International Journal of Future Engineering Innovations

Internet of Things in Banking

Matthew NO Sadiku [1*], David Padi [2], Janet O Sadiku [3]
[1] Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, Texas 77446, USA
[2] Aluminums Graduate School of International Business and Leadership, Midwest University, Wentzville, Missouri, USA
[3] Juliana King University, Houston, Texas, USA

* Corresponding Author: **Matthew NO Sadiku**

Article Info

ISSN (online): 3049-1215
Impact Factor (RSIF): 8.25
Volume: 03
Issue: 05
Received: 26-06-2026
Accepted: 28-07-2026
Published: 30-08-2026
Page No: 43-51

Abstract
The Internet of Things (IoT) is defined as a network of physical objects equipped with sensors, software, communications technology, and data-processing capabilities. Within the banking sector, IoT expands digital financial services beyond traditional websites and mobile applications by integrating payment instruments, wearable devices, vehicles, industrial equipment, bank branches, automated teller machines, and other physical assets. The importance of IoT in banking is demonstrated by its capacity to link financial decisions with real-world events. Strategic partnerships between financial institutions and technology providers are essential for IoT adoption and for shaping the future of banking. This paper presents a comprehensive analysis of the growing role of the Internet of Things in the banking industry.

DOI: https://doi.org/10.54660/IJFEI.2026.3.5.43-51

Keywords: Internet of things, IoT, industrial Internet of things, IIoT, banking, banker, banking industry

1. Introduction

The banking industry has always relied heavily on information. Banks gather and analyze data related to customers, transactions, assets, businesses, and markets to facilitate money movement, provide credit, and manage risk. The Internet of Things (IoT) enhances this information landscape by connecting physical objects to digital networks. The National Institute of Standards and Technology defines IoT as a network of devices equipped with hardware, software, firmware, sensors, and actuators that enables these devices to connect, interact, and exchange information. In banking, these devices can include smartwatches, payment rings, connected vehicles, industrial machinery, biometric sensors, automated teller machines, security systems, and smart home devices. IoT has the potential to make banking more immediate, personalized, and closely aligned with real economic activities. It can facilitate convenient payment options, improve fraud detection, reduce operational costs, and provide lenders with timely information regarding financed assets [1].

The Internet of Things (IoT) plays a crucial role in optimizing processes and facilitating real-time data analysis within the financial services sector. It has significantly transformed banking and finance, enhancing operational efficiency and revolutionizing customer experiences. This evolution has enabled the Banking, Financial Services, and Insurance (BFSI) industry to adopt IoT-enabled devices and networks, thereby reshaping traditional banking practices. As a result, the banking sector is evolving into a "smart banking" model, providing customers with more personalized, efficient, and secure services [2].

2. Methodology

The study employs a descriptive qualitative design to examine Internet of Things (IoT) technologies in the banking sector. Based on a literature review of scholarly journals, official reports, and industry publications, the paper explores IoT characteristics, adoption, applications, benefits, and challenges. This approach provides insight into the organizational, technological, security, financial, privacy, and regulatory factors influencing IoT implementation.

3. Overview of Internet of Things

The concept of the Internet of Things (IoT) has existed since the late 1990s but gained significant momentum in the 2000s due to the rise of Internet-connected devices. The Internet itself began with military computers in the Pentagon, known as ARPANET, in 1969. It expanded throughout the 1980s as a collection of four parallel military networks, each operating at different security levels. The evolution of IoT is illustrated in Figure 1 [3].

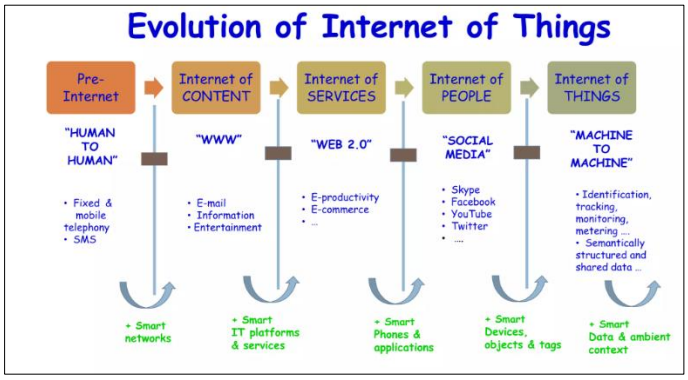

Fig 1: The evolution of IoT [3].

The core technology that gives the Internet its defining characteristics is Transmission Control Protocol/Internet Protocol (TCP/IP), a set of communication rules [4]. The Internet of Things (IoT) is a global network that connects devices to the Internet and to each other using wireless technology. These devices are equipped with hardware such as sensors and electronics, enabling them to interact with other objects and be monitored and controlled remotely. The goal is for physical devices equipped with sensors or data-collection capabilities to share information with websites. This data can then be analyzed either in real time or later to create efficiencies. IoT is expanding rapidly, and it has been estimated that by 2020, there would be approximately 50 billion devices connected to the Internet. These devices include smartphones, tablets, desktop computers, autonomous vehicles, refrigerators, toasters, thermostats, cameras, alarm systems, home appliances, insulin pumps, industrial machines, intelligent wheelchairs, wireless sensors, and mobile robots, among others. Figure 2 illustrates the Internet of Things [5], while Figure 3 shows its various applications [6].

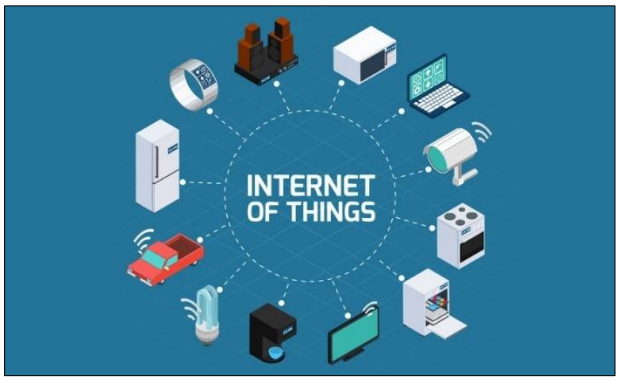

Fig 2: The Internet of things [5].

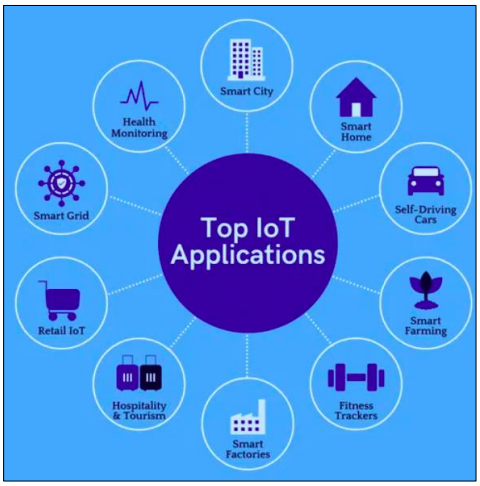

Fig 3: Applications of IoT [6].

There are four main technologies that enable the Internet of Things (IoT)[7]: 1. Radio-frequency identification (RFID) and near-field communication technologies. 2. Optical tags and quick response (QR) codes: These are used for low-cost tagging. 3. Bluetooth Low Energy (BLE). 4. Wireless sensor networks: These networks are typically used to monitor physical properties in specific environments. Communication technologies in the Internet of Things are illustrated in Figure 4 [8].

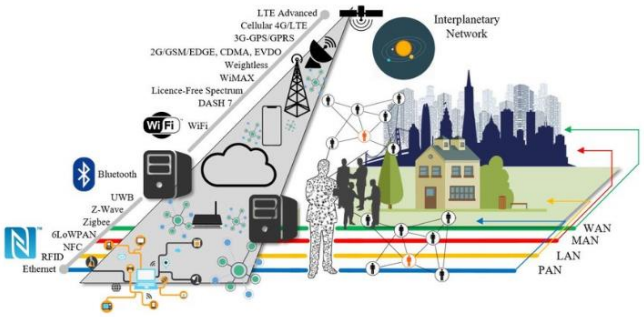

Fig 4: Communications technologies in Internet of things [8].

IoT technology facilitates interaction between people and objects. It is utilized in various fields, including smart transportation, smart cities, smart energy, emergency services, healthcare, data security, industrial control, logistics, retail, structural health monitoring, traffic management, manufacturing, and waste management. The Internet of Things has seen extensive development worldwide, with a strong focus on civilian applications such as electric power distribution, intelligent transportation systems, healthcare, industrial control, precision agriculture, and environmental monitoring. The growth of the Internet of Things (IoT) is significantly impacting both homes and industries. While IoT affects areas such as transportation, healthcare, and smart homes, the Industrial Internet of Things (IIoT) specifically pertains to industrial environments. IIoT represents a new industrial ecosystem that integrates intelligent and autonomous machines, advanced predictive analytics, and machine-human collaboration to enhance productivity, efficiency, and reliability. This advancement is leading us toward a world where smart, connected embedded systems and products operate as part of larger systems [9]. The Industrial Internet of Things (IIoT) refers to the application of IoT technology across various industries such as manufacturing, logistics, oil and gas, transportation, energy/utilities, chemicals, aviation, and other industrial sectors. A typical industrial Internet of Things system is depicted in Figure 5 [10].

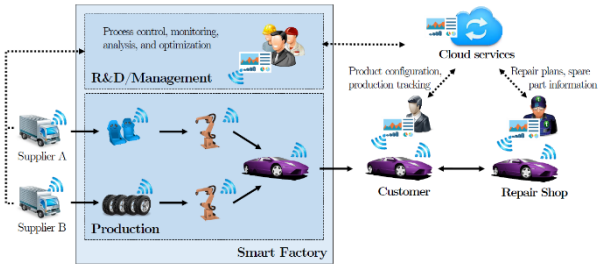

Fig 5: A typical industrial Internet of things [10].

4. Internet of Things Banking

The Internet of Things (IoT) refers to physical objects such as sensors, cameras, payment terminals, vehicles, wearable technologies, and automated machines that connect to digital networks and exchange data. In the banking sector, IoT extends digital services beyond computers and smartphones by enabling financial institutions to collect data from connected devices and respond to events in real time. IoT also increases banks' technological and ethical responsibilities. Consequently, banks must strike a balance among innovation, strong security, transparent data practices, regulatory compliance, operational resilience, and inclusive service design. By meeting these requirements, IoT can help create a banking system that is not only more automated but also more responsive, reliable, and better aligned with the actual needs of customers and businesses. When implemented responsibly, IoT has the potential to enhance customer service, improve security, reduce operational costs, support better lending decisions, and enable the creation of innovative financial products. [11].

IoT in banking is experiencing significant growth. The market is moderately concentrated, dominated by a few large players along with several niche companies. IoT devices, such as wearables and smart home appliances, are increasingly being integrated into financial transactions, paving the way for new opportunities in personalized and contextualized services. Currently, North America and Europe lead the market due to their early adoption of digital technologies and stringent regulatory frameworks. Regulations such as GDPR and PSD2 have a substantial impact on the market by establishing data privacy and security standards. While traditional banking systems and other digital financial services serve as product substitutes, IoT's unique capabilities are increasingly setting it apart.

5. Applications of Internet of Things in Banking

The applications of IoT include contactless and machine-to-machine payments, personalized notifications, biometric authentication, fraud detection, smart branches, predictive ATM maintenance, collateral monitoring, and embedded finance. These capabilities can improve efficiency, convenience, security, and access to timely financial information. Figure 6 shows some IoT use cases in banking and finance [2]. Common applications of IoT in banking include the following [1, 2]:

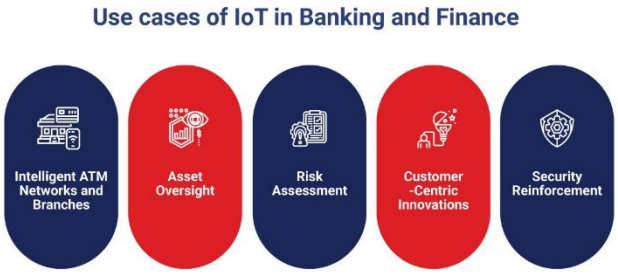

Fig 6: Some use cases of IoT in banking and finance [2].

Connected payments are among the most visible applications of IoT, including connected and contactless payment technologies. A smartwatch or payment ring can be linked to a bank account and used for contactless purchases. Connected vehicles can initiate payment for fuel, charging, parking, or tolls, while smart appliances may eventually purchase approved supplies automatically. Such arrangements reduce the distance between a customer's need and the resulting transaction. They also change the nature of payment security because credentials are distributed across numerous devices rather than confined to a card or banking application. Connected assets can improve secured lending and leasing. Figure 7 shows an example of wearable device payment [11].

Fig 7: A wearable device payment [11].

Fraud detection and customer authentication are other significant areas of application. Banks already consider transaction amounts, merchants, locations, and device information when assessing risk. IoT introduces additional context. A payment initiated by a recognized wearable in a location consistent with the customer's activity may appear less suspicious than a transaction from an unknown endpoint. Biometric and behavioral sensors may further support identification.

Internet of Things Banking shows that IoT systems are equally valuable in managing smart branches, ATMs, and banking infrastructure. Security cameras, electronic locks, check scanners, printers, digital signs, and other connected devices form part of this environment. Sensors can monitor temperature, power consumption, customer traffic, door access, cash levels, and equipment condition.

For example, mobile banking brought financial services onto a device that customers deliberately use. IoT will take the next step by integrating financial functions into objects and environments that people use for other purposes. Connected wearables, vehicles, appliances, and industrial equipment can already support contextual and contactless payments. However, location, movement, household routines, voice, health-related signals, and purchasing behavior could allow a bank to conclude a person's employment, habits, relationships, or vulnerability. In internet banking, digital banking has transformed how we move money, so seamlessly that even a few minutes of downtime can disrupt billions of transactions and erode customer trust. Internet banking, also known as e-banking or online banking, is the process of conducting financial transactions through digital channels rather than traditional offline channels. It also allows individuals and businesses to initiate fund transfers, check balances, pay bills, and even apply for loans. All of this happens instantly, on your mobile or laptop. The evolution of Internet banking has been one of relentless innovation and convenience. The core idea that the era of digital banking offers is accessibility: anytime, anywhere banking, enabled through secure online platforms. With growing Internet penetration, customers could now check balances, make payments, and transfer funds online. Figure 8 shows some benefits of Internet banking [13].

Fig 8: Some benefits of Internet banking [13].

The Automated Teller Machine (ATM), introduced in the 1960s, was a significant milestone in banking automation, pre-dating the formal concept of the Internet of Things (IoT). ATMs do not technically fall under the IoT, since they do not collect and analyze massive amounts of data; still, they laid the groundwork for the interconnected, automated systems that characterize today's IoT applications in banking and beyond. Modern ATMs extend far beyond cash withdrawals and balance checks. They now offer bill payments, mobile phone top-ups, fund transfers, depositing checks and cash without envelopes, printing or emailing detailed transaction receipts, changing PINs, accessing financial products like loans and insurance, and much more. The banks can analyze how customers use ATMs in various areas and adjust the number of ATMs installed there based on usage volumes. Figure 11 shows an ATM [11].

Furthermore, with Embedded Banking, IoT can enable automated, embedded banking. In embedded banking, financial services operate within non-banking products or activities. A connected car, home, factory, or retail system can interact with a bank through secure interfaces. With prior authorization, a device might pay for a service, transfer funds to a savings account when a defined event occurs, or activate short-term financing when inventory reaches a specified level. Such event-driven services can make banking more convenient and can create new products for households and businesses.

Risk management was introduced, and IoT also changes how banks assess risk. IoT-generated data may also improve credit assessment and risk management. Traditional lending decisions often depend on historical financial statements, credit scores, and information supplied periodically by borrowers. Connected equipment can provide more current evidence about the use or condition of an asset. When used with proper consent, effective governance, and human judgment, these data can help banks price risk more accurately, monitor collateral, and offer financing to customers whose circumstances are not fully represented by conventional credit records.

Data Analytics is a key benefit of IoT in banking: the ability to generate valuable insights from data collected across various touchpoints. The wealth of data generated by IoT presents a goldmine of information on customer behavior and preferences. By utilizing this data, banks can precisely tailor their services, develop robust marketing strategies, and introduce innovative financial products that resonate with customer needs. Business intelligence in banking helps convert this data into actionable insights to make informed decisions and meet evolving end-user demands.

6. Benefits and Challenges

When it comes to banking, IoT offers many benefits. The central benefit of IoT is its ability to connect financial decisions with real-time physical conditions. IoT can improve customer experience by reducing waiting times, simplifying authentication, and delivering services through familiar devices. For customers, the principal gains are convenience, speed, and services that respond more closely to individual circumstances. Other benefits of IoT in banking include the following [1,2]:

Automation in IoT-powered systems excels at executing specific operations, from handling requests to opening new bank accounts and even deactivating credit cards. This level of automation drastically reduces the dependence on manual intervention and the occurrence of human errors. It will ultimately help streamline complicated processes in the banking and finance industry.

One of the most valuable features of IoT is its ability to support real-time decision-making. By collecting and analyzing data in real time, IoT systems help to respond more quickly, improve operational efficiency, and make more informed decisions.

Conventional banking systems often depend on data received after an event has occurred. IoT devices can generate continuous streams of information, enabling banks to recognize changes quickly and automate routine responses. A branch manager can be alerted to unusual congestion, a security team can respond immediately to suspicious ATM activity, and an operations center can identify equipment problems before they affect many customers. Additionally, one of the most important benefits of IoT in banking is an improved customer experience. Connected devices can make financial services more convenient, responsive, and personalized. A customer may use a smartwatch to receive balance alerts, approve payment, or find a nearby branch. Inside a branch, connected systems can measure waiting times and direct customers to the appropriate service point. With informed consent, banks may also combine device-generated information with account data to provide timely reminders or relevant financial guidance. IoT can help transform banking from a service that customers must actively seek out to one that responds to their needs at the right moments. Another advantage is greater operational efficiency. Banks manage large networks of ATMs, security systems, servers, climate-control equipment, and other physical assets. IoT sensors can continuously monitor the condition and performance of these assets. Instead of waiting for an ATM to stop working, for example, a bank can receive an alert indicating that cash is running low, a component is

overheating, or maintenance is likely needed.

Furthermore, predictive maintenance can reduce service interruptions, prevent unnecessary inspections, and extend the useful life of equipment. Smart energy systems can also regulate lighting, heating, and cooling in branches based on actual occupancy, thereby reducing waste and expenses. By converting physical conditions into timely digital information, IoT enables managers to allocate staff, maintenance, and other resources more effectively.

Financial Inclusion in IoT may contribute to financial inclusion. People and small businesses without extensive credit histories are often difficult to assess through conventional scoring methods. With appropriate consent and validation, operational or asset data may offer additional evidence of income-generating activity and repayment capacity. Yet more data do not automatically produce fairer decisions. The success of IoT-based inclusion should therefore be judged by whether it expands access on fair and understandable terms, not merely by whether it increases the quantity of data available to lenders. Other benefits include personalization. Personalization is another potential benefit. A bank might warn a customer about an unusual transaction from a connected device, offer timely equipment finance to a business, or suggest a relevant service when an asset requires replacement. Responsible personalization can make banking more useful. Irresponsible personalization can become manipulation or unwanted surveillance. The difference depends on transparent purposes, genuine customer choice, proportionate collection, and a clear connection between the data used and the service provided.

Figure 9 shows some benefits of IoT in banking [2].

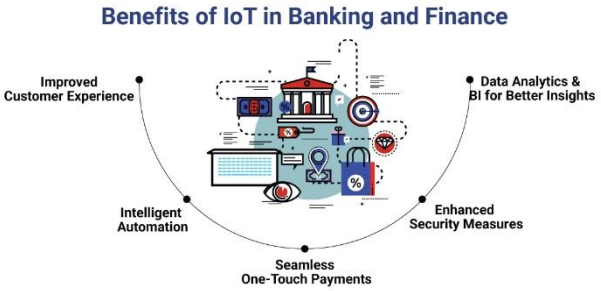

Fig 9: Some benefits of IoT in banking [2].

7. Challenges

Despite its promise, IoT poses serious cybersecurity and operational risks. Other barriers include privacy, interoperability, resilience, compliance, governance, inclusion, cost of implementation, incompatible technical standards, unreliable connectivity, third-party dependence, regulatory uncertainty, and shortages of specialized staff. Because banking depends on trust, financial institutions must balance innovation with robust security, privacy, transparency, and accountability. Other challenges of IoT in banking include the following [1]:

Regardless, the benefit-cost is a significant factor. The initial investment and ongoing maintenance cost of IoT technology can be significant. This includes the costs of hardware, software, integration, and the maintenance of continuous security and compliance. For smaller banks, the cost of deploying an IoT infrastructure may be prohibitive, limiting their ability to adopt IoT solutions.

Privacy presents an equally significant challenge. IoT data can reveal where people travel, what they purchase, when they are at home, how they behave, and which assets they use. When these data are combined with account records, they can create a detailed portrait of an individual's life. The Office of the Privacy Commissioner of Canada advises organizations in IoT ecosystems to define legitimate purposes, obtain meaningful consent, limit data collection and retention, maintain data accuracy, provide transparency, and protect data according to its sensitivity. Privacy, fairness, and security requirements should be incorporated into product design, procurement, contracts, and data architecture rather than added after deployment. Customers should receive concise explanations of the data being collected, the reason for collection, the retention period, the parties receiving the data, and the consequences of refusing or withdrawing consent.

Cybersecurity is a major concern. The most immediate risk is cybersecurity. Every connected device may become a point of attack. Weak passwords, insecure communications, outdated firmware, poorly protected interfaces, and unsupported products can expose data or interrupt services. A compromised payment device may facilitate fraud, while a vulnerable ATM, camera, or building sensor may provide a route into a wider network. Security must extend beyond the bank's internal network. The European Union Agency for Cybersecurity treats IoT security as a whole-life-cycle and supply-chain responsibility, covering requirements, design, delivery, operation, maintenance, and disposal.

Consequences of IoT adoption may widen the digital divide. Connected banking presumes access to compatible devices, reliable communications networks, technical skills, and confidence in digital services. Customers who cannot afford connected products, live in poorly served areas, have disabilities, or prefer traditional channels should not be excluded from essential services. Banks must retain accessible alternatives and avoid making invasive monitoring a condition for basic products on reasonable terms.

Governance: The principal challenge of IoT in banking is not connectivity itself, but the secure and accountable governance of a large, distributed, and constantly changing technological ecosystem. Effective governance requires clear ownership. Banks need to know who approves devices, who maintains inventories, who patches firmware, who monitors anomalies, who evaluates data use, and who is accountable when a vendor stops supporting a product. These tasks demand cooperation among cybersecurity, technology, risk, compliance, legal, procurement, operations, and business teams.

Internet of Things Banking trust is especially important

because banking depends on customers' belief that institutions will safeguard both money and confidential information. An IoT-related breach may cause harm even when no funds are stolen. The exposure of location histories, routines, or behavioral profiles can create risks of stalking, discrimination, manipulation, and identity theft. Excessive monitoring can also make personalization appear intrusive rather than helpful. Interoperability presents another significant obstacle. IoT is not a single technology but a collection of devices, networks, platforms, protocols, applications, and data models. A bank may acquire equipment from many vendors while continuing to operate decades-old core systems. Connecting these environments requires interfaces, gateways, and middleware, each of which increases technical complexity and creates additional points of failure. Poor interoperability also weakens security and oversight. If devices report status in inconsistent formats, a bank may struggle to maintain an accurate asset inventory or identify abnormal behavior across its network. Further, operational resilience is another key factor. The Federal Reserve defines operational resilience as the ability to deliver critical operations and core business lines through disruption and emphasizes preparation, adaptation, endurance, and recovery. It also notes that technology-led transformation, increasingly sophisticated cyber threats, and reliance on third parties expose financial institutions to operational risks. This principle has direct implications for IoT. Resilience cannot be achieved by protecting central data centers while ignoring thousands of connected endpoints.

Another important area is regulatory compliance: IoT complicates regulatory compliance because it crosses boundaries that traditional banking controls often treat separately. A single service may involve payment regulation, cybersecurity rules, banking secrecy, consumer protection, outsourcing requirements, data-retention obligations, breach notification, and restrictions on cross-border data transfers. Determining which rules apply can be difficult when data move automatically between a device, a mobile phone, an edge gateway, a vendor platform, and a bank. Regulators may also expect evidence that controls operate effectively, yet proprietary devices can offer limited logging or auditability.

Research shows that many banks operate on legacy systems that are not initially designed to interface with IoT technologies. Integrating IoT solutions can be a complex and costly process, involving substantial changes to existing IT infrastructure. A notable example is the challenge older banks face in incorporating mobile banking solutions, which can be seen as a precursor to more complex IoT integrations. Figure 10 shows some challenges and risks of IoT in banking [14].

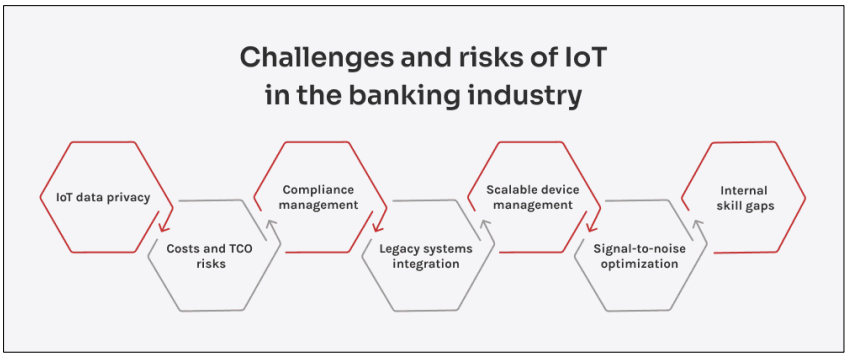

Fig 10: Some challenges and risks of IoT in banking [14].

8. Future of Internet of Things in Banking

The future of IoT in banking will probably involve deeper integration between financial institutions and connected environments. Payments may become increasingly invisible, occurring automatically after a verified event. Successful adoption will depend less on the number of connected devices than on the quality of governance surrounding them. The most valuable IoT projects will be those that solve genuine customer or operational problems rather than adopting technology merely because it is available.

The future of IoT in banking will therefore involve a transition from banking as a destination to banking as an embedded capability. Financial services will increasingly operate within homes, vehicles, factories, farms, shops, and supply chains. This shift offers major opportunities for convenience, inclusion, risk management, and efficiency. The banks that benefit most will not necessarily be those that collect the greatest volume of sensor data, but those that use limited, relevant data responsibly and turn it into trustworthy services. The future regulatory model will probably combine financial supervision, cybersecurity standards, privacy law, consumer protection, and rules for artificial intelligence. Banks will need to demonstrate not only that a connected service works, but also that its data is accurate, its automated actions are authorized, its vendors are accountable, its models are fair, and its essential functions can continue during disruption.

9. Conclusions

The Internet of Things is transforming banking by connecting financial services with physical devices, locations, assets, and real-world events. The integration of IoT into banking is not just a glimpse into the future; it is a vivid portrayal of the present, where efficiency, security, and personalized customer service converge. IoT in banking can reshape banking by linking financial services to the physical world. It has the potential to make banking more immediate, personalized, and closely aligned with events in the physical economy.

Connected payments can make transactions more convenient; intelligent ATMs and branches can improve efficiency; sensor data can strengthen asset finance and underwriting; and real-time context can support fraud prevention and personalized service. Above all, responsibility must remain with the bank even when technology is supplied by others.

IoT will strengthen banking only when institutions treat connected devices not as convenient accessories, but as integral components of critical financial infrastructure. The

strongest institutions will use security and privacy by design, collect only what they need, maintain customer choice, test operational resilience, and hold technology partners to clear standards. If these conditions are met, IoT can make banking more accessible and responsive. If they are ignored, convenience may be purchased at the cost of autonomy, fairness, and trust. More information about the Internet of Things in banking can be found in the books in [15-17] and the following related journal: *IEEE Internet of Things Journal.* [15-17] and the following related journal: *IEEE Internet of Things Journal.*

Fig 11: A representation of IoT in banking [11].

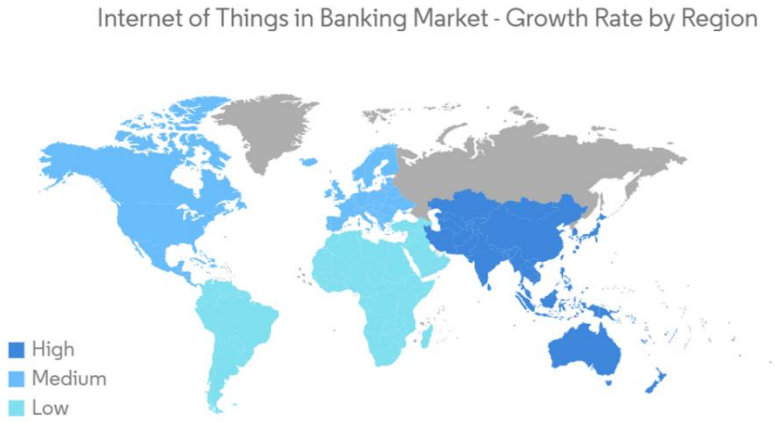

Fig 12: The regional market growth rate [12].

Fig 13: An Automated Teller Machine (ATM) [11].

References

1. Manus AI. Manus: hands on AI [Internet]. 2026 [cited 2026 Sep 7]. Available from: Manus AI
2. Rishabh Software. IoT in banking and finance: benefits, use cases and real-world examples [Internet]. 2024 Jan [cited 2026 Sep 7]. Available from: Rishabh Software – IoT in Banking and Finance
3. Yawson RM, Woldeab D, Osafo E. Human resource development and the Internet of Things. In: Proceedings of the 25th Annual Academy of Human Resource Development International Research Conference in the Americas; 2018 Feb 14-17; Richmond, VA, USA. doi:10.31124/advance.9638417.v1.
4. Townes M. The spread of TCP/IP: how the Internet became the Internet. Millennium: J Int Stud. 2012;41(1):43-64.
5. Alam AZ. Analysis of Internet of Things in DHL logistics (smart warehouses) [Internet]. LinkedIn; 2020 May [cited 2026 Sep 7]. Available from: Analysis of Internet of Things in DHL Logistics (Smart Warehouses)
6. Gaurav H. IoT (Internet of Things): everything you need to know [Internet]. STL Tech; 2022 Jul 28 [cited 2026 Sep 7]. Available from: STL Tech – IoT (Internet of Things)
7. Sadiku MNO, Musa SM, Nelatury SR. Internet of Things: an introduction. Int J Eng Res Adv Technol. 2016;2(3):39-43.
8. Sadeghi P, *et al*. Towards a reliable modulation and encoding scheme for Internet of Things communications. In: Proceedings of the 13th IEEE International Conference on Application of Information and Communication Technologies (AICT); 2019 Oct. Available from: ResearchGate.
9. Sadiku MNO, Wang Y, Cui S, Musa SM. Industrial Internet of Things. Int J Adv Sci Res Eng. 2017;3(11):1-4.
10. Sadeghi AR, Wachsmann C, Waidner M. Security and privacy challenges in industrial Internet of Things. In: Proceedings of the 52nd Annual Design Automation Conference; 2015 Jun.
11. Shamrei Y. Overview: IoT in banking—existing and future use cases [Internet]. SumatoSoft; 2024 Mar 14 [cited 2026 Sep 7]. Available from: SumatoSoft – Overview: IoT in Banking
12. Mordor Intelligence. Internet of Things in banking market size & share analysis—growth trends and forecast (2026-2031) [Internet]. 2026 [cited 2026 Sep 7]. Available from: Mordor Intelligence – Internet of Things in Banking Market
13. Saxena V. Evolution of Internet banking: from ATMs to NetBanking 2.0 [Internet]. Decentro; 2025 Oct 14 [cited 2026 Sep 7]. Available from: Decentro – Evolution of Internet Banking
14. Sukhadolski S. IoT in banking: welcome to the age of intelligent finance [Internet]. Innowise; 2025 Apr 30 [cited 2026 Sep 7]. Available from: Innowise – IoT in Banking
15. Sadiku MNO. Internet of Things and its applications. Chișinău, Moldova: Lambert Academic Publishing; 2024.
16. Parker PM. The 2027-2032 world outlook for Internet of Things (IoT) in BFSI (banking, financial services, and insurance). San Diego, CA, USA: ICON Group International, Inc.; 2026.
17. Parker PM. The 2023 report on Internet of Things (IoT) in BFSI (banking, financial services, and insurance): world market segmentation by city. San Diego, CA, USA: ICON Group International, Inc.; 2022.

How to Cite This Article

Sadiku MNO, Padi D, Sadiku JO. Internet of Things in banking. Int J Future Eng Innov. 2026;3(5):43-51. doi:10.54660/IJFEI.2026.3.5.43-51.