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

TECHNOLOGY FEATURE Industrial News

Encryption in Digital Payments and FinTech Security: Safeguarding the Future of Financial Transactions

Building Trust in an Information-Driven Money Economy. These days people are using money in a different way. We can pay bills, shop online send money to countries and even buy coffee with just a few clicks. This has made life easier and faster. It also means we have to deal with new threats to our money and personal info. The thing that keeps all our transactions safe is encryption technology. Without it bad people could easily steal our money and info. When we send money or make a payment online encryption makes sure that only the right people can see the details.

Muhammad Nawaz | Department of Computer Science | Published: August 2026
muhammadnawazghaffar@email.com | Position: Student

Introduction

Encryption technology converts information into encrypted code and only allows access to the information to those who are authorized to access it. This helps to keep communications between the customer and the bank private from unauthorized access, such as online transactions, customer identity, banking details and payment history. To safeguard payment infrastructures and uphold consumer trust in finance platforms the modern financial ecosystem needs to rely on various layers of encryption cybersecurity experts explained. Encryption is very important for the industry. Cybersecurity experts say that encryption is necessary to protect transactions. The financial industry needs encryption to keep customer information safe. Encryption is essential for the future of systems. Cybersecurity experts say that encryption will help to maintain customer trust, in payments. Encryption is like a lock that keeps our money and info safe. Trust is not something that is given it is built with encryption.

Paying for things is something we do every day, and digital payments are a part of that. FinTech or financial technology is changing the way we make payments from using our phones to contactless cards.. With more digital transactions there is also a higher risk of cyber attacks.

When we make a payment online, we must give out info like our credit card numbers and personal details. If this info gets into the hands, it can cause big problems. That's where encryption comes in. It's like a shield that keeps our info safe. Encryption is a way of changing our info into a code that only the right people can understand. It's like a box that keeps our money and info locked up tight.

Industrial analysis:

The financial technology industry is quickly developing its cybersecurity capabilities as digital payment systems expand around the world. There is investment in encryption technology for banks FinTech companies, payment gateways and cloud services to protect financial transactions from cybercrime, fraud and data breaches.

According to industry analysts the increase in banking, digital wallets, contactless payment and blockchain financial services has increased the need for advanced encryption systems. Financial service providers are making cybersecurity a top priority over requirements and a core business necessity.

> ***"Layers of encryption work behind the scenes to keep our transactions safe".***

Technology Overview

Encryption is the key to keeping our payments safe. There are a few ways to encrypt info:

- **Symmetric Encryption:** this is a way of encrypting and decrypting info using just one key. It's fast and good for making lots of transactions at the time.
- **Asymmetric Encryption:** this is also called public-key cryptography. It uses two keys. One public and one private. It's a way to keep info safe when sending it over the internet.
- **End-to-End Encryption (E2EE):** this means that only the person sending and the person receiving the info can see it. No one in between can access it.

- **Hashing:** this is a way of changing info into a code that can't be changed back. It's often used to keep passwords safe.
  - All these methods work together to create a defence system that keeps our digital payments safe.
  - Practical Applications in FinTech
  - Encryption is used in lots of ways in FinTech
- **Digital Wallets and Mobile Payment Apps**: these use encryption to keep our passwords and payment details safe.
  - Contactless and NFC-Based Transactions: this use encrypted signals to make sure our info is safe.
  - Blockchain and Cryptocurrencies: these use codes to keep transactions safe and transparent.
  - Payment Gateways and APIs: encryption keeps our info safe when we make payments online.
  - Cloud-Based Financial Services: encryption keeps our info safe when its stored and sent over the internet.

Figure 1: layers of encryption protecting digital payments and fintech transactions across multiple platforms. Source: industrial technology illustration

Key Findings & Impact

Since we started using encryption in FinTech our transactions have become much safer:

- We have defences against cyber attacks and financial crime.
- People are more confident in using payments.
- Our transactions are safer and more reliable.
- We are following rules to protect our info.
- We are less likely to have our info stolen or compromised.

One of the advancements in recent years is the use of encryption with smart monitoring systems. These systems can spot activity and stop fraud from happening.

■ Emerging Trends (2025–2026)

There are some exciting developments in FinTech security:

- **Quantum-Resistant Encryption**: this is a new way of encrypting info that will keep it safe from quantum computers.
- **AI-Driven Security Systems:** these use intelligence to make encryption stronger and more effective.
- **Zero-Trust Architecture:** this means that we don't trust anyone or anything and we verify everything all the time.
- **Tokenization & Data Masking**: this is a way of replacing info with tokens so it's safer.
- **Biometric Encryption:** this uses things like fingerprints and facial recognition to make encryption stronger.

■ Ethical Challenges and Data Security: Trust, Privacy and Protection in a Hyper Digital World

While encryption is great there are some challenges we need to think about:

- More cyber attacks on systems.
- It can be hard to manage encryption keys.
- We need to balance security with ease of use.
- We must be careful when using systems with new encryption.

- To stay safe financial organizations, need to:
  - Use encryption protocols.
  - Keep their cloud infrastructure safe.
  - Be transparent about how they use our info.
  - Monitor their systems all the time.

We need to find a balance between keeping people safe and innovating technologies.

What's Next?

In the future we will see smarter and more adaptable security systems. Some of the developments include:

- Real-time evolving AI encryption systems.
- Completely secure finance ecosystems.
- The use of Quantum Safe Cryptography around the world.
- Smart fraud prevention platforms.

Encryption will keep being a part of financial innovation as digital transactions become more common. Encryption is the hero that keeps our digital finance landscape safe. It protects our info helps prevent fraud and gives us confidence in our financial systems. As cyber threats get more sophisticated we will need encryption more.

The future of transactions depends on how well we can develop and use encryption technologies. The FinTech industry can create an more trustworthy digital economy by improving encryption and adopting new innovations.

We need to look at the role of encryption in payments and FinTech security and how it will help the future of monetary transactions. The subject of encryption in payments and FinTech security is very important. As cyber threats get worse the global financial industry is investing more in encryption technologies. The financial industry is making investments in encryption technology because it is urgent to protect against increasing cyber threats.

Cybersecurity experts say that the future of systems will depend on encryption environments that can adjust to cyber threats as they happen. If we do not update the cybersecurity infrastructure this can result in risks, fines and damage to the reputation of financial institutions.

With more people using payments in the world of commerce it is likely that encryption will continue to play a crucial role in maintaining financial stability, customer trust and secure online transactions. Cyber threats are a growing problem for the digital payments industry. This is a payments area that is increasingly targeted by cyber threats.

> ***"Trust is not taken for granted in the financial world it is built with encryption."***

About the Author
Muhammad Nawaz is a student at University of Agriculture Faisalabad of information technology. He can be reached at muhammadnawazghaffar@gmail.com.

Keywords: Fintech; Digital payments; cybersecurity; blockchain; AI security; data protection;

References

[1] World Bank – Digital Financial Services. Available at: https://www.worldbank.org/ext/en/development-topics
[2]PCI Security Standards Council (PCI SSC): The Standard, for Payment Security Standards Throughout the World. Available at: https://www.pcisecuritystandards.org/?
[2] European Commission – GDPR..Available at: https://commission.europa.eu/law/law-topic/data-protection_en?
[3] The National Institute of Standards and Technology (NIST) provides standards regarding cryptography. Available at: https://www.nist.gov/cryptography?
https://www.nist.gov/publications/zero-trust-architecture?
[5]IBM Security – Financial Services Cybersecurity. Available at: https://www.ibm.com/solutions/data-security
[6] Google Security – Encryption Practices. Available at: https://safety.google/?
[7] Microsoft Security – Cloud & FinTech Protection. Available at: https://www.ibm.com/solutions/ai-cybersecurity?