digital- finance history. Over a period of several weeks, hundreds of customers reported unauthorized withdrawals from their ac- counts, facilitated through interception of one-time passwords (OTPs) intended for transaction verification [12]. The attackers supposedly employed coordinated social engineering campaigns, phishing calls and SIM swap techniques to gain control over victims' mobile numbers. This incident not only highlighted technical vulnerabilities but also underscored weaknesses in institutional coordination and regulatory oversight within the country's rapidly digitizing financial sector.

## Technical and Institutional Vulnerabilities

From a technical perspective, the scam exploited multiple points of failure. SIM swapping allowed attackers to reroute OTPs, undermining two-factor authentication. In several cases, SCB's transaction-monitoring protocols failed to flag unusual patterns, partly due to reliance on assumptions that mobile numbers were secure under user control. At the institutional level, the case revealed fragmented responsibility among banks, MFS providers and telecom operators. Banks depended on telecom operators for secure communication channels, while telecom

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

operators operated under the guidance of the Bangladesh Telecommunication Regulatory Commission (BTRC). This protocol lacked mechanisms for proactive coordination with financial institutions. Regulatory oversight by the Bangladesh Bank and the Digital Security Agency was largely reactive, addressing fraud after occurrence rather than providing preventive monitoring. The systemic weaknesses were compounded even after the fraud was reported. Instead of coordinated action to halt on- going attacks and trace stolen funds, stakeholders engaged in a cycle of blame-shifting. This post-incident inertia underscores a critical absence of a clear framework delineating who is responsible for such incidents.

**User-Level Vulnerabilities**

Several news reports indicates that victims of the SCB OTP scam included not only elderly individuals or users with limited technological literacy—but also well-educated and technologically aware users. Interviews and reports from affected customers revealed that even users who understood digital security concepts were deceived by sophisticated social engineering tactics, mostly calls or messages identical to be from bank officials or regulators [13]. These interactions persuaded users to disclose sensitive information, including OTPs, creating critical points of failure in the human-technology interaction chain.

This pattern demonstrates that user-level vulnerabilities were not merely a result of ignorance or lack of awareness. Instead, they functioned as enablers within a system already weakened by technical and institutional gaps. Elderly users with limited tech experience were naturally more susceptible, but even informed users became targets when attackers exploited trust, authority and urgency.

**System-Level Analysis**

The SCB OTP scam illustrates how interdependent actors interact to propagate risk. Combination of technical, institutional and human vulnerabilities combined to exploit security gaps, institutional fragmentation delayed responses and user susceptibility allowed social engineering to be succeed. This multi- layered failure demonstrates that cyber fraud in Bangladesh is a systemic problem, not solely a result of individual or organizational errors. The lack of a coordinated framework for account- ability meant no single actor could fully prevent the frauds in question.

**Key Insights**

Analysis of the SCB OTP scam yields several critical in- sights. First, cyber security failures are rarely isolated; they emerge from interactions among multiple actors. Second, fragmented governance and unclear lines of accountability create exploitable gaps that can undermine robust technical systems. Third, user vulnerability remains a decisive factor, but it is amplified by institutional and technical shortcomings rather than acting alone. These patterns underscore the necessity of a multi-actor responsibility approach, which recognizes that banks, MFS providers, telecom operators, regulators and users must all share accountability to prevent systemic failures.

**Systemic Vulnerabilities Across**

**Actors**

The SCB 2025 incident revealed not a failure of one institution, but a collapse of coordination across the digital-finance chain. Each actor—banks, mobile-financial-service providers, telecom operators, and regulators—fulfilled its own compliance obligations, yet the interfaces between them remained unguarded. Responsibility was treated as a bounded checklist rather than a shared continuum. When the scam exploited those seams, every institution could plausibly claim it had "followed protocol," leaving victims stranded in a gray zone of accountability.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

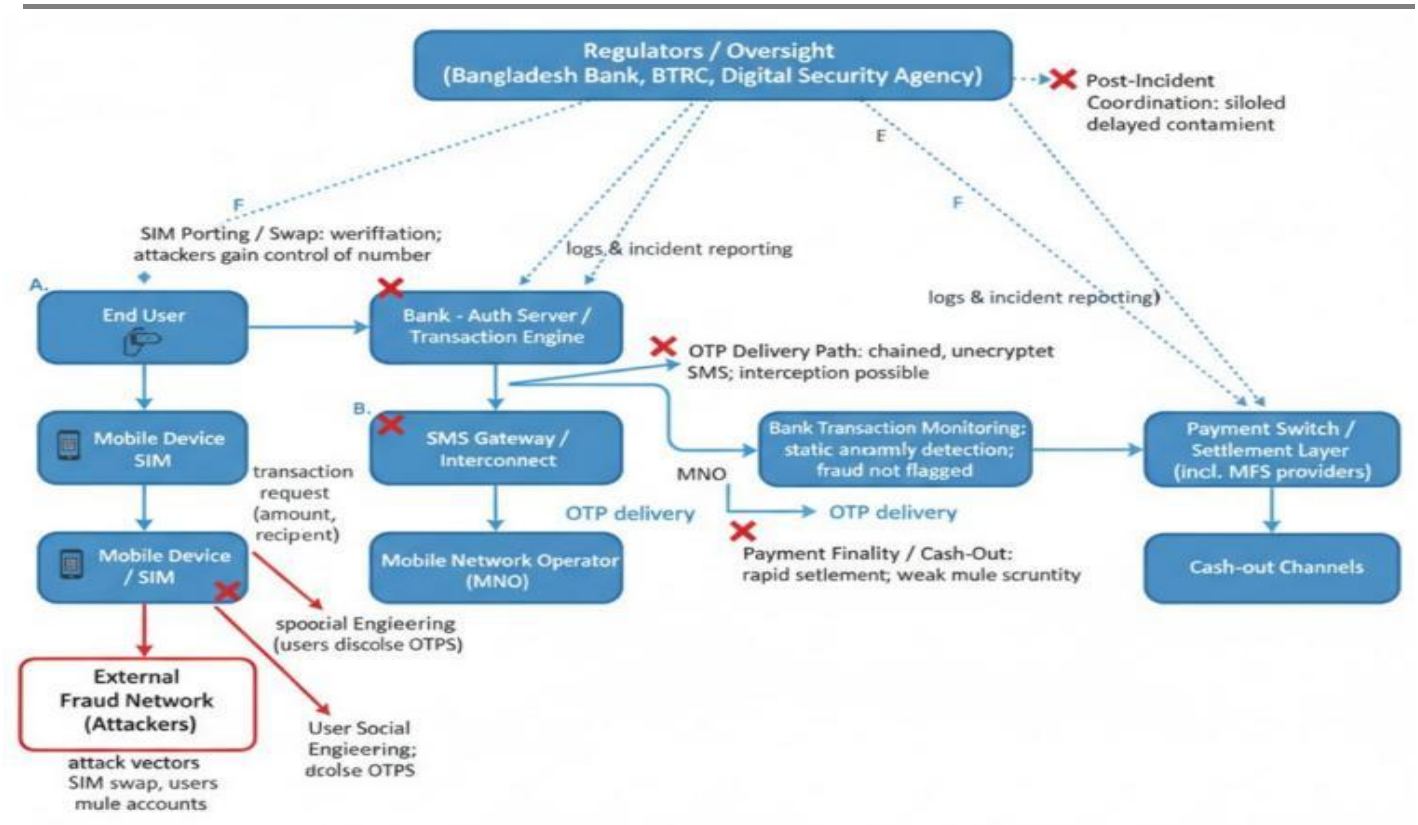


Figure 2. System map of Bangladesh's digital-finance transaction flow showing actors, core data paths and exploited weak points (red X) identified in the SCB 2025 OTP scam.

Bangladesh's regulatory architecture reinforces this diffusion of responsibility. The Bangladesh Bank oversees banks and MFS platforms; the BTRC monitors telecoms; CIRT handles cyber incidents; yet no body owns the intersections where fraud actually occurs. Reporting flows are fragmented, cross- institutional data sharing is minimal, and there is no unified mechanism for rapid joint response. The result is a governance vacuum: a system technically dense but institutionally porous. This framework extends existing cybersecurity governance models by emphasizing accountability as an emergent property of multi-actor interaction rather than isolated institutional duty.

This diffusion also shapes public discourse. Blame routinely shifts downward to users—often portrayed as careless for sharing OTPs—while the systemic design that allows criminals to impersonate officials or reroute messages goes unchallenged. Such framing externalizes risk, erodes digital-trust, and discourages the very adoption the financial-inclusion agenda depends on.

The lesson is structural: cybersecurity in financial ecosystems cannot be managed within organizational silos. Responsibility must extend across networks, covering not only what each actor controls but also how their systems interact. Until accountability becomes a shared architecture rather than an after-the-fact blame game, the vulnerabilities exposed by the SCB scam will persist—reproduced in new forms, across the same fault lines.

## Toward a Multi-Actor Accountability Framework

The findings from the SCB OTP scam demonstrate that cyber fraud in Bangladesh's digital-finance sector is not simply the result of technical lapses or user error but a manifestation of systemic disconnection between interdependent actors. Banks, MFS providers, telecom operators and regulators operate within overlapping but weakly coordinated domains, leaving critical gaps where accountability diffuses. To address this fragmentation, this study proposes a **Multi-Actor Accountability Framework (MAAF)** —a systemic model that redefines cyber security responsibility as a shared governance function rather than an isolated institutional task. The **MAAF** envisions a connected ecosystem in which information flow, oversight, and risk management are integrated across technical, institutional, and human levels.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

**Core Principles of the Framework**

The framework is grounded on four interlocking principles designed to promote resilience and transparency:

**Shared Accountability** — Every actor in the digital-finance chain carries both individual and collective responsibility for security outcomes. The framework rejects the prevalent culture of blame-shifting and instead emphasizes co-ownership of risks and responses.

**Data Interoperability and Transparency** — Cross-institutional information exchange must be standardized. Banks, MFS providers and telecoms should operate through interoperable platforms where fraud alerts, anomaly reports and risk signals circulate in real time under regulatory supervision.

**User - Centric Protection** — End-users represent the most vulnerable link in the ecosystem. The framework prioritizes user safety through default safeguards—secure transaction notifications, verified communication identifiers and digital-literacy initiatives—without assuming high technical literacy.

**Preventive Oversight** — Regulators must transition from reactive enforcement to proactive monitoring. Rather than responding post-incident, oversight bodies should deploy early-warning mechanisms, continuous risk audits, and coordinated incident- response protocols.

**Institutional Roles and Coordination**

Under the MAAF, distinct institutional roles are defined but integrated through continuous coordination:

- Banks and MFS Providers serve as the first line of detection and reporting. They maintain joint fraud-monitoring systems, shared anomaly-detection databases, and unified customer-notification standards.
- Telecom Operators provide the technical backbone for secure authentication, ensuring verified SMS routing and fraud-flagging protocols for suspicious SIM activities.
- Regulators—specifically the Bangladesh Bank, the BTRC, and the Digital Security Agency—form a Joint Cyber- Finance Task force, responsible for centralizing intelligence, coordinating inter-agency response, and enforcing compliance with shared cybersecurity standards.
- End-Users are incorporated as active stakeholders through structured awareness programs and secure reporting channels that enable direct communication with banks and regulators without bureaucratic delay.

This configuration ensures that information does not stagnate within institutional silos and that responsibilities are explicit, traceable, and enforceable.

**Implementation Pathways**

A phased implementation strategy is essential to translate the MAAF from principle to practice:

**Short-Term (0–1 year)**: Establish a unified reporting protocol for cyber fraud incidents, accessible to banks, MFS providers, and telecom operators. Launch an encrypted communication channel supervised by the Bangladesh Bank for real-time alert sharing.

**Mid-Term (1–3 years)**: Develop a National Digital-Finance Fraud Intelligence Platform (NDFFIP) integrating transaction risk data, SIM-swap alerts, and phishing trend analytics.

**Long-Term (3–5 years)**: Institutionalize cross-sector account- ability clauses in financial and telecommunication regulations. Conduct annual joint security audits and publish transparent national reports on cyber-fraud trends and response effectiveness.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

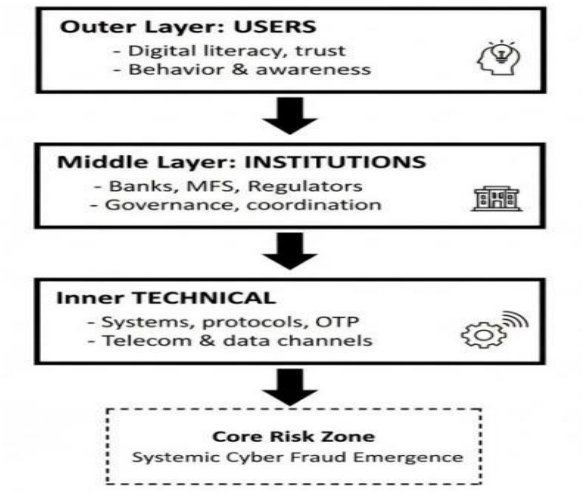


Figure 3. Conceptual schematic of the Multi-Actor Accountability Framework (MAAF), integrating technical, institutional and human responsibility layers.

## Expected Impact

The proposed Multi-Actor Accountability Framework fundamentally reorients the governance of digital-finance cybersecurity from isolated reaction to collective prevention. By clarifying roles, promoting data transparency, and embedding user protection into system design, the framework addresses the accountability vacuum that has long undermined resilience. Its implementation would likely produce faster incident containment, improved trust between stakeholders, and measurable public confidence in digital financial platforms. Ultimately, the MAAF offers a structured pathway toward a coordinated, responsibility sharing ecosystem capable of reducing systemic vulnerability in Bangladesh's digital financial services.

## Insights and Future Research

## Directions

Analysis across Bangladesh's digital-finance ecosystem reveals recurring patterns that go beyond isolated technical failures or user errors. Fraud frequently emerges at the intersections of multiple actors—banks, MFS providers, telecom operators, regulators, and end users—highlighting that vulnerabilities are systemic rather than incidental. Even tech-savvy users, including educated and elderly individuals, are susceptible to sophisticated social engineering, demonstrating that human behavior cannot be treated as uniformly predictable. Fragmented regulatory oversight further compounds this risk, delaying detection and response and leaving gaps that malicious actors exploit. Together, these patterns illustrate that cyber fraud arises from complex interactions within the ecosystem, rather than from any single point of failure.

The sector-wide implications are significant. Users of all demographics face exposure to fraud, challenging assumptions that only low-literacy or elderly populations are at risk. Financial institutions and telecom operators must recognize their operational inter dependencies and design processes with cross- sector vulnerabilities in mind. Regulators, similarly, must adopt a system-level perspective, prioritizing coordination and intelligence-sharing rather than reactive enforcement. Under- standing these patterns shifts the focus from managing individual incidents to anticipating systemic weaknesses and designing measures that enhance resilience across the ecosystem.

Despite growing awareness of these challenges, substantial research gaps remain. Quantitative modeling of fraud propagation could clarify how vulnerabilities interact across inter- dependent actors, while studies of human-technology interaction would help identify why even informed users are deceived. Empirical evaluation of cross-institutional coordination mechanisms and integrated fraud-detection systems would provide evidence for scalable, sector-wide interventions. Addressing these gaps is essential for developing practical strategies to safeguard users, institutions, and regulators alike, and for building a more resilient digital-finance ecosystem in Bangladesh.

## CONCLUSION

In conclusion, cyber fraud in Bangladesh is fundamentally a system-level problem that arises from the interplay of technical, institutional, and human factors. By recognizing patterns of vulnerability across the entire ecosystem, rather than focusing on individual cases, researchers, policymakers, and industry actors can develop strategies that strengthen resilience, improve trust, and support sustainable growth of digital financial services. Future research integrating behavioral, technical, and institutional perspectives will be critical to achieving these goals.

## REFERENCES

1. Sharif, J. B., Hasan, M., Kwosar, M., Ahmed, M. F., & Mandal, P. (2024). A short review of mo- bile financial services in Bangladesh. World Journal of Advanced Research and Reviews, 23(2), 2479–2485. https://doi.org/10.30574/wjarr.2024.23.2.2610
2. https://www.ti-bangladesh.org/images/2025/report/mfs/Executive- Summary-Mobile-Financial-Services-Sector-En.pdf?v=1.1
3. Rashid, M. M. (2025). The impact of mobile fi- nancial services in Bangladesh: Usage, benefits, and challenges. World Journal of Advanced Engi- neering Technology and Sciences, 16(2), 271–277. https://doi.org/10.30574/wjaets.2025.16.2.1290
4. "Cyber Fraud and Identity Theft in Bangladesh: A Rising Concern", IJEDR - INTERNATIONAL JOUR- NAL OF ENGINEERING DEVELOPMENT AND RESEARCH (www.IJEDR.org), ISSN:2321-9939, Vol.13, Issue 2, page no.193-210, April-2025, Available:https://rjwave.org/IJEDR/papers/IJEDR2502027.pdf
5. Islam, R., Ahmed, S., Rahman, M., & Al Asheq, A. (2020). Determinants of Service Quality and Its Effect on Customer Satisfaction and Loyalty: An Empirical Study of Private Banking Sector. The TQM Journal. https://doi.org/10.1108/TQM-05-2020-0119
6. Kaur, Jagpreet & Ramachandran, Ramkumar. (2021). The Recent Trends in CyberSecurity: A Review. Journal of King Saud University - Computer and Information Sci- ences. 34. 10.1016/j.jksuci.2021.01.018.
7. Aker, Jenny & Mbiti, Isaac. (2010). Mobile Phones and Economic Development in Africa. Journal of Economic Perspectives. 24. 207-32. 10.2139/ssrn.1629321.
8. Rahman, Khandaker & Jiow, Hee Jhee & Lee, Brenda. (2025). Preventing Crimes of Online Scams Across Countries: A Comparative Study Between Bangladesh and Singapore. Social Science Review. 42. 45-62. 10.3329/ssr.v42i1.85321.
9. Akinbowale, Oluwatoyin & Mashigo, Polly & Zeri- hun, Mulatu. (2024). Fraud investigation and mitigation. 10.4102/aosis.2024.BK485.02.
10. Modi, Seema & Premani, Vanshika & Kaur, Mandeep. (2021). A critical analysis of e-banking frauds and laws in India. International journal of health sciences. 931-938. 10.53730/ijhs.v5nS2.13925.
11. Brici, Iulia & Violeta, Achim. (2023). Does the Digitaliza- tion of Public Services Influence Economic and Financial Crime?. Studies in Business and Economics. 18. 67-85. 10.2478/sbe-2023-0025.
12. https://www.thedailystar.net/tech- startup/news/scammers-target-50-scb-credit-cards- steal-bdt-27-lakh-report-3992241
13. https://en.prothomalo.com/business/local/5oi7ncs555
14. Bangladesh Cyber Threat Landscape 2024, BGD e- GOV CIRT, https://www.cirt.gov.bd/documents/bd-cyber- landscape-2024