



Banking, financial services
and insurance (BFSI):
Digital transformation using
edge computing

BFSI's digital metamorphosis

The BFSI sector is revamping its digital landscape across the globe to enable more personalised and secured banking and financial services for customers. Faster cloud-adoption followed by the use of generative AI, machine learning (ML), autonomous systems, privacy enhancing computing and internet of things in the BFSI sector indicate that a digital transformation has begun. Gartner predicted that the BFSI's expenditure on IT will exceed USD 623 billion in 2023.¹ Furthermore, the spending on software by the BFSI sector will exhibit the largest growth with an increase of 13.5% in 2023.² IT spending by global enterprises is expected to see a five-year compound annual growth rate (CAGR) of 6.5%, to reach an estimated USD 761 billion by 2025.³ However, even though the BFSI sector is undergoing major transformation, there are some factors which are impeding this growth.



Challenges

1. Latency and network congestion

In the current scenario, vast amounts of data transfer to a centralised data centre over long distances creates latency issues and increases congestion in network traffic.⁴ Both increasing latency and network congestion have adverse effects on the successful application of generative AI for real-time fraud prevention and detection. Therefore, the BFSI sector needs to upgrade its existing infrastructure strategies.

Some real-life incidents of malicious attacks also indicate that the BFSI requires a technological breakthrough. In June 2022, one of the leading US banks experienced malicious attacks, resulting in the breaching of customers' personal information related to credit card applications. The bank had to pay out USD 190 million to the customers who were affected. Furthermore, the bank was charged a fine of USD 80 million.⁵

2. Increasing server downtime

In the current cloud computing systems, the successful deployment of ML models depends on the responses received from a centralised server located far away. In this case, issues like network failure during heavy data flow can increase server downtime substantially.

Eventually, this may result in a massive delay in receiving responses, which in turn will affect the use of ML models for advanced security features.

Moreover, many malicious entities or hackers have been trying to take advantage of such systems during the downtime. Nearly 60% of BFSI companies, with more than USD 5 billion in assets, experienced various types of cyberattacks in 2022.

3. Security and compliance issues

BFSIs use centralised systems to implement multilingual conversational AI chatbots and AI-driven autonomic system for real-time analysis of financial actions, suggesting personalised financial plans, insurance services, automated lending facilities, credit reports and autonomous debt management systems. However, during the data traveling, crucial customer data may be exposed to malicious attacks. Eventually, this raises questions on the security of the personal information collected by the BFSI sector using this centralised cloud computing system. Thus a centralised system is fuelling regulatory and compliance issues, and creating an atmosphere hostile to the application of an AI-driven autonomic system.

1 <https://www.gartner.com/en/newsroom/press-releases/2022-05-24-gartner-identifies-three-technology-trends-gaining-tr>

2 <https://economictimes.indiatimes.com/tech/information-tech/global-it-spending-on-banking-investment-services-to-reach-652-billion-in-2023-gartner/articleshow/101165430.cms>

3 <https://www.gartner.com/en/documents/4003505>

4 <https://www.gartner.com/en/documents/4006926>

5 <https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/#:~:text=In%20addition%20to%20paying%20out,enhance%20its%20cloud%20security%20standards.>

Cloud-readiness is not enough, BFSI should be edge-ready

Switching to edge computing can help the BFSI sector to eliminate all constraints in its digital transformation path and create business value. Unlike cloud computing, edge computing allows the transfer of computing workloads and storage of data closer to its origin. Thus, edge computing can assist the BFSI sector by providing a highly flexible distributed platform to implement emerging technologies and achieve the objectives behind digital metamorphosis, in order to provide more personalised and secured banking and financial services.

Edge-enabled use cases for proactive fraud detection

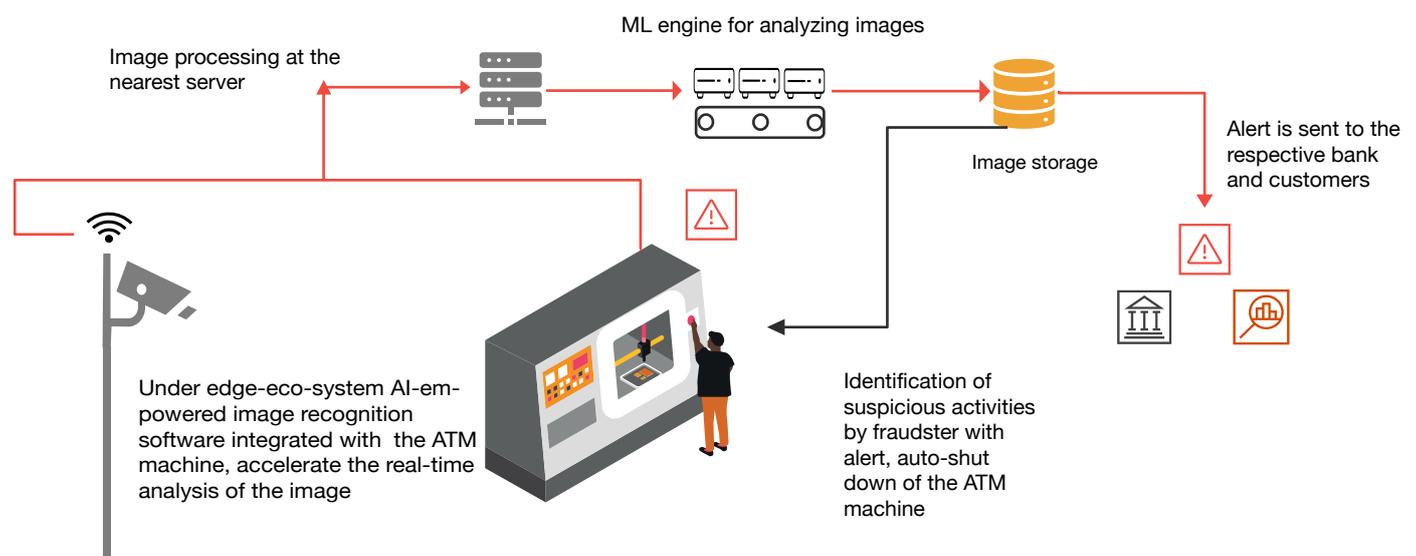
1. Automatic prevention and detection of suspicious activities by fraudsters

Edge computing enables the execution of ultra-low latency use cases of AI and ML for enhanced security features that can further be utilised to prevent money laundering activities. Under the edge ecosystem, AI-empowered image/video recognition software can accelerate the real-time analysis of the images and video feed. This will be helpful for stopping fraudsters trying to tamper with the items shown on the screens of ATMs with an instant shutdown of the machine (as shown in Figure 1).

As edge computing allows the data processing closer to the genesis of the data and eliminates the chances of unnecessary congestion, unplanned downtime and latency delays, the BFSI can apply advanced AI and ML models and perform instant recognition of fraudulent patterns. As a result, proactive measures can be taken to stop fraudulent transactions before their occurrence and enhance the scope for regulatory compliance.

Figure 1: Automatic prevention and detection of suspicious activities by fraudsters in ATMs

Edge-readiness for automatic and prevention of suspicious activities by fraudsters in ATMs



2. Auto-detection of concealed weapons and robbery prevention

An edge computing infrastructure will enable deep learning algorithms like convolutional neural networks (CNNs) to develop a real-time, one-stage model to detect hidden objects. It is already evident that edge infrastructure offers fastest processing of large datasets at the nearest data centre. Thus, in the edge environment, deep learning models are able to perform accurate and real-time processing of large datasets (images and videos) collected via CCTVs of banks, ATMs and other institutions.

Edge-enabled proactive detection of weapons concealed under the clothes of miscreants will be useful for preventing robberies in advance. Automatic detection of weapons will trigger proactive alerts to the security department of the respective financial institution, and instant measures for robbery prevention can be adopted. Thus, edge-enabled banks, ATMs or other financial institutions may not require human intervention to analyse and eliminate the chances of potential fraud and maintain security compliance more effectively.

3. Eliminate regulatory and compliance issues while offering hyper-personalisation

In the edge computing infrastructure, a system does not need to send confidential data to a remote data centre – rather, derivation of analytics from customers' confidential data can occur locally. A real-life example of edge-induced hyper-personalisation with end-to-end security is the application of semi-humanoid robot by a leading banking institution of Hong Kong and Shanghai (Figure 2). These institutions have deployed edge-enabled robots which implement natural language processing for interpreting and complying with the requests made by customers. Edge-empowered robots are able to perceive basic human emotions and adjust their behaviour accordingly. As a result, when a prospective customer indulges in remote banking activities, these robots will analyse their inputs, chat and other personal history, and conduct segmentation and offer customised car loans, home loans and savings plan instantly.



Such technologies can prove useful in assisting the BFSI sector to analyse corporate documentation and chat logs with bank representatives for individual customers. Edge-enabled applications will help the sector to gain a thorough understanding of its customers, depending on which, BFSI institutions can offer facilities like autonomous debt management and automated lending to their customers. With such hyper-personalised and secured services, BFSIs can boost their user experience as well as customer satisfaction rate significantly.

How PwC's Technology Consulting can help

As one of the pioneers in providing consulting services for edge computing, PwC is extending its services to make the BFSI sector edge-ready. The objective of these services is to de-risk BFSI's edge transformation. Some exclusive offerings by PwC will include:

- edge-readiness assessment
- edge-native application development
- outcome-focused and fit-for-purpose solutions for businesses.

In a nutshell, the experts at PwC have adopted a business-first approach to understand the specific requirement of the organisations operating in the BFSI sector, while deriving edge adoption strategies. The adept management and technical teams at PwC can conduct simulations and trace out the probable risks that banking and other financial institutions may face while adopting edge computing technologies. Thus, PwC encourages collaboration of technical and management services to help the BFSI sector with optimum spending for edge implementation.

Conclusion

As discussed, we can safely proclaim that edge-readiness will prove to be instrumental in driving the BFSI sector's digital metamorphosis, with the inclusion of advanced features like lower latency, larger bandwidth, improved security and better computing capacity. This will be a forward-looking strategy for BFSI, which will look beyond common challenges and achieve automation in fraud detection, along with facilitating hyper-personalisation and an enhanced customer experience. From a technological perspective, the sector needs to focus on developing its infrastructure – i.e. a network architecture compatible with a distributed computing system that enables seamless IT/OT integration to become edge-ready. This should be followed by outcome-focused investment planning, capable of generating the maximum returns on investment.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2023 PwC. All rights reserved.

Contact us

Ashootosh Chand

Partner, Emerging Technologies
PwC India
ashootosh.chand@pwc.com

Abhishek Verma

Associate Director, Emerging Technologies
PwC India
abhishek.verma@pwc.com

Contributors

Abhishek Verma

Suchandra Bose

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2023 PricewaterhouseCoopers Private Limited. All rights reserved.

SG/October 2023 - M&C 32528