PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 15 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Data Encryption in Financial Transactions

Data Encryption has become an important technology of modern financial security for protecting sensitive information. This article provides an analysis of encryption technologies in financial transactions across payment systems. Recent searches tell that encryption has reduced the risks, but there are some difficulties that we will face in the future.

By **Muhammad Usman Haider** | Department of Computer Science | Published: August 2026
ittxusman091@gmail.com | Position: Software Engineer

Introduction

The rapid digitization of financial services has also fundamentally transformed, increasing security risks. Every day, trillions dollors transaction is done, also having sensitive information such as credential information, Identification and personal data. Simultaneously, cyberattacks are also increasing, targeting mobile banking to interbank settlements. From 2025 to 2030 stated that there will 56 USD billion-dollar breach. But emerging technologies such as zero-knowledge proofs **(ZKPs) ,** Multiparty computation **(MPC),** and Homomorphic encryption are enabling new privacy-preserving capabilities that were previously impossible.

Technology Overview

Financial Encryption Includes:

- For data in transit, TLS 1.2 or 1.3 is the universal standard that secures data between mobile applications, browsers, and servers.
- For data in rest, AES-256 (Advanced Encryption Standard with 256-bit keys) dominates as symmetric encryption.
- Symmetric encryption uses the same encryption for encryption and decryption.
- Asymmetric encryption uses a private-public key pair without sharing secrets.

- Advanced technologies such as Zero -Knowledge Proofs (ZKPS) , Multi-Party Computation (MPC) , and Homomorphic Encryption (HE), which were once considered impossible, are now being used.

Key Findings & Impact

Encryption stops data theft through tight security. If a hacker steals the data, but he cannot read it. Banks that follow encryption rules are more secure than other banks. The most important thing is key management, which is as important as encryption itself. Good key management results in good security and encryption. Technologies like Homomorphic Encryption are advanced tools that offer amazing privacy, but are much slower than basic encryption tools.

What's Next?

Quantum computers will be necessary within the next 5 to 10 years which will break today's encryption systems. A hybrid encryption system will be used in order to protect the data. Crypto-agility (the ability to swap encryption algorithms without shutting down) will become a basic requirement for all payment systems. Privacy tools like **HE** (homomorphic encryption) are still too slow, but progress will make them practical for fraud detection soon. AI-powered monitoring will watch for unusual data even when the data itself is encrypted.

About the Author

Muhammad Usman Hiader is a BSIT student interested in Data Encryption and Security. They can be reached at itxusman091@gmail.com.

Keywords: Artificial Intelligence; Cybersecurity; IoT; Software Engineering; Pakistan Tech

References

[1] Abadi, A., et al. (2025) – *Starlit: privacy-preserving federated learning to magnify financial fraud detection*. IEEE Conference on Federated Learning Technologies and Applications (FLTA). [Citation: 7]

[2] Elysium Research Group (2025) – *Practical Considerations for Post-Quantum Cryptographic Migration in Financial Systems*. Zenodo. [Citation: 10]

[3] G7 Cyber Expert Group (2026) – *Roadmap for the transition of the financial sector to post-quantum cryptography*. Banca d'Italia. [Citation: 6]