happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

ARTIFICIAL INTELLIGENCE IN DIGITAL BANKING

CONTENTS

BACKGROUND

The most prevalent trend in today's financial services industry is the shift to digital, specifically mobile and online banking. In the era of unprecedented convenience and speed, consumers don't want to trek to a physical bank branch to handle their transactions. While on the one hand, banks are releasing new features to attract more customers and retain the existing ones, on the other hand, startups and neo banks with disruptive banking technologies are breaking into the scene.

The use of Artificial Intelligence (AI) in the banking industry can revolutionize the way banks operate and provide services to their customers, improving efficiency, productivity, and customer experience.

DIGITAL TRANSFORMATION IN THE BANKING INDUSTRY

Covid has accelerated the digital transformation and brought even those digitally shy consumers to the newer fold. The digital shift is changing the whole customer experience with an estimation of 75 to 80 billion devices being connected to the internet by 2025.

As people want the convenience of banking right at their fingertips, it is also increasing the number of frauds at a staggering rate.

One of the major challenges in the banking industry is cyber fraud.. The world is losing about $5 trillion annually to such crimes with the number expected to double in the next five years. It is a big problem and India ranks among the top-5 most attacked countries in the world.

Every day, a huge number of digital transactions take place as users pay bills, withdraw money, deposit cheques, and do a lot more via apps or online accounts. Thus, there is an increasing need for the banking sector to ramp up its cybersecurity and fraud detection efforts.

This is where Artificial Intelligence in banking comes to play.

ARTIFICIAL INTELLIGENCE

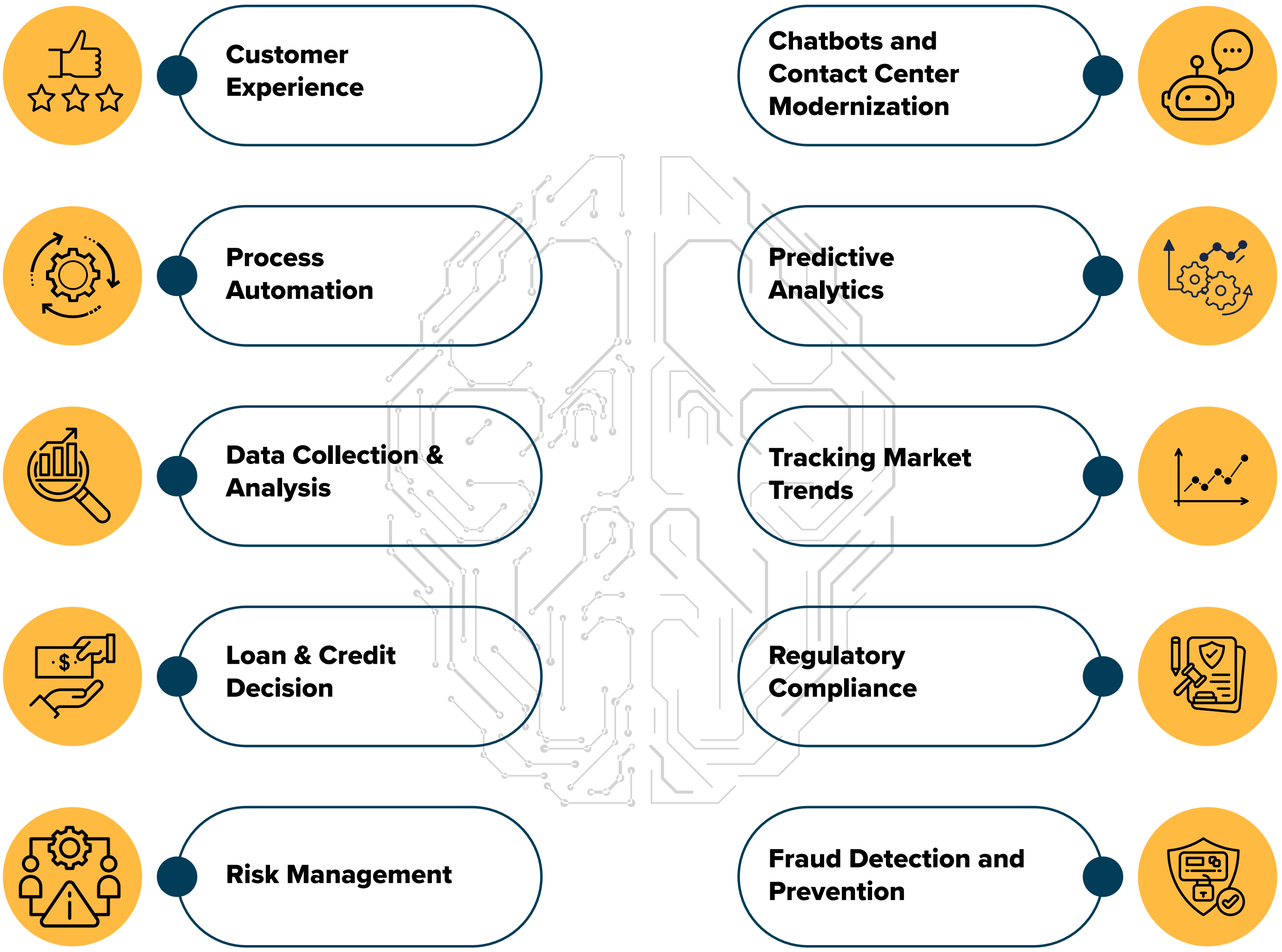
Artificial Intelligence or AI comprises a range of technologies and techniques that enable machines to mimic or perform tasks that would typically require human intelligence, such as learning, problem-solving, and pattern recognition. This can include techniques like Natural Language Processing, Machine Learning, Deep Learning, and Expert Systems.

Artificial Intelligence can help banks improve the security of online finance, track the loopholes in their systems, and minimize risks.

AI with Machine Learning

It can quickly identify fraudulent activities and alert customers as well as banks. It can also be used to classify customers into different segments based on their demographics and spending patterns or to predict which customers are most likely to default on a loan. It can also predict which transactions are most likely to be approved or denied. Additionally, it can be used to identify which products or services a customer is most likely to be interested in and to recommend them to customers based on their past behavior.

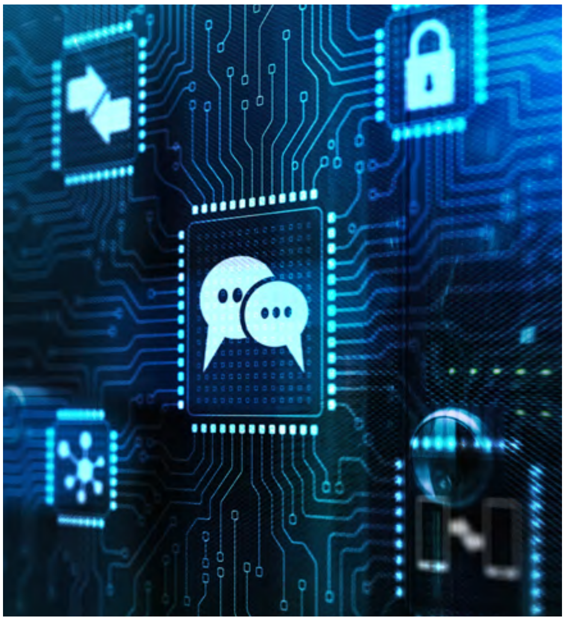
These are a few reasons why AI is being widely adopted in the banking industry. Some of the other benefits of using AI in banking include:



- Customer Experience
- Process Automation
- Data Collection & Analysis
- Loan & Credit Decision
- Risk Management
- Chatbots and Contact Center Modernization
- Predictive Analytics
- Tracking Market Trends
- Regulatory Compliance
- Fraud Detection and Prevention

AI with Natural Language Processing

An example of a Conversational Experience in banking might be a chatbot that customers can interact with through a messaging platform or a banking app. The chatbot could be trained to understand and respond to various customer inquiries, such as account balances, transaction history, and account management. For example, a customer might ask the chatbot, "What is my account balance?" The chatbot would then use Natural Language Processing to understand the question, access the customer's account information, and respond with the current balance. Some other examples of Conversational Experience would include Voice Assistant, Contact Center Modernization, etc.



AI with Deep Learning

It is a powerful technique that can help banks improve the accuracy and efficiency of many processes and enhance the customer experience. For instance: Deep learning algorithms can be trained on historical data to identify patterns and anomalies indicative of fraudulent activity. This can help banks detect and prevent fraud more effectively and help banks make better-informed decisions. Other examples include Loan & Credit Decisions and Risk Management.

AI for Cybersecurity

What is a cyber threat?

The banking sector has been under attack for hundreds of years. First, it was the physical theft of money, and then computer fraud. Cyber security is critical in banking because today , it's not only cyber fraud being committed but criminals are also hacking into servers to obtain a customer's personally identifiable information (PII). As individuals and companies perform most transactions online, the risk of a data breach increases daily. Therefore, there's a greater emphasis to examine the importance of cyber security in banking sector processes.

There are several other reasons to adopt this approach as well. At first, banks handle large amounts of sensitive financial information, including customer accounts, credit card numbers, and personal identification information. If this information were to fall into the wrong hands, it could be used for identity theft or other financial crimes. In addition to protecting customer information, banks also have a responsibility to protect their own assets and operations from cyber threats. This includes protecting against cyber-attacks that could disrupt the bank's operations or compromise its systems and data.

In the digital age, cyber threats to the banking industry are becoming increasingly sophisticated and widespread. Banks must therefore implement robust cybersecurity measures to protect themselves and their customers from these threats. This includes measures such as firewalls, intrusion detection and prevention systems, and data encryption to prevent unauthorized access to sensitive information. It also includes training employees to recognize and prevent cyber-attacks, and regularly testing and updating systems to ensure that they are secure.

Overall, cybersecurity is a critical concern for the banking industry, and banks need to invest in robust cybersecurity.

Some of the other items to be concerned about include:

MORE RISKS FROM MOBILE APPS

More individuals access their bank accounts on mobile apps. Many of these people tend to have minimal or no security, and this makes the potential of attack much greater. Hence, banking software solutions are required at the endpoint to prevent malicious activity.

BREACHES AT THIRD-PARTY ORGANIZATIONS

As banks have upgraded their cyber security, hackers have turned to shared banking systems and third-party networks to gain access. If these aren't as protected as the bank, the attackers can get through with ease.

INCREASED RISK OF CRYPTOCURRENCY HACKS

In addition to standard funds, hacks have increased in the growing world of cryptocurrency. Since the sector is unsure how to implement cyber security software for banking in this ever-changing market, the ability for attackers to grab large amounts of this currency is greater, especially when it quickly jumps in value.

HOW CAN AI HELP THE BANKS?

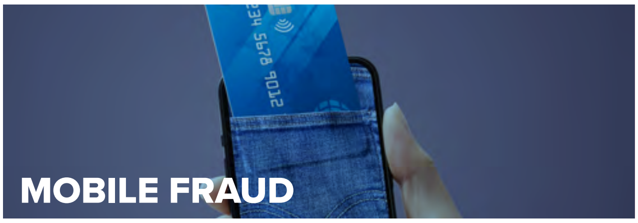
The different areas where financial fraud detection software can assist enterprises.

EMAIL PHISHING

This is a type of cybercrime wherein attackers send fake messages and website links to users via email. These emails are seemingly legit and authentic so that anyone can misjudge them and enter vulnerable data that puts them at risk. To avoid such situations, one can use automated methods for detecting phishing through machine learning. These methods are based on classical machine learning algorithms for classification and regression.

CREDIT CARD FRAUD

In an increasingly digital world, credit card fraud has become quite common. This type of financial fraud involves stealing debit cards or credit card numbers through unsecured internet connections. Machine learning algorithms help identify which actions are authentic and which ones are illegal. If someone tries to cheat the system, an ML model can alert the bank and take necessary measures to negate the activity.



MOBILE FRAUD

Machine learning integration in anti-fraud systems is particularly crucial when payment methods extend beyond physical cards and into the realm of mobile phones. Smartphones now feature NFC chips, enabling users to pay for products just with their phones. This means your smartphone is prone to hacking and cyber threats. Machine learning in Finance is an effective tool to detect abnormal activities for each user, thus minimizing mobile fraud risks.

IDENTITY THEFT

Information such as user's name, bank details, passwords, login credentials, and other extremely sensitive information is under great threat if a cybercriminal comes into play. Identity theft puts both individuals and enterprises at risk. Machine learning in Finance helps examine and check identity documents such as passports or driving licenses against secure databases in real-time to ensure all fraud cases are detected. Besides, ML can be also used for fighting fake IDs by enabling biometric scanning and face recognition.

INSURANCE CLAIMS

Insurance fraud typically includes fake claims of car damage, property, and even unemployment. To reduce such frauds, insurance companies spend an extensive amount of time and resources to validate each claim. However, this process is expensive as well as prone to hacking. Due to its superior pattern recognition capabilities, machine learning helps resolve insurance claims with utmost accuracy and find fake ones. .

SAFEGUARD WITH SECURED SOFTWARE

When looking at the ongoing state of security on the internet, one must consider enhancement or complete replacement of the current protection applications. Here are some things to look at in banking software development.

SECURITY AUDIT

A thorough audit is imperative before implementing any new cyber security software. The review reveals the strengths and weaknesses of the existing setup. Furthermore, it provides recommendations that can help save money while also allowing for the proper investments.

ANTI-VIRUS AND ANTI-MALWARE APPLICATIONS

While a firewall upgrade increases protection, it won't stop attacks unless anti-virus and anti-malware applications are updated. Older software might not contain the latest rules and virus signatures. In turn, it can miss a potentially disastrous attack on the system.

BIOMETRICS

It is another version of MFA which is more secure than a texted code. This form of authentication relies on retina scans, thumbprints, or facial recognition to confirm a user's identity. Though hackers have accessed this type of authentication in the past, it is more difficult to accomplish.

FIREWALLS

Cyber security banking configuration does not include only applications. It also requires the right hardware to block attacks. With an updated firewall, banks can block malicious activity before they reach other parts of the network.

MULTI-FACTOR AUTHENTICATION

The multi-factor authentication also known as MFA, is extremely critical to protect customers who utilize mobile or online apps to do their banking. Many users never change their passwords and if they do, they make small changes. With MFA layering attackers are prevented from reaching the network because it asks for another level of protection. For instance, a six-digit code sent to a customer's cell phone.

AUTOMATIC LOGOUT

Many websites and apps allow a user to stay logged in if they allow it. Thus, they can access their information at any time without entering their login credentials. However, this also permits attackers to easily obtain your records. Automatic logout minimizes this by closing a user's access after a few minutes of inactivity.

EDUCATION

All of the above measures can increase cyber security in the banking sector. Nevertheless, they can't help if customers continue to access their information from unprotected locations or improperly protect their login credentials. This is why education is important. When banks notify their customers of consequences related to these vulnerabilities it may move them to change their habits for fear of losing their investments.

AI for Customer Experience

Traditional IVR Contact centers in banks are customer service centers that handle incoming calls and other forms of communication from bank customers. These centers are typically responsible for providing information, answering questions, and resolving issues related to banking products and services. Following are some of the main challenges faced by traditional contact centers in banks which could result in lost sales and dissatisfied customer.

Managing high call volume — These centers may not be able to handle the volume of calls. Validation of the customer could become a cumbersome repetitive task.

How can AI help the Banks in improved Customer Experience?

Artificial intelligence (AI) can be used in the banking industry to improve customer experience in several ways. AI-powered chatbots and virtual assistants can be used to provide automated customer service, answering common questions and helping customers to resolve issues more quickly and efficiently. This will enable an omni-channel interaction, which could result in an improved customer experience.

Providing accurate and timely information—They normally operate only during prescribed business hours. There are routing of calls to irrelevant department and the overall customer experience is disrupted. There are too many options provided in IVR, where customer would have to listen carefully and decide, which may result in the customer not getting the required information.

Other challenges include maintaining security and compliance with regulations, managing and training staff, and dealing with complex and changing technology systems.

Improved efficiency and productivity

AI can automate a variety of tasks and processes in the banking industry, freeing up human employees to focus on more complex or value-added tasks and improving efficiency and productivity. IVR solution can be enabled 24/7 to handle queries and request across the globe. Triaging of calls to right agent will increase customer satisfaction and improve efficiency. Banks can gather inputs from IVR system for frequently enquired products / services which can be offered. Based on this bank can launch new products / services.

Personalized recommendations

AI can be used to analyze customer data and make personalized recommendations for products or services that may be of interest to them. This can help banks to better meet the needs of their customers and provide a more personalized and convenient experience. For the banks and financial institutions, it would reduce the Turn Around Time and money saved.

Predictive analytics

AI can be used to analyze customer data and make predictions about their future financial performance, helping banks to make more informed investment and lending decisions. This can help banks to identify opportunities to upsell or cross-sell products, as well as to identify potential issues that customers may face and proactively address them. This would result in regaining the trust of customers confidence and improved brand reputation.

WHY ARE BANKS SLOW IN USING AI?

Some of the challenges that banks may face when adopting AI technology include:

Regulatory compliance

The financial industry is heavily regulated, and banks need to ensure that any new technology they adopt is compliant with these regulations. This can be a time-consuming and costly process.

Integration with legacy systems

Many banks have large, legacy IT systems that are difficult to integrate with new technologies. This can be a challenge when it comes to adopting AI systems, as the technology may require access to data from these legacy systems in order to function effectively.

Data privacy and security

Banks handle a large amount of sensitive customer data, and any new technology that is adopted must be able to protect this data. This can be a challenge when it comes to AI, as the technology often requires access to large amounts of data in order to function effectively.

Lack of skilled personnel

There is currently a shortage of individuals with the necessary skills to develop and implement AI systems. This can make it difficult for banks to find the personnel they need to adopt the technology.

Resistance to change

As with any new technology, there may be resistance to adoption from employees or customers. Banks may need to invest in training and education in order to overcome this resistance and ensure the successful adoption of AI.

What are the challenges faced by end users?

Lack of understanding

Many people may not understand how AI works or what it can be used for, which can make them hesitant to use it.

Concerns about security and privacy

Some people may be concerned about the security of their personal or financial information when using AI-powered banking services.

Resistance to change

Some people may be resistant to using new technologies, especially if they are used to traditional methods of banking.

Lack of access

Not everyone may have access to AI-powered banking services, either because they are not offered in their region or because they do not have the necessary technology (e.g. a smartphone) to use them.

Costs

Some AI-powered banking services may come with additional fees, which may be a barrier for some users.

WHAT IS THE CURRENT ADOPTION RATE OF AI IN BANKING INDUSTRY?

It is difficult to say exactly what the current adoption rate of AI in the banking industry is, as it can vary widely from one bank to another. Some banks have been early adopters of AI and have implemented a wide range of AI-powered services, while others have been slower to adopt the technology. It is generally accepted that the adoption of AI in the banking industry has been increasing in recent years, and it is expected to continue to grow in the coming years. According to a survey conducted by Accenture, 37% of banks reported using AI in 2019, and that number increased to 53% by 2020 and is increasing further.

What are the key drivers that would lead to widespread usage of AI by banks?

1 **Increasing competition**
As more banks adopt AI, those that do not may struggle to keep up with their competitors in terms of efficiency and customer service.

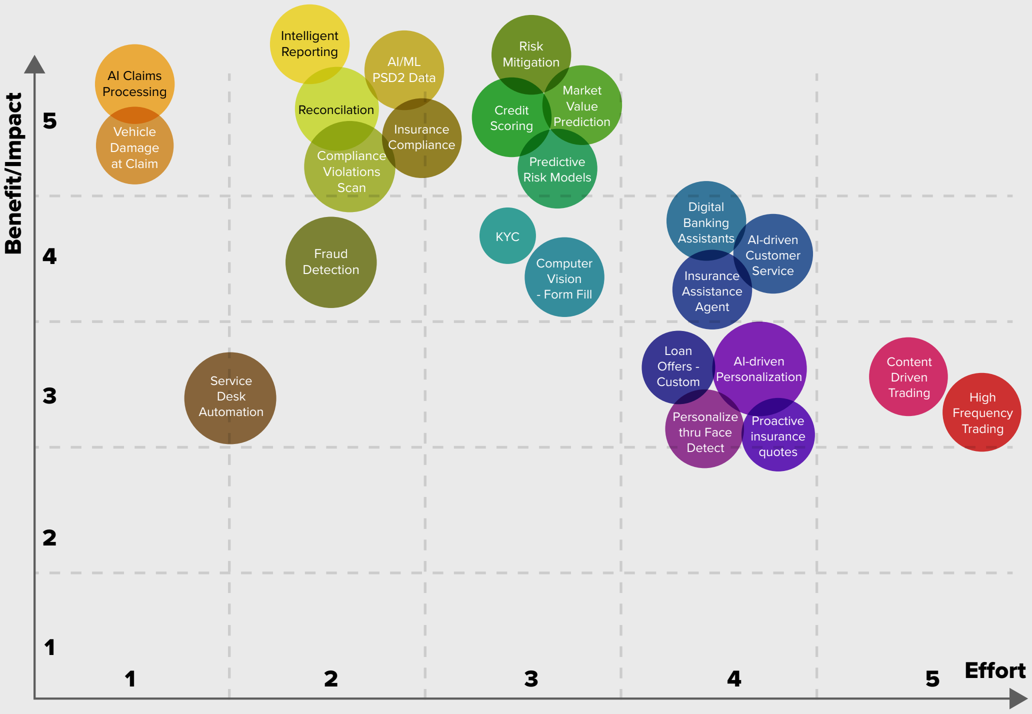
2 **Customer demand**
As more and more customers become accustomed to using AI in their daily lives, they may come to expect similar technologies from their banks.

3 **Cost savings**
AI can help banks reduce costs by automating many tasks that were previously done manually, such as fraud detection and customer service.

4 **Improved decision making**
AI can help banks make more informed and accurate decisions by analyzing large amounts of data in real-time.

5 **Regulatory pressure**
Some governments and regulatory bodies are encouraging or mandating the use of AI in the financial industry to help reduce risk and improve the overall stability of the financial system.

The following chart provides a bird's eye analysis of the Effort vs Benefit while implementing AI in Banking.



CONCLUSION

Overall, the use of AI in the banking industry can help to improve customer experience by providing personalized recommendations, faster and more efficient customer service, and improved fraud detection and prevention.

In 2023 and beyond, one of the main driving forces for change impacting the banking and financial services industries will be the need to meet customer experience expectations. The main aspects of this open banking trend are the need for financial institutions to provide an omnichannel banking experience, which means that customers can move seamlessly between their actions (mobile, online or face-to-face) without needing to initialize the action each time. For this to work, it is essential that the user experience can be personalized, with the interactions being based on knowledge of the customer's needs and past experiences and requirements. Personalizing means that the customer will build a deeper relationship with their bank and be less inclined to shop around in the highly competitive market. To provide a fully personalized experience, the bank needs comprehensive and up-to-date data on which it can apply the powers of Artificial Intelligence and Machine Learning. This power will generate insights that help understand customer needs better and offer targeted marketing of products and services.

Hence, 70% of the banks are looking ahead to integrating AI in mobile banking apps and stepping forward to embrace the golden opportunities of AI in banking industry.

Overall, the use of AI in the banking industry has the potential to bring significant benefits for both banks and their customers, but it is important for banks to carefully manage and utilize these technologies in a responsible and ethical manner.

References

1. Case studies from banks and financial institutions that have implemented AI solutions.
2. Reports and studies from consulting firms such as McKinsey, Deloitte, and Accenture, which provided insights on how AI is being used in the banking industry and its potential impact on the industry.
3. Industry reports which provided a broader look at the overall impact of AI on the financial services industry.

ABOUT THE AUTHOR

Shobita K Sridharan is a Business Analyst Consultant at Happiest Minds Technologies Ltd. She has around 15 years of experience in the IT Industry in Project Management, Customer Relationship Management across Supply Chain Management, BFSI, Insurance, e-Governance domains.

For more information, write to us at

business@happiestminds.com

About Happiest Minds Technologies

Happiest Minds Technologies Limited (NSE: HAPPSTMNDS), a Mindful IT Company, enables digital transformation for enterprises and technology providers by delivering seamless customer experiences, business effciency and actionable insights. We do this by leveraging a spectrum of disruptive technologies such as: artificial intelligence, blockchain, cloud, digital process automation, internet of things, robotics/ drones, security, virtual/augmented reality, etc. Positioned as 'Born Digital . Born Agile', our capabilities span digital solutions, infrastructure, product engineering and security. We deliver these services across industry sectors such as automotive, BFSI, consumer packaged goods, e-commerce, edutech, engineering R&D, hi-tech, manufacturing, retail and travel/transportation/hospitality.

A Great Place to Work-Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, Canada, Australia and Middle East.

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

www.happiestminds.com