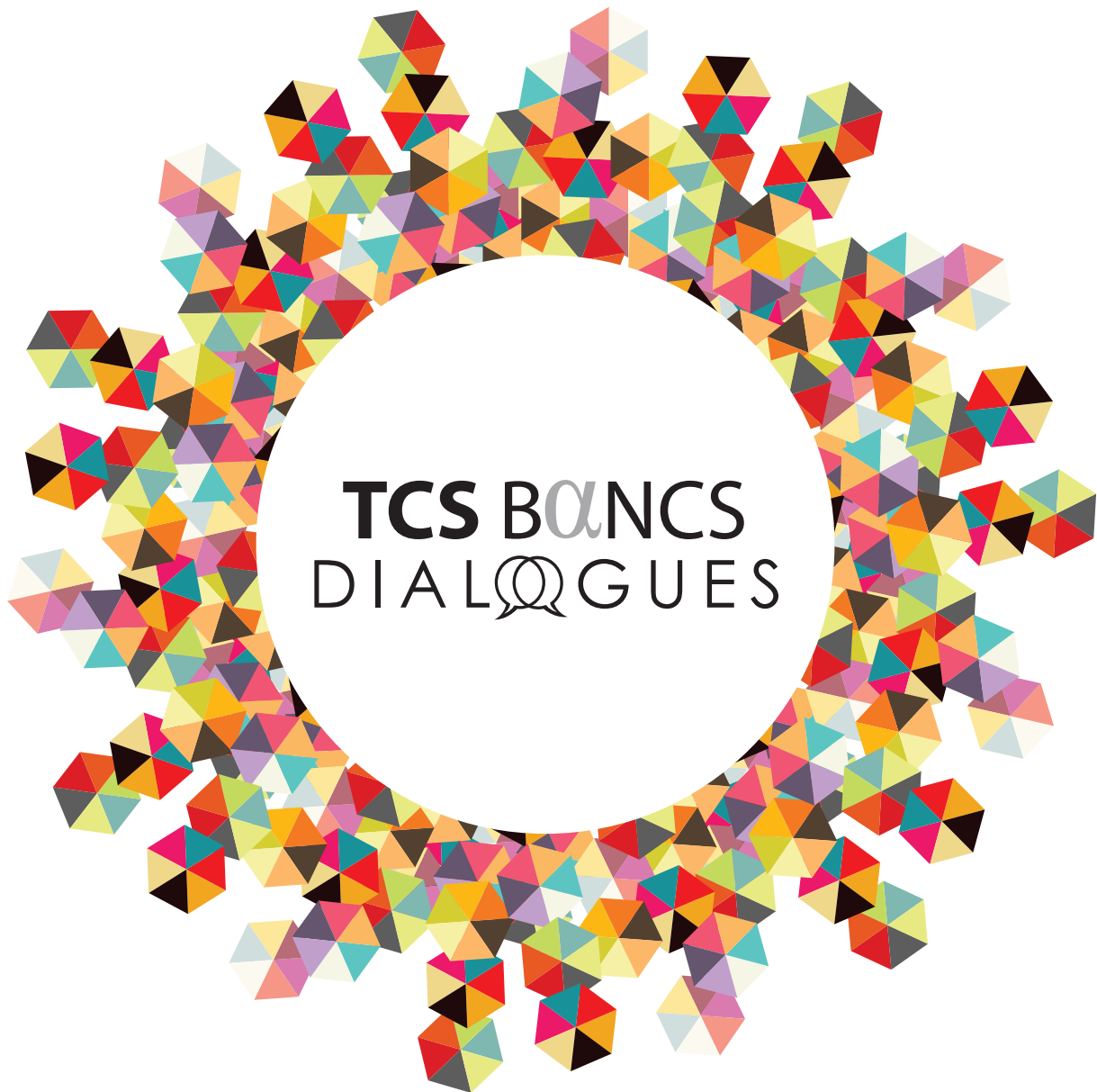


RESEARCH JOURNAL





Bank Yahav set out to transform its banking landscape, in a first of its kind for Israel. They found a certain way.

Bank Yahav, a retail bank, was looking for an end-to-end universal banking system to offer a wide spectrum of services in banking, payments, securities trading and advisory services across local and international markets. They selected TCS BaNCS for Universal Banking from Tata Consultancy Services to fulfill this strategic imperative. TCS deployed an end-to-end solution to meet the bank's business requirements, including infrastructure and data security set up, and a range of IT and operational services. This core banking transformation entailed integrating over 500 interfaces with nearly 100 entities into a complex ecosystem as well as ensuring compliance with over 1,800 regulations. As the first bank in the country to adopt an international core system, Bank Yahav has set a benchmark in the Israeli banking industry.



IT Services
Business Solutions
Consulting



TATA CONSULTANCY SERVICES

Experience certainty.

TATATATA

FOREWORD

Digitization of the global economy is progressing at a furious pace. Large parts of the economic supply chain, which were manual, are now getting automated; and, those already automated are getting autonomous. At the core of the digital wave, lie data and networks. The ability to leverage data and the power of networks are crucial to those who wish to ride the digital wave or derive sustained economic value, as traditional business value creation chains are constantly getting disrupted. Our own evolution at TCS BaNCS and our forward looking product strategy revolves around these themes of data and networks to a large degree while, at the same time, we continue with our investments in traditional core transaction processing capabilities in line with market and regulatory expectations.

Data is the fuel of the digital economy. The ability to process data of various types to provide insights, intelligence and intuition are going to be key differentiators in the future. One of the most powerful manifestations of the power of data is AI, which is slowly but surely occupying center stage in organizational strategies. While AI as a field of research has existed for decades, it is with the ever increasing power to process disparate types of structured and unstructured data in large volumes and in real time, that AI has “come of age” and is finding application at scale.

Another interesting evolution which has come to characterize the digital economy is the increasing number of ecosystems and networks of organizations/ individuals/devices connected together to provide a game-changing value proposition. In this context, technologies like blockchain are beginning to find industrial use cases and hold promise of increased adoption in eliminating friction in the information value chain, thereby building trust.

While businesses cope with the disruption induced by the digital economy, significant regulatory evolution in the form of PSD2 and GDPR, as well as the more recent Consultative Document on “Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors”, issued by the Bank for International Settlements reflect regulators’ keenness to open up various financial supply chains, while at the same time protecting data, privacy and customer interest. There is a heightened awareness of risk implications of industry evolution as hyper-connectivity also exposes financial infrastructures to ever increasing security threats and malware.

This edition of the TCS BaNCS Research Journal brings you a collection of viewpoints and articles, which shine the spotlight on specific topics encompassing AI, blockchain and analytics. Insights into regulatory compliance, data privacy and security that we have presented here endeavor to present the risk angle in perspective.

I hope you enjoy reading the Journal.



Venkateshwaran Srinivasan
Head, TCS Financial Solutions (TCS BaNCS)

VIEWPOINT

The term 'Fintech' has come to symbolize new technology, innovation, disruption and financial startups; however, this upstart marriage of finance and technology has also become a genuine alternative to the conventional delivery of financial services and technology. Fintechs have truly arrived and are no longer small or niche; in fact, they are as mainstream as the smartphone. So much so, that in niche areas such as regulatory compliance, we are seeing the rapid evolution of RegTechs, who address specific aspects of the regulatory landscape.

Digital, cloud, AI and, gradually, block chain are becoming centerpieces to new and emerging business models that will shape the financial industry of tomorrow; and, we are yet to imagine the many avatars that the fourth industrial revolution is set to bring about. Complex regulations are being translated into APIs by Regtechs, streamlining compliance processing with the help of machine learning, biometrics and distributed ledgers.

Even as the industry debates the many possibilities and variants in which Fintechs and incumbents can work together, many financial institutions and their established technology partners have been collaborating to create meaningful and open financial services ecosystems, that foster greater integration with fintechs.

Fintechs have intricate methods of storing—and gleaning intelligence from—data, in addition to making many, inventive technological advances. On the other hand, banks and financial services players continue to remain leaders in the trust department in customer experience.

While this interplay between trust, scale and innovation, aided by a slew of technologies and maturing simultaneously like never before, will create a more level playing field between Fintechs and incumbents, it will also make it easier for the financial services industry to address the large underbanked population worldwide.

We have been watching all of these developments closely while also investing in—and deploying—new technologies that bestow our customer organizations with a stronger digital backbone, making them nimble and more responsive to what their customers need.

TCS BaNCS, along with its customers, is now partnering with Fintechs and RegTechs to create vibrant and open ecosystems. Be it collaborating with a RegTech firm for tax compliance in a particular country or creating a smart network with fintech partners to facilitate blockchain based Forex transactions, we are in some sense at the intersection between these worlds.



R Vivekanand
Vice-President and Co-Head,
TCS Financial Solutions - TCS BaNCS

EDITORIAL

Dear Reader,

This edition of the TCS BaNCS Research Journal shares perspectives about how data analytics, artificial intelligence and blockchain are creating new business opportunities in the financial services industry. As you have seen in the points of view articulated by Venkat and Vivek earlier, there are two things that will determine success in this metamorphic era: data and trust.

The usage of data, like a kaleidoscope does, to create meaningful patterns, and then to act on them in the right manner and at the right time cannot be overemphasized. Concurrently, how these insights are then applied in a business to engender trust and loyalty becomes vital.

The authors in this edition have crafted their viewpoints based on the many years of education and experience they have in designing and deploying solutions for financial services organizations worldwide. They take you through how the industry will expand into new territories, with partnerships, to create an open ecosystem of products and services, which may just not be related to the financial services domain alone.

Happy Reading.



Anjana Srikanth
General Manager
Marketing and Communications
TCS Financial Solutions (TCS BaNCS)

EDITORIAL BOARD



Dennis Roman
Chief Marketing Officer
TCS Financial Solutions (TCS BaNCS)



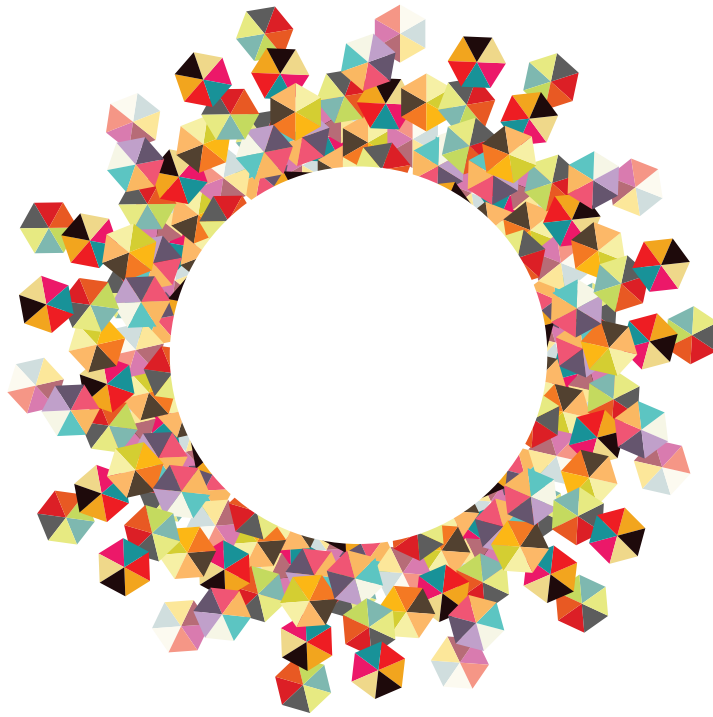
Anjana Srikanth
General Manager
Marketing and Communications
TCS Financial Solutions (TCS BaNCS)



Arun Arunachalam
Head, Product Management
TCS Financial Solutions (TCS BaNCS)

Do you remember the first time you saw a kaleidoscope? You would peer inside as the tube turned slowly and marvel at the fine patterns formed by the bits of colored glass pieces inside. In fact, the word kaleidoscope comes from the Greek phrase, "beautiful form to see".

A kaleidoscope uses light and mirrors to reflect objects and create beautiful patterns. Data when collected and mined the right way can create meaningful structures, offering numerous insights.



CONTENTS

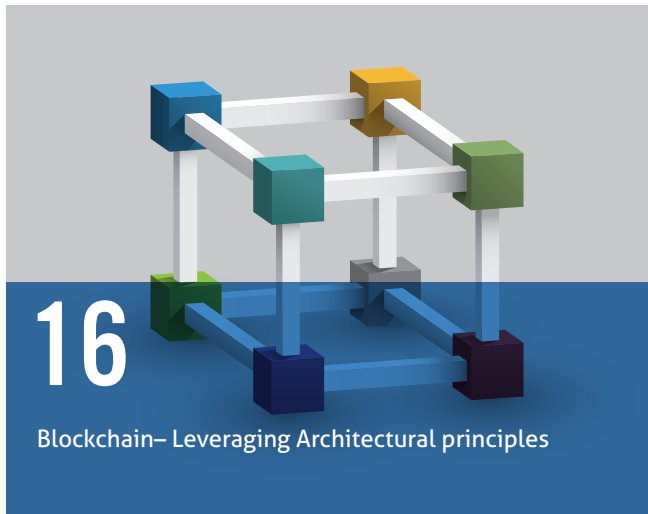
RESEARCH JOURNAL



10

Artificial Intelligence in Asset Servicing

The cover features a glowing blue portal on a dark surface. Above the portal, various white icons are scattered, including a shopping bag, a bar chart, a plus sign, an envelope, a clock, the letters 'ABC', a hanger, a car, a fork and spoon, an AI chip, a speech bubble, and a musical note.



16

Blockchain– Leveraging Architectural principles

The cover shows a 3D architectural structure made of white beams and colored blocks (blue, yellow, green, red) on a blue base. The structure is a cube-like frame with some blocks missing or in different positions.



22

RegTech - At the Crossroads of FinTechs and Regulatory Compliance

The cover depicts a stylized cityscape at night with various digital devices and icons. A hand is shown typing on a laptop, another holding a tablet, and a third holding a smartphone. Icons include a helicopter, a calendar, a mail envelope, a person profile, and a document.

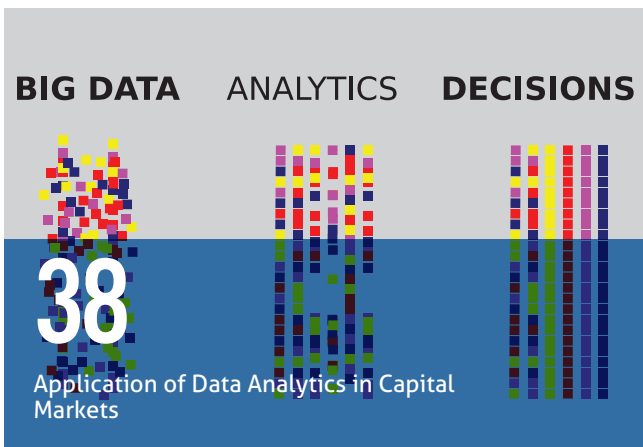


30

Understanding Data Privacy in the Financial Services World

The cover features a central shield icon with a white and orange design. Surrounding the shield are various icons: a calendar, a gear, a shopping cart, a cloud with a refresh symbol, a credit card, a padlock, and a document with a person icon.

BIG DATA ANALYTICS DECISIONS



38

Application of Data Analytics in Capital Markets

The cover displays three vertical bar charts of varying heights and colors (red, yellow, green, blue). The background is a light grey top half and a dark blue bottom half.

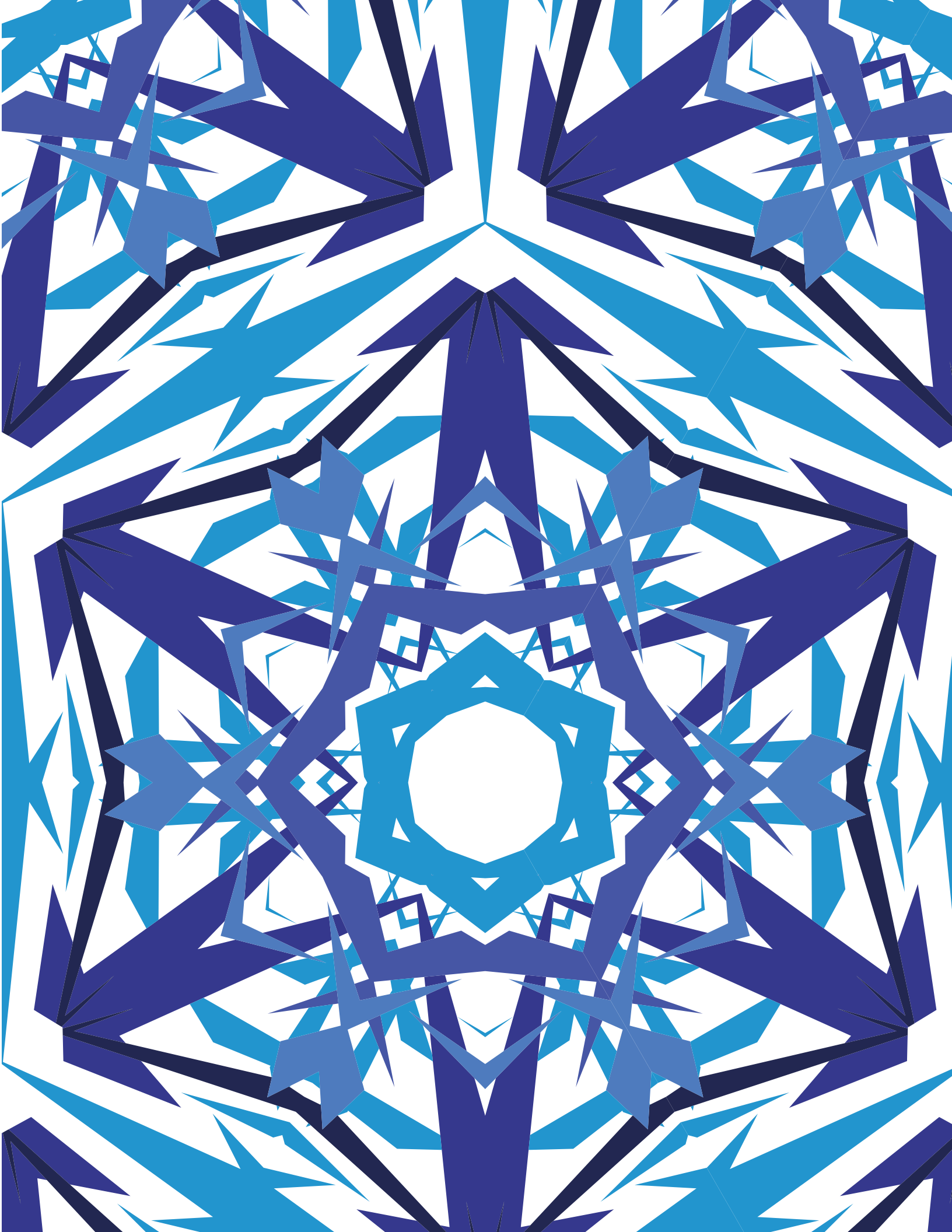


46

Viewing Connected Things through a Security Lens

SMART CITY

The cover shows a stylized city skyline with various colored buildings. Above the skyline are blue clouds, some with padlock icons. The text 'SMART CITY' is written in a light blue font at the bottom right.



ARTIFICIAL INTELLIGENCE IN ASSET SERVICING



Artificial Intelligence (AI) technology becoming main stream is strongly dependent on the quality of data that is used to embed 'intellect' into algorithms. AI—as a tool that utilizes value-added data—is used to build smart programs that negate the need for human intervention, especially, in performing repetitive tasks. The phrase “data is the new oil”, coined by Clive Humby, UK Mathematician and architect of Tesco’s Clubcard, has become a game changer in the prevailing

technology scenario. Drawing a corollary to oil -- although data is valuable, it cannot be used unless it is refined; oil goes through refinement and is converted into gas, plastic, chemicals, eventually creating a valuable entity that drives profitable activity. Just like oil, data must be broken down and analyzed for it to reap value.

If AI has to live up to its promise of driving transformative change in business, especially through

digitization, there is a need to focus on the challenge of maintaining accurate and valuable data. Early adopters of AI are bound to gain a huge first mover advantage in the market because they know that the sooner these systems begin learning about the context in which they operate, the sooner they can mine data to make increasingly accurate predictions.

In today’s context, tech firms are investing considerably in AI

platforms to help their clients increase bottom-line by cutting operational costs. Data driven insights not only enable strategic decisions for business leaders but also provide timely operational intelligence to automate business processes and provide more targeted and personalized service delivery for improved customer experience.

AI Trends

AI and machine learning have reached a tipping point today, and will increasingly augment virtually every technology enabled service, thing or application. More than 80% of companies across all industries presently use AI, and even those that don't use AI today are expected to be adopters by 2020.

AI technologies are being deployed for varied use cases across consumer, enterprise and government markets, resulting in a rise in demand. Advanced analytics based applications are slated to utilize structured as well as unstructured data, including

alternative data gleaned from emails, news, social media as well as satellite and drone images to derive market insights. AI is also powering autonomous business processes (such as surveillance and fraud detection) and conversational applications (such as chatbots).

AI is an umbrella term that encompasses multiple technologies, with each tool being distinct and used to tackle different business issues:

- **Robotic Process Automation (RPA):** This technology aims to replace manual handling with automated processes for repetitive and high-volume tasks.
- **Machine Learning (ML):** This is a process around which most AI is being built today and involves the usage of large volumes of data that can be used to train a system and fine tune its responses and behavior. Enfolding a set of techniques by which computer programs
- **Deep Learning (DL):** DL algorithms involve AI that acts as an input to other forms of AI. Such architectures can be quite complex with a large

can improve the answers they give over time without requiring programmers to change the underlying code, it can generate continuous improvement and intelligent responses. For example, machine learning is being used to balance portfolios and manage risks by wealth and portfolio managers, by giving investment recommendations based on various parameters like risk-return profiles of a client, and so on. Also, in stock trading, algorithms help clients with getting the fastest trades at the best price and in providing data from counterparties to help judge the risk of conducting a deal. It may be possible for the algorithm to detect if a big buy order is coming from a giant mutual fund company or a high-frequency trading shop.

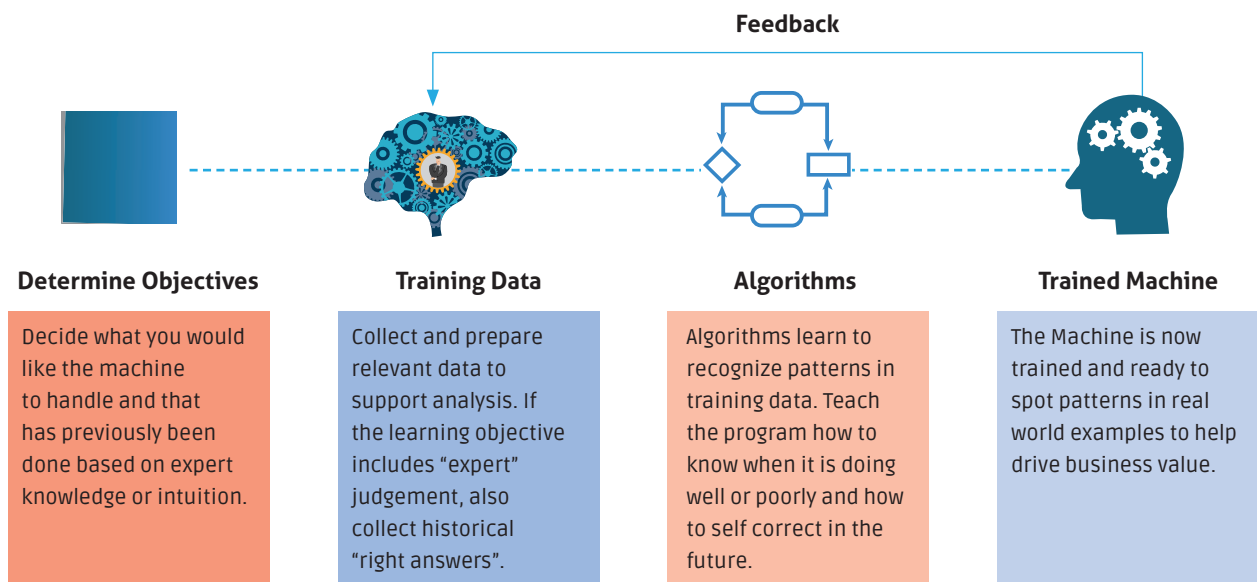


Figure 1: How does a machine learn?

number of machine learners giving their opinion to other machine learners. This is a specific method of machine learning that has been a game changer in data-intensive, machine-learning processes. DL models using graphic processing units are being used by banks to catch fraudulent activities with improved accuracy as the technology can adapt to ever changing fraud patterns.

- Cognitive Analytics (CA): This approach mimics the human brain in making deductions from vast amounts of data. For example, in the insurance industry, by reviewing data from closed claims, CA technology can identify both straightforward and complex

claims for automatic processing and those that are more likely to require human intervention. By identifying commonalities in closed claims that resulted in litigation, it could predict which new claims might take a similar path and recommend preventative measures. For example, it is being used to flag abnormal prescription patterns from pharmacies and alert an adjuster that some kind of clinical review might be necessary.

costs), which enable them to anticipate customer expectations and serve them better. Those using AI are more likely to be able to revamp their businesses faster, and in a competitive market, this can result in raising barriers to entry. Since financial institutions are virtually swimming in large pools of data, which is a prerequisite for any AI system to be efficiently trained, they definitely have a clear advantage over potential new entrants.

AI In Financial Services/Capital Markets

A significant part of the financial services industry has been using AI for the past three years, and is more invested in it as firms are able to foresee its myriad benefits (increased efficiencies and reduced

With dynamic and complex regulatory environments in global capital markets alongside the uncertain and slow pace of economic growth, both buy and sell side firms are faced with shrinking margins and increased competition. Looking ahead to 2020, the banks

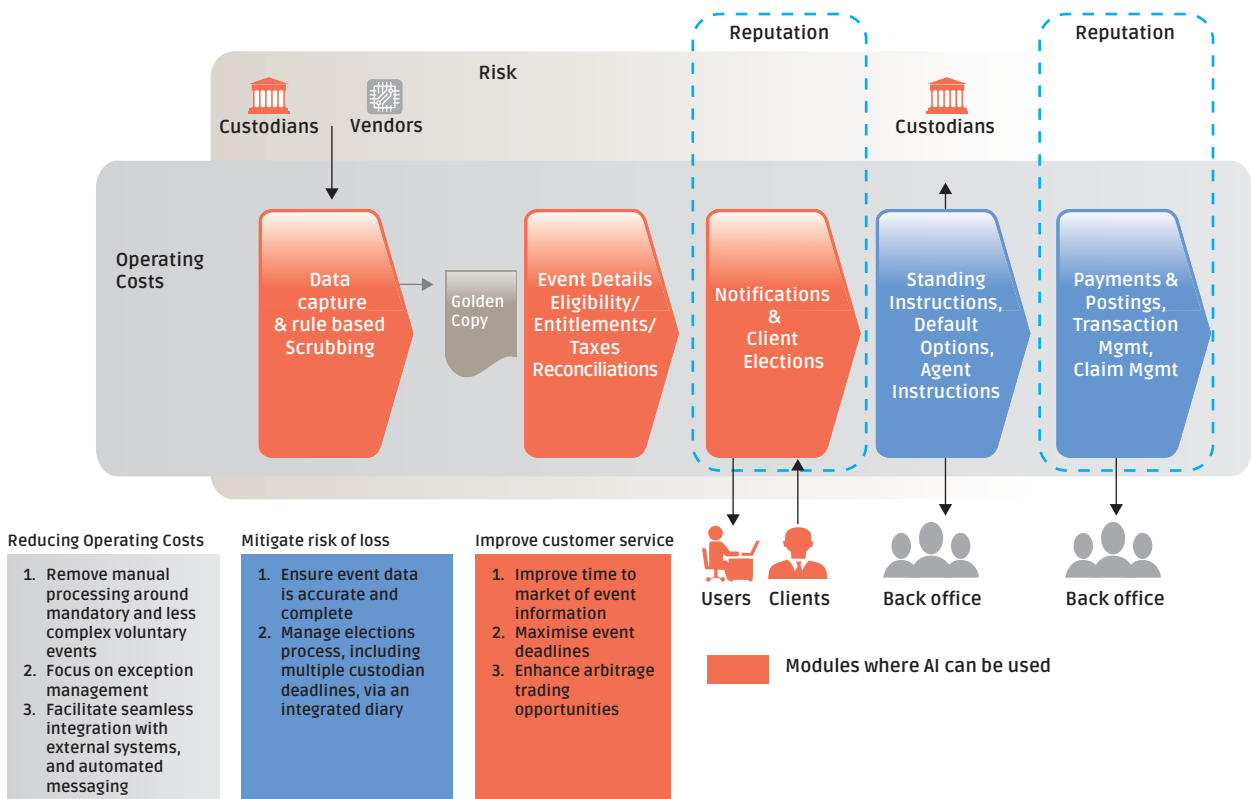


Fig 2: Drivers of a Corporate Actions Event Lifecycle

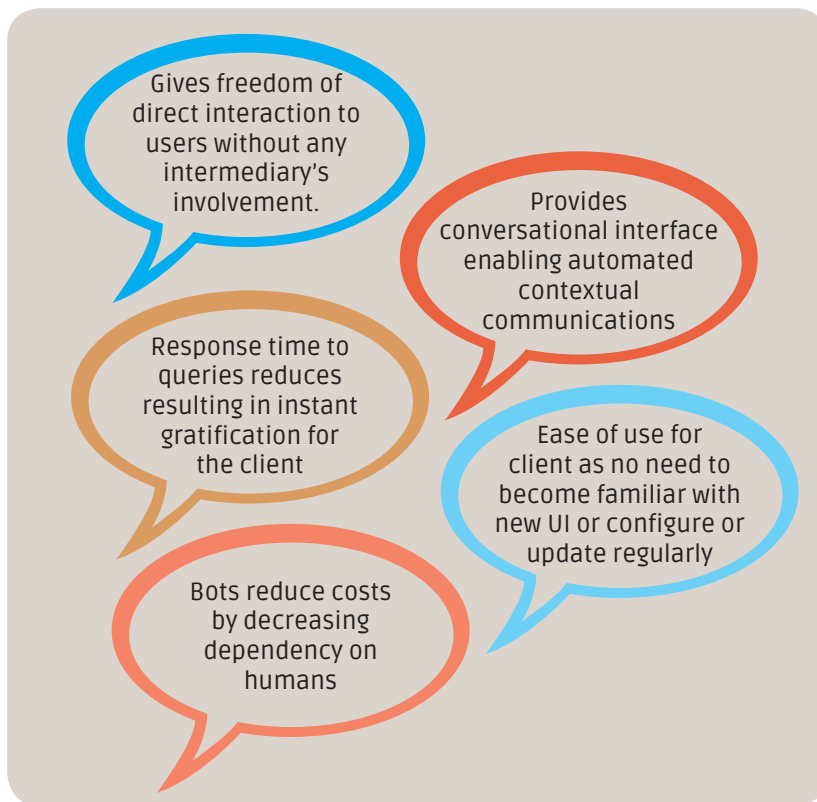


Figure 3: Benefits from using Chatbots

expect their investments in AI to increase to USD 99 million on average per company, notably increasing by 29% over 2015.

Industry analysts estimate a 28% improvement in financial institutions' cost-to-income ratio by 2025, as routine processes become automated. Among this crop, cognitive analytics and machine learning solutions are expected to garner the lion's share.

It is a given that most business operations will benefit from AI; therefore, prioritizing use cases based on an organization's position will become critical. RPA, for example, is more likely to appeal to securities players with large, back-office processing activities who can create useful, meaningful information from

new unstructured data sources for data providers, hedge funds and brokers. Other non-financial players in the capital markets ecosystem will have to adapt to the new world ahead.

As with any technological revolution, AI will decrease the value of traditional services that it's replacing and increase that of adjacent ones. Hence, BPO and IT solution providers will have to reconsider their business models and value proposition. Data providers such as exchanges/depositories may have to accelerate build and/or acquire services in the unstructured data space as the value of traditional market data may soon diminish.

AI in Corporate Actions

Post-trade operations have suffered from relative underinvestment in

technology in comparison with the front office. As a result, asset servicing tends to involve higher levels of manual processing and fragmentation. AI presents firms with opportunities to reduce headcount costs associated with running repetitive and low-value-adding tasks. The objective of using AI in asset servicing is to deliver a streamlined and automated approach to complete timely and accurate event processing.

Artificial Intelligence can be used in asset servicing broadly in the following two areas:

1. Client servicing

Business relationships are founded on trust. They are also predicated on the personal knowledge that a relationship manager has about a client, which is then studied and analyzed to present the best possible solution. This process can be hugely enhanced by systematically improving the quality, richness, relevance and insightfulness of available data. Where clients interact directly with a firm's systems, there are huge opportunities to increase client satisfaction and "stickiness" through well-designed, intuitive and value-adding interfaces like chatbots.

Chatbots are user interfaces (UIs) that provide a conversational experience for end clients. These tools have fast gained acceptance, alongside their extension to mobile applications with a combination of speech, text and touch interfaces, thereby, accelerating the introduction of new services to a client in rapid time. When applied to touch points such as client portals, capabilities such as these can be great differentiators, supporting client attraction and

retention, helping to contain costs as clients opt to self-serve their asset servicing needs, and enabling servicing of smaller clients via a “lower-touch” model.

As per industry reports, 80% of organizations worldwide intend to use a chatbot by 2021, resulting in a CAGR of 37.11% with USD744M in revenue. The BFSI sector accounted for the maximum market share during 2016 and may continue to dominate the market for the next few years.

The chatbots being used today are quite simplistic, as the bot is powered by an engine that learns over time. When chatbots are proactive and begin to understand the ‘intent’ rather than the ‘command’ and are even able to display shades of empathy, the experience can be delightful. This is exactly the sort of experience that will reinstate customer trust and ultimately create brand loyalty.

On one hand, chatbots can respond to customer queries instantaneously, eliminating the tedium arising from waiting. Questions that clients ask frequently in asset servicing are concerned with an event’s deadline, the ratio of stock that can be availed in the case of a merger, entitlement, documentation for tax rebates and so on. Chatbots provide both chat and voice based services and can further be used to capture elections and upload/download tax documents/forms/prospectus. Needless to say, the round-the-clock availability of chatbots without clients having to depend on call center executives, makes this tool most convenient. It is estimated that for a single customer transaction with an agent over the phone that can cost up to

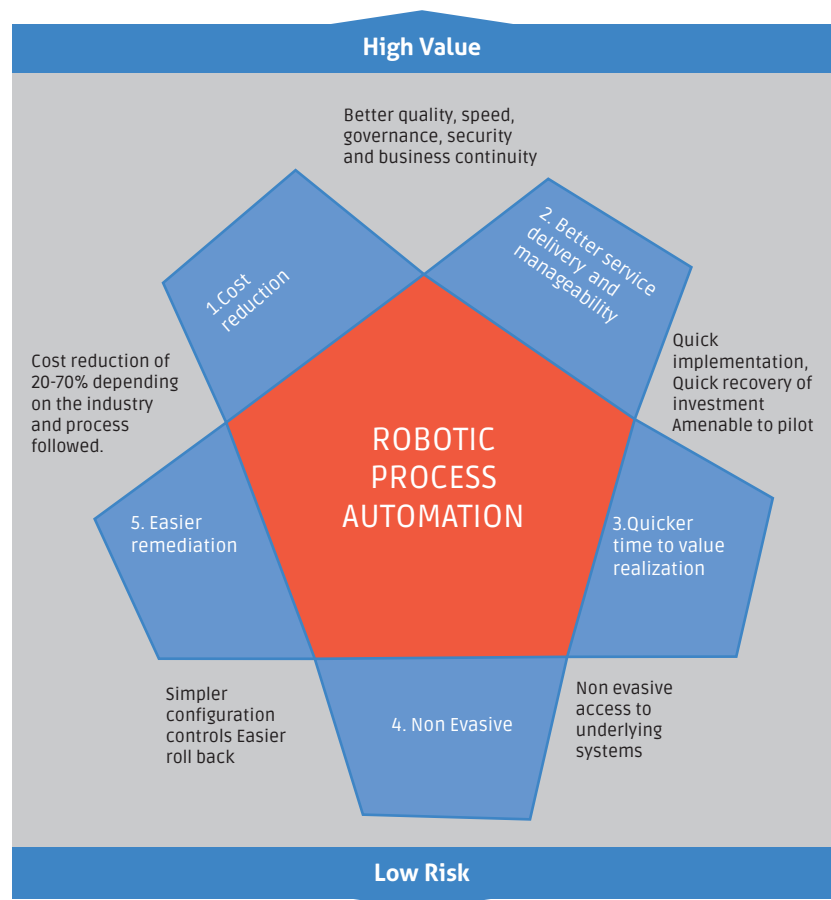


Figure 4: Benefits of RPA

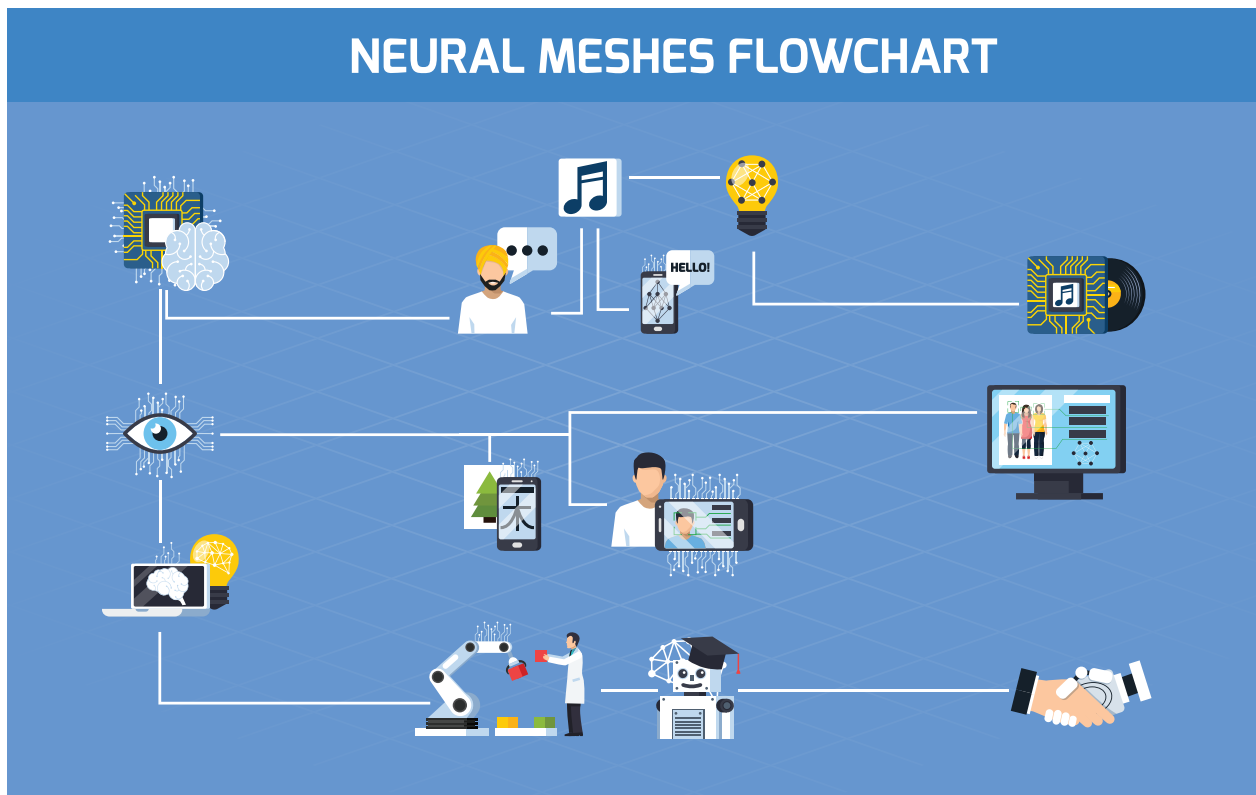
USD4.00, a chatbot will push down the expense by a handful of cents.

2. Transaction processing

There is an increasing need to automate various parts of the asset servicing value chain, and this is where RPA technology can help. It offers a quick and cheap way to improve the quality of automated data in addition to a host of other benefits such as capturing announcements by scanning and reading of printed material or web data; ensuring compliance with tax regulations; data preparation and break resolution related to

completion of reconciliations, and election capture of physical instructions, etc. The global RPA market is forecast to reach USD2,467.0 million by 2022 at a CAGR of 30.14% during (2017-2022), driven by the ease in business processing it offers and its convergence with traditional business process industries.

Deployment of RPA technology may result in a cost reduction of 20-70% depending on the type of industry and the process. Also since RPA is easier to implement, the time taken to reap its benefits is also lesser compared to other technologies.



Conclusion

Financial institutions are faced with a unique challenge when they automate asset servicing processes as the twin objectives that this is expected to bring in the form of reduced operational risk and costs can be easily derailed due to many other factors affecting the business. This is where, AI, with its ability to enable an operations team to greatly reduce risk while also making them less susceptible to processing volume peaks, comes in. Additionally, with the removal of repetitive, manual tasks and the attainment of STP (Straight-Through-Processing) wherever achievable, staff can be freed up to concentrate on adding value to the service they provide and focus on complex voluntary events, where the greatest risk truly lies.

Although chatbots promise simplicity and, RPA, low cost efficiency, a host of factors – analytics, flow optimization, platforms – have to be considered by financial services institutions to create a seamless experience in asset servicing. They may also need to evaluate the regulatory impact of an error before adopting chatbots or RPA technologies.

The most successful advances made in AI and machine learning place the customer at the center of all processes. The new crop of fintechs and their successes are demonstrative of this philosophy, as they play a pioneering role in following a design-led approach that is focused on using new technology to solve specific problems faced by their customers, and in a way that is fast and convenient.



Kanupriya Gupta
Business Analyst
TCS Financial Solutions (TCS BaNCs)

BLOCKCHAIN- LEVERAGING ARCHITECTURAL PRINCIPLES

HOW THE PRINCIPLES OF CO-EXISTENCE, INTEGRATION AND INTEROPERABILITY CAN ACCELERATE BLOCKCHAIN ADOPTION

The blockchain journey

Blockchain technology is steadily moving from the hype cycle to the adoption stage. As the maturity and understanding of the technology increases, organizations are moving from the experimental/'PoC' stage to implementing the technology for specific business processes, which are likely to be followed by more large scale commercial implementations. Business process innovation will be a key driver of this change and is expected to bring about positive disruption in the way services are delivered.

This journey of blockchain adoption is visibly underscored by strong collaboration amongst all players in the value chain, quite unlike the traditional model where

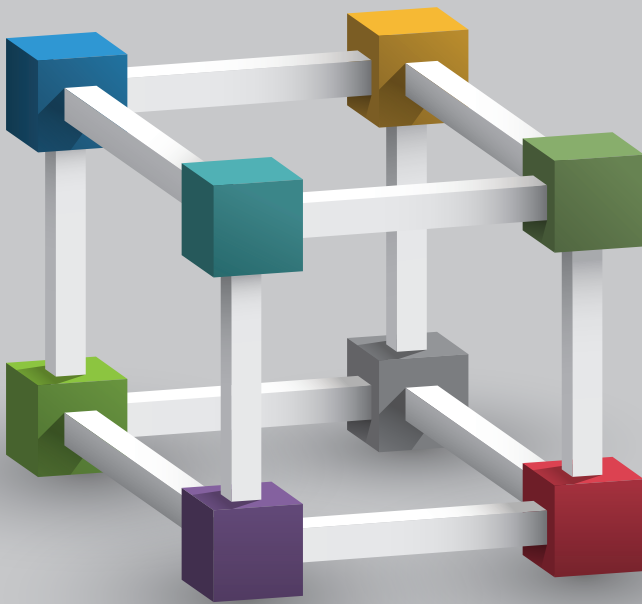
organizations have been known to compete with each other - where secrecy was the norm with respect to the choice of technology, launch plans and even business models. Active collaboration is being witnessed between financial institutions, traditional technology firms, fintechs, and as well as regulators and governmental agencies. Organizations will therefore need to use the right levers of IT, infrastructure and tools, domain expertise and collaboration in order to drive digital transformation of their businesses.

Can architectural principles hold the key to faster blockchain adoption?

As with traditional IT projects, robust architectural principles can

be the key enabler for organizations intending to implement blockchain. A well-designed architecture can provide a strong foundation and aid organizations in embracing blockchain-led innovation in a faster and more structured manner.

Co-existence – It has taken organizations several years to reach where they are today and operate efficiently and effectively with external stakeholders. The journey has been interspersed with regulatory mandates and directives aimed at reducing risk, promoting transparency in business as well as passing on cost efficiencies to investors. Organizations have not only developed specialized platforms, but also invested significantly in enhancing these



platforms and processes over the course of the years.

Any move, therefore, to replace investments of this magnitude is bound to be met with resistance – not only from internal stakeholders but also the ecosystem comprising external stakeholders, regulators, etc. Even more importantly, it is bound to add enormous risks and costs, notwithstanding the obvious benefits that blockchain can bring. Therefore, a prudent approach for organizations would be to leverage the best of both worlds – i.e., existing (systems and technology) and the new (blockchain), while adopting this rapidly evolving technology in a minimally disruptive manner. Co-existence between prevailing systems using

conventional database technology along with blockchain based systems hence becomes a necessity.

Integration – When a transaction needs to be executed in a multi-system context, where one of the systems is being replaced by blockchain, there is a challenge with respect to all systems uniquely understanding the transaction in the same manner. Add to this the fact that there is no 'one technology' as far as blockchain is concerned - there are multiple underlying flavors of blockchain such as the Linux Hyperledger, Ripple, Ethereum, R3 Corda, Chain Core, and Multichain, to name just a few. The choice of the technology which an organization wants to make will therefore depend on the

THIS JOURNEY OF BLOCKCHAIN ADOPTION IS VISIBLY UNDERSCORED BY STRONG COLLABORATION AMONGST ALL PLAYERS IN THE VALUE CHAIN, QUITE UNLIKE THE TRADITIONAL MODEL WHERE ORGANIZATIONS HAVE BEEN KNOWN TO COMPETE WITH EACH OTHER.

THE ABILITY TO ORCHESTRATE MULTIPLE BUSINESS PROCESSES AND SERVICES BETWEEN TRADITIONAL PLATFORMS (SOME OF WHICH COULD POTENTIALLY BE PROVIDED BY MULTIPLE VENDORS) AND BBOCKCHAIN WILL BE A KEY ENABLER OF ADOPTION IN THE FUTURE.

Blockchain – Leveraging Architectural principles

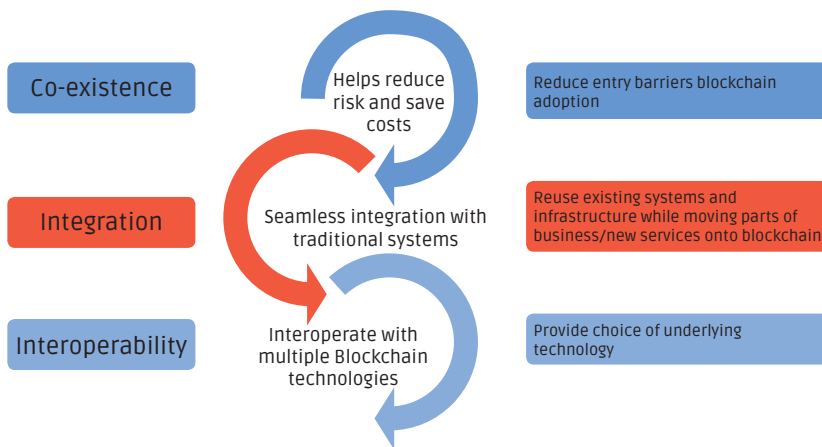


Figure 1: Core Principles of Blockchain

specific use case being explored, further adding to the complexity of integration.

This is especially true for large organizations which straddle multiple data sets and business processes. The ability to orchestrate multiple business processes and services between traditional platforms (some of which could potentially be provided by multiple vendors) and blockchain will be a key enabler of adoption in the future.

Specialized 'gateway' solutions can make a huge difference, in terms, of how existing systems talk to blockchain based platforms. A gateway solution can help remove the complexities of integration, by providing simple API based connectivity between traditional and blockchain based platforms. These solutions can take the place of a dedicated integration layer that is capable of handling the transformation of market standard messages, including ISO15022/ ISO20022, FiXML, and others, into the format recognized by the blockchain platforms. This approach can eliminate the need for large scale and continuous changes to be made to existing systems, even as

new business processes continue to evolve on the blockchain platform.

Interoperability – Data exchange between various blockchain networks will be the first step towards interoperability, which will further extrapolate to transaction flows. Examples of areas where interoperability of blockchains may be actively explored include cross-border settlement, where a CSD may operate a blockchain for domestic settlement while also acting as a node on a blockchain network operated by a foreign CSD. This model can therefore do away with the need to build CSD links, i.e., specific interfaces with the foreign CSD involved in the settlement transaction.

Instead, the transaction can flow from one blockchain network to another and get executed in that network instantaneously, leading to tremendous savings not only in interface development and testing efforts but also in operational aspects – such as through the elimination of reconciliation and reporting. Collaborative models are therefore likely to play a significant role in the world of blockchain technology, which means that interoperability of blockchains

COLLABORATIVE MODELS ARE THEREFORE LIKELY TO PLAY A SIGNIFICANT ROLE IN THE WORLD OF BLOCKCHAIN TECHNOLOGY, WHICH MEANS THAT INTEROPERABILITY OF BLOCKCHAINS WILL BE A CRITICAL REQUIREMENT FOR ORGANIZATIONS ACROSS THE GLOBE.

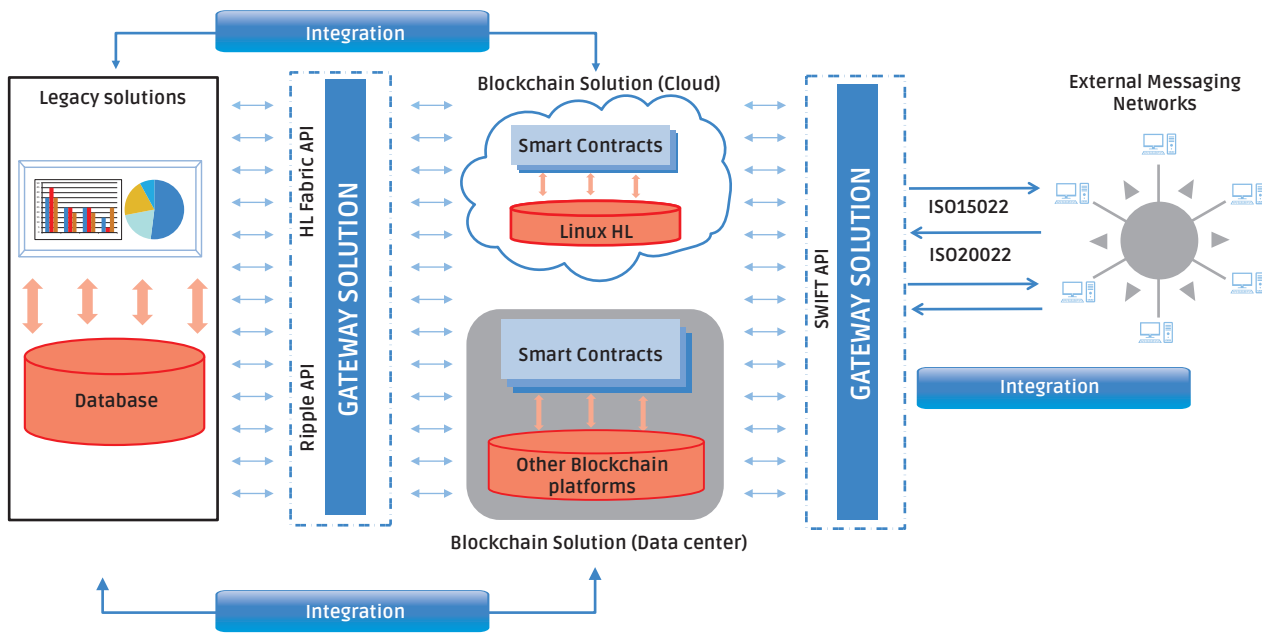


Figure 2: Collaborative models with blockchain

will be a critical requirement for organizations across the globe.

Organizations stand to benefit enormously as a result of the flexibility that the right architecture can provide towards equipping them in harnessing the technology for the most blockchain friendly aspects of business. In addition, blockchain applications as well as tools and development frameworks designed to equip organizations in their roll out strategy must incorporate data security and confidentiality features.

The challenges that exist today in adopting blockchain are real, which organizations cannot afford to underestimate. Tools and frameworks that help drive co-existence, integration and interoperability can provide a strong thrust for organizations looking to integrate blockchain technology into their businesses. They can deliver the following key benefits:

Co-existence

- Re-use of existing, fit-for-purpose platforms where appropriate
- Reduction of risk arising from adopting a technology that is still evolving, for core processes
- Cost reduction

Integration

- Ability to leverage the most efficient technology for a given use case
- Reduced complexity in integration by using specialized gateway solutions
- Achieving end-to-end transaction flow

Interoperability

- Eliminate siloes and share data across networks and ecosystems
- Interoperate with existing messaging networks to benefit

IT CAN HELP REDUCE THE NUMBER OF INTERMEDIARIES REQUIRED FOR A TRANSACTION, PAVING THE WAY FOR SERVICES TO BE OFFERED IN A MUCH MORE COST EFFECTIVE WAY THAN IS THE CASE NOW.

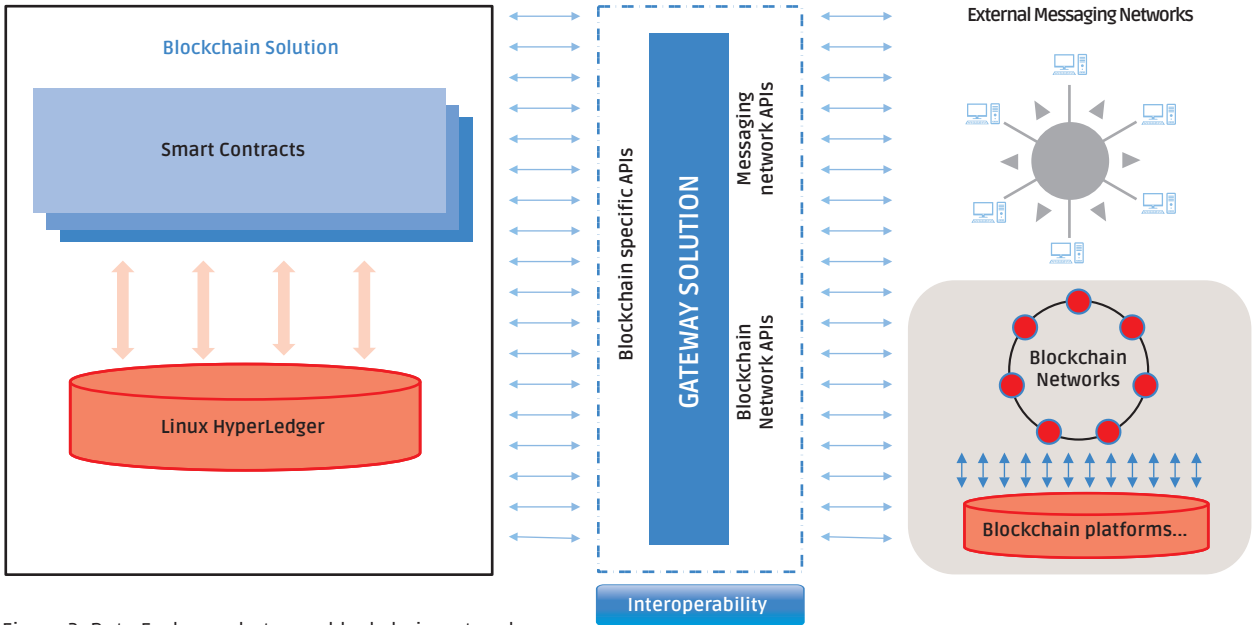


Figure 3: Data Exchange between blockchain networks

from the standardization investments made till now

Blockchain thus clearly holds the promise of revolutionizing the way businesses are run - across a wide range of domains including financial services, banking, insurance, e-governance, and others. It can help reduce the

number of intermediaries required for a transaction, paving the way for services to be offered in a much more cost effective way than is the case now. Importantly, it can help address the 'trust' factor by democratizing the way data is available to all participating entities on the network.

DATA EXCHANGE BETWEEN VARIOUS BLOCKCHAIN NETWORKS WILL BE THE FIRST STEP TOWARDS INTEROPERABILITY, WHICH WILL FURTHER EXTRAPOLATE TO TRANSACTION FLOWS.



Saravanan Prathapkumar
Project Manager
TCS Financial Solutions (TCS BaNCs)



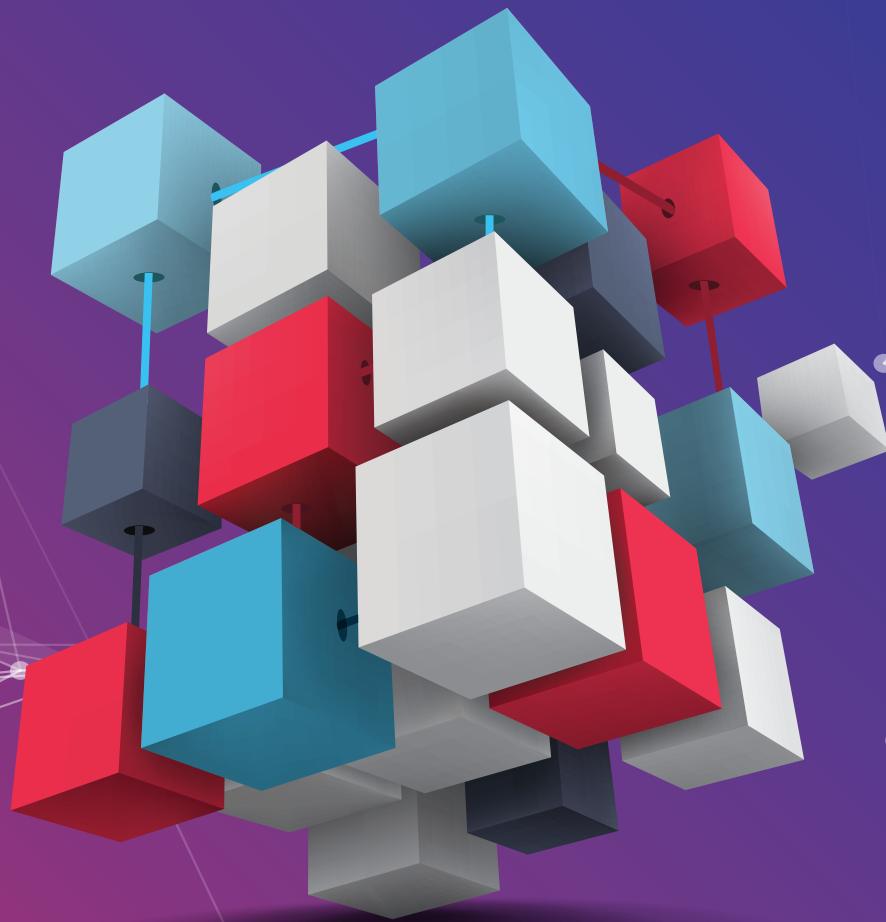
Malini Raman
Product Manager
TCS Financial Solutions (TCS BaNCs)



R Vivekanand
Co-Head and Vice President
TCS Financial Solutions (TCS BaNCs)

QUARTZ

Co-existence. Integration. Interoperability
Quartz Blockchain Solutions



Synchronize data across entities
Build **trust and collaborate**
Eliminate duplication
Settle **instantly**

REGTECH - AT THE CROSSROADS OF FINTECHS AND REGULATORY COMPLIANCE



The credit crisis of 2008 resulted in regulatory norms in the financial services industry going through a significant overhaul. Since then, the regulatory climate has witnessed multiple changes, fines and penalties, and financial services institutions have found the continuous onslaught demanding and challenging. With most regulations being information demanding, financial institutions have been compelled to pay more attention to their back offices and spend significant costs on people and processes for compliance and risk management more than ever before (please see figure 1).

Since then, financial institutions have turned to technology to help them address, deploy and comply with regulations, thereby, giving rise to the concept of RegTech or Regulatory Technology. RegTech

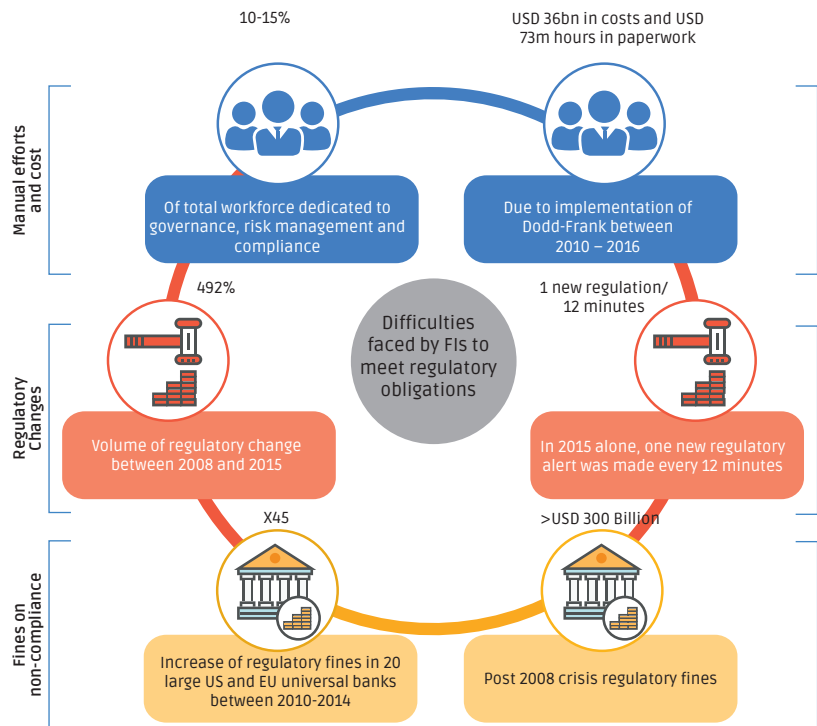


Figure 1

Data Source: FT Research Deloitte McKinsey



REGTECH IS A SUBCLASS OF WHAT IS COMMONLY KNOWN AS 'FINTECH' (FINANCIAL TECHNOLOGY), WHICH INITIALLY INCORPORATED TECHNOLOGY INTO THE FINANCIAL SERVICES INDUSTRY TO IMPROVE OPERATIONAL AND CUSTOMER ENGAGEMENT.

is a subclass of what is commonly known as 'Fintech' (Financial technology), which initially incorporated technology into the financial services industry to improve operational and customer engagement capabilities. RegTech solutions are aimed at gaining significant savings in cost and effort and automatic reporting of the information demanded by each of the concerned supervisory bodies in a more accurate manner.

RegTech is not a single and unique solution all the time. The solution can vary depending on the type of financial institution and the regulatory requirements that they face in their market. For e.g., RegTech solutions catering to regulatory reporting are different from those intended for KYC (Know-your-customer) or AML (Anti-Money Laundering) regulatory compliance.

Technologies Embraced by RegTech

RegTech solutions use new and innovative technological and hi-tech scientific methods such as:

- Machine learning, robotics and artificial intelligence
- Data mining and analytics
- Blockchain and other distributed ledgers
- Application programming interfaces (APIs)
- Cloud computing and Service Oriented Architecture (SOA)
- Visualization solutions
- In-memory data grid (IMDG)
- In-memory computing grid (IMCG)

Characteristics Contrasting Regtech from other Traditional Solutions

Though technology has been used to address regulatory requirements for quite some time, RegTech has the following key characteristics, which differentiates it from other traditional solutions:

- **Security** – Achieved through data encryption and secure transmission channels
- **Agility** – RegTech allows the use of advanced technologies to extract, transfer and load muddled data sets to create useful and consumable information. This gives financial institutions (FIs) the agility to solve real-world issues and stay ahead of the competition
- **Speed** – Quick configuration and generation of reports

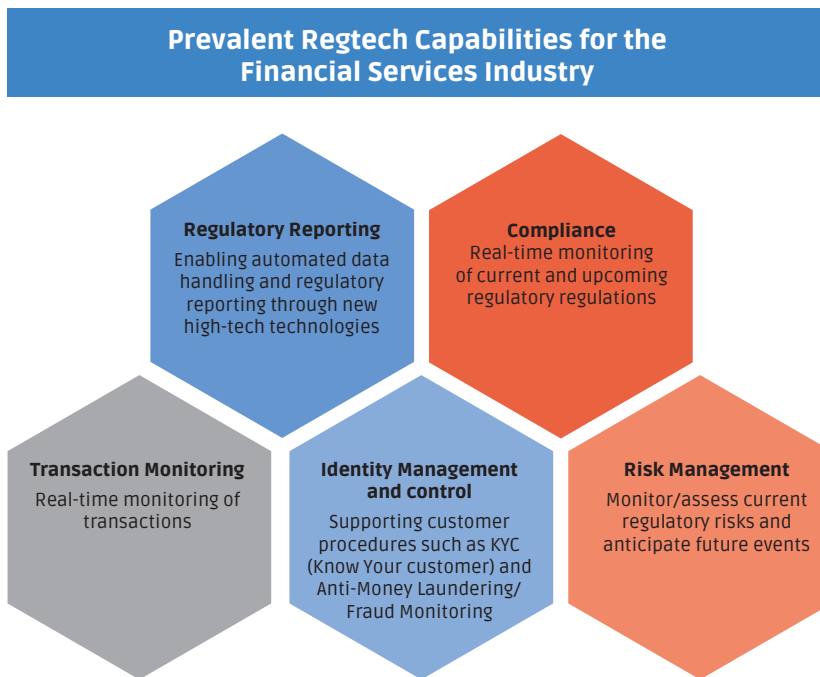


Figure 2

- **Integration** – Quick to market solutions; and, short timeframes to get solutions up and running
- **Analytics** – RegTech uses contemporary analytical tools, which help explore available data sets in distinct ways and extract useful information from it. This information can be utilized by FIs in many ways to make important and strategic decisions.

Benefits Realized by FIs in Adopting RegTech Solutions

External benefits from a regulatory and compliance perspective:

- 1) **Scale down the cost of compliance:** RegTech can reduce compliance cost by automating and standardizing processes, thereby, reducing the need for manual efforts
- 2) **High reporting accuracy:** The automated compliance process results in increased levels of information accuracy, granularity

and availability—achieved almost in real time.

- 3) **Flexibility to adapt to new business changes:** Unlike traditional and rigid enterprise risk management systems, RegTech utilizes sustainable and scalable solutions, which allows FIs to easily adapt to new initiatives/regulations in the market.

Internal benefits - adding value to customers and the organization

- 1) **Meaningful management information:** The advanced data analytics that are an inherent part of RegTech allow for available Big Data to be inspected in new ways resulting in more useful management information and insights. This helps senior executives come up with new strategic decisions and introduce new capabilities, which may give them a competitive edge. For example, Big Data is used

to analyze customers' past and present expenses and transactions to understand their spending patterns. This information can be used by banks to target new products and services only to certain customers (picked based on the spending pattern), thereby achieving the highest possible conversion rate with reduced effort.

- 2) **Identify risks and issues:** RegTech analyses transactional data in various ways to identify money laundering, terrorism financing, etc., thereby, helping firms proactively identify risks and issues.
- 3) **Improved customer confidence:** RegTech solutions can even be leveraged to enhance consumer confidence through better customer experience. For example, a robust RegTech solution can identify fraud and risks and reduce the number of defaults, improving consumer trust or confidence in trading.

Who is the RegTech community?

Regulatory and legislative bodies, RegTech firms and financial institutions comprise the RegTech community. Collaboration between these members fosters synergy, and it is very important for the successful implementation of any RegTech solution to overcome hurdles, such as understanding of complex requirements imposed by regulatory bodies and solution formulation to meet the requirements in an efficient and automated way. Needless to say, joint efforts can also help regulators come up with more effective compliance procedures.

Once a financial institution decides to upgrade its technical platform with RegTech, for the successful

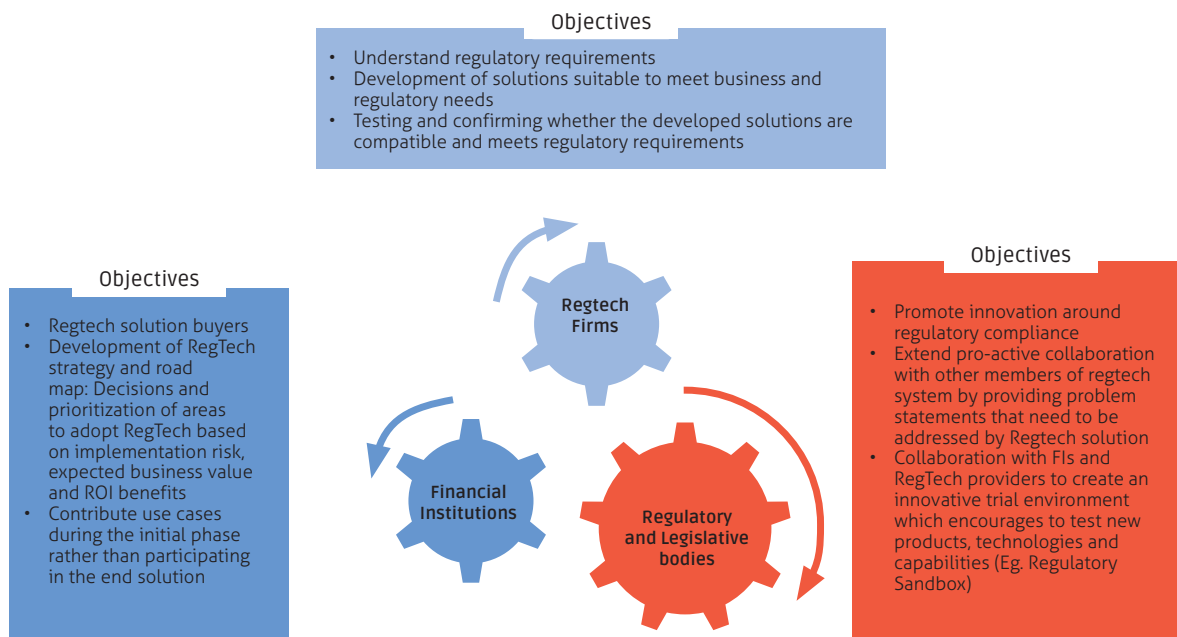


Figure 3

implementation of the same, each of the aforementioned stakeholders are required to get acquainted with the additional objectives as depicted in Figure 3.

RegTech can work only with the support of both legislative and regulatory bodies all over the world. As an initiative to support RegTech, in 2015, the UK government announced that the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), two of their key financial services regulators, will assist to encourage the adoption of RegTech all over the world. One of their latest initiative to support RegTech is a 'Regulatory Sandbox', which enables RegTech firms to test their new capabilities and services in a safe region without the fear of being penalized or fined by the regulator. This means that potentially high-risk capabilities can be evaluated prior to going operational in the markets.

RegTech - Redefining the Custodian Reporting Framework

Though RegTech is a common technology that can be exploited across the financial services industry; for elucidatory purposes, the application of RegTech from a custodian view is detailed below.

Custodians are imposed with a huge burden to comply with new and emerging regulations on one hand and to lower operational costs on the other. Figure 4 lists some of the recent regulations applicable to the US and European capital markets. Each of these regulations may require specific reports to be

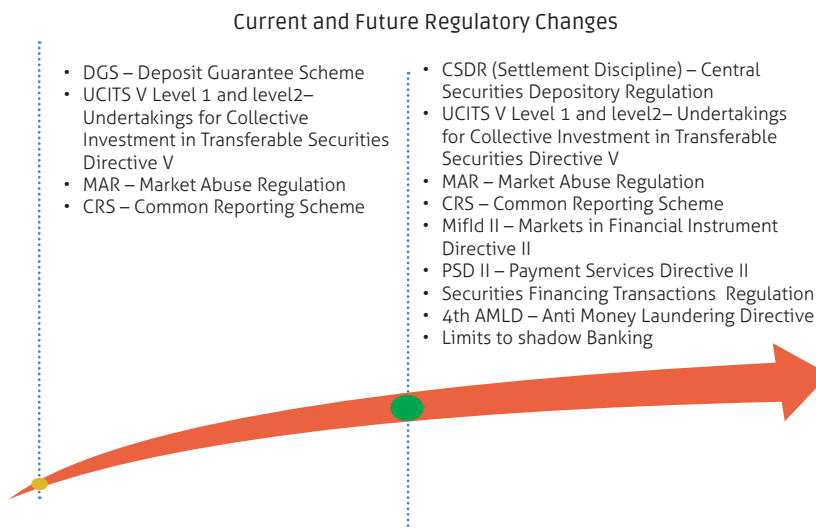


Figure 4

generated by custodians in order to be compliant.

There are several regulatory reporting requirements targeted specifically at a custodian's asset managers and its customers, which require data provisions for adherence. For example, the EU's Solvency II directive demands that asset managers be more transparent by providing clear information on investment pricing, valuation and risk pertaining to the clients that they manage. This in turn is making asset managers push custodians to generate their investment data and valuations along with their source at a more precise and granular level. Similarly, customers are battling to comply with new rules like the EU's Alternative Investment Fund Management Directive (AIFMD), which requires increased transparency around valuation of investments for hedge and other alternative investment funds. This

again puts pressure on custodians to provide the corresponding information. Therefore, to meet a custodian's implicit and explicit global regulatory obligations efficiently and to reduce the cost of compliance and imposing of fines, custodians are forced to restructure their reporting framework and data architectures. Having the aforementioned characteristics, RegTech can help custodians fulfil their mandatory reporting requirements related to most prevailing regulations by managing available data in an effective manner, thereby helping them derive maximum value. RegTech is a cost-effective and energy-efficient way to be compliant with regulations, thereby reducing custodians' operational cost.

RegTech also enables data to be inspected in multiple ways, providing additional insights that can be used to reveal new business opportunities. More accurate

business insights can likely be used to boost business performance, profitability and growth; for example, many times, investors may place a trade, but then later, may change their minds. Big Data mining and insights can help custodians detect such erratic investor behavior and design their processes in a way that clients are not able to revert their trades once confirmed.

Conclusion

RegTech is an emerging concept that is revolutionizing financial services technology, and the community is presently adjusting itself to this new idea. From a market stand point, it is still too early to predict how the concept of RegTech will evolve. Until now, around 80 RegTech start-ups have popped up who are leveraging data mining and analytics, API, machine learning, etc. Figure 5 is a good indication of the potential RegTech market; however, there is

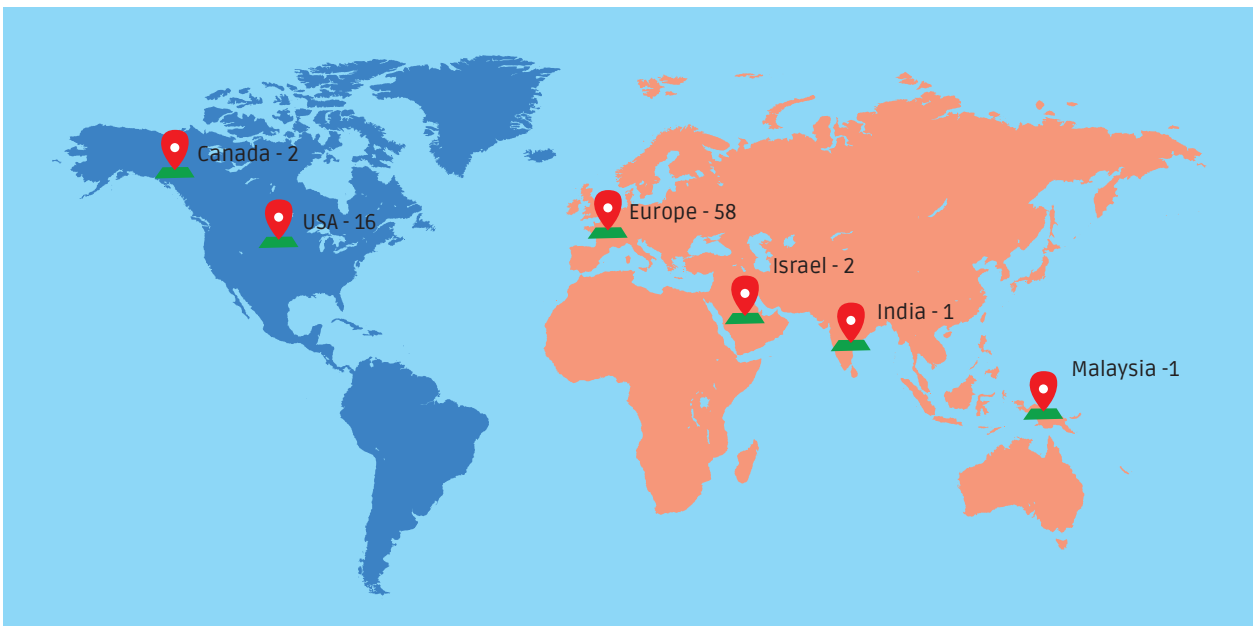


Figure 5: Worldwide Count of Regtech Start-ups

a long way to go for these firms in standardizing the concept and getting their solution validated by the top players of the financial services industry.

Blockchain and artificial intelligence technologies are evolving and slowly gaining acceptance and proving to be reliable, whereas biometrics, APIs, cloud computing are in a mature stage.

While many RegTech capabilities are in a preliminary stage, start-ups (since 2012) have raised 2.99 USD BN in investment funds across 405 deals worldwide (Source: CB Insights - www.cbinsights.com). It is evident that these institutions are fast evolving and growing with speed and confidence. It's surely only a matter of time for a landmark achievement to be made by RegTech in the history of the financial services industry. Now, it's time for financial institutions to buckle up their shoes, analyze opportunities and devise new strategies that add value to their customers while also honing their competitive advantage.

Reference Links:

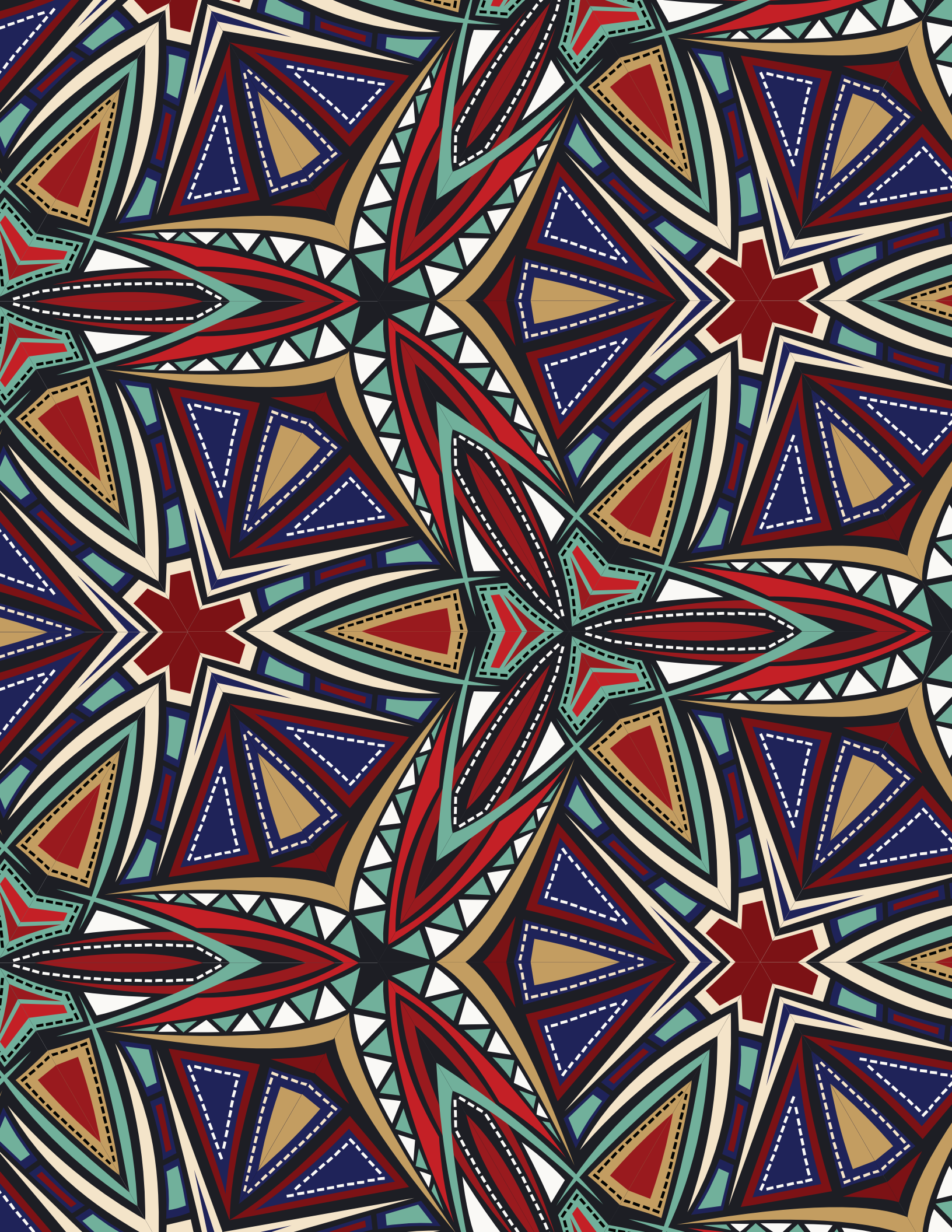
- 1) <https://www.421.se/regtech-time-turn-regulatory-compliance-competitive-advantage/>
- 2) <http://www.bankingtech.com/870331/regtech-features-that-make-data-work-harder-and-smarter/>
- 3) [http://www.ey.com/Publication/vwLUAssets/EY-Innovating-with-RegTech/\\$FILE/EY-Innovating-with-RegTech.pdf](http://www.ey.com/Publication/vwLUAssets/EY-Innovating-with-RegTech/$FILE/EY-Innovating-with-RegTech.pdf)
- 4) <https://letstalkpayments.com/21-hottest-regtech-startups-that-are-defining-the-industry/>
- 5) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf
- 6) https://en.wikipedia.org/wiki/Regulatory_technology
- 7) <http://www.investopedia.com/terms/r/regtech.asp>
- 8) <https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/ie-regtech-pdf.pdf>
- 9) <https://due.com/blog/everything-need-regtech-new-fintech/>
- 10) <http://www.techworld.com/picture-gallery/startups/12-uk-regtech-startups-watch-3648554/>
- 11) <https://news.crowdvalley.com/news/how-financial-firms-can-benefit-from-regtech>
- 12) <https://www.cbinsights.com/research/regtech-regulation-compliance-market-map/>
- 13) <https://www.bbva.com/en/10-keys-understand-regtech/>
- 14) <https://home.kpmg.com/xx/en/home/insights/2017/05/the-transformative-power-of-regtech.html>
- 15) <http://bankingblog.accenture.com/regtech-what-is-it-what-are-benefits>
- 16) https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu_inside-regtech-universe-on-rise.pdf
- 17) <http://hexanika.com/regtech-is-the-new-fintech/>
- 18) <http://tabbforum.com/opinions/cost-of-compliance-2016-handling-regulatory-overload-with-fintech>
- 19) <https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf>
- 20) <https://www.cbinsights.com/research/regtech-startup-deal-geography/>



Dhaarani Ravichandran
Analyst
TCS Financial Solutions (TCS BaNCS)



Sumesh B
Product Specialist
TCS Financial Solutions (TCS BaNCS)



TCS BaNCS Digital



Designed for Financial Services **Ecosystems and Marketplaces**

Omni Channel, Hybrid Architecture

Integrated **Analytics and Enterprise Apps**

APIfication, enabling integration with Fintechs for Banking Services

Conversational AI - Chatbots for banking and securities trading

Data encryption

Secure data exchange



UNDERSTANDING DATA PRIVACY IN THE FINANCIAL SERVICES WORLD

"WE SHOULDN'T ASK OUR CUSTOMERS TO MAKE A TRADE-OFF BETWEEN PRIVACY AND SECURITY. WE NEED TO OFFER THEM THE BEST OF BOTH. ULTIMATELY, PROTECTING SOMEONE ELSE'S DATA PROTECTS ALL OF US."
- TIM COOK, CEO, APPLE

In the wake of recent high profile data breaches worldwide, the data privacy debate has assumed greater significance and assumed center-stage in the regulatory world; and, more so in the financial services industry given the vast amounts of personal data processed by banks/ financial services organizations and their third party IT solution

providers. The customer onboarding process in a bank entails capturing personally identifiable information, and this can range from sharing non-financial data such as names, addresses, e-mail ids, contact and social security numbers to financial data in the form of savings, loans accounts and debit/ credit card numbers.



GOING FORWARD, ORGANIZATIONS WILL REQUIRE STRONGER GROUNDS TO PROCESS SENSITIVE PERSONAL DATA THAN REQUIRED WITH “REGULAR” PERSONAL DATA.

From a regulatory compliance perspective, it is also important to distinguish between personal and sensitive personal data. Personal data relates to information about identified or an identifiable natural person (“data subject”) with particular reference to an identifiers, such as names, identification numbers, location data, and online identifiers, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This also includes financial privacy that refers to the maintenance of confidentiality of customer information about transactions and finances by financial institutions. Sensitive personal data, on the other hand, refers to personal information that reveals racial or ethnic origin, political opinions,

religious or philosophical beliefs, trade-union membership; or data concerning health or sex life and sexual orientation; and genetic data or biometric data. Going forward, organizations will require stronger grounds to process sensitive personal data than required with “regular” personal data.

Cost Implications of Non Compliance

It is also important to understand the costs associated with the data breaches resulting from non-compliance to data privacy regulations. Average costs associated with each breach such as related to its detection, response plans, notifications et al have been rising over the last few years. Implementing a robust data compliance framework that enables adherence to data privacy

regulations can help organizations avoid the costs associated with various data breaches.

There are also huge financial penalties envisaged by regulators for privacy infringements, and serious focus is required to implement and review data governance across an organization, its operations and information systems.

In addition to financial penalties, the industry also faces a significant reputational risk to the business in the event of any personal data breach.

Emerging Trends in Data Privacy in the Face of Evolving Threats

As seen in the preceding section, the banking industry is one of the primary data breach targets due to the perceived value of the underlying data. To capitalize on

emerging growth opportunities, banks need to be flexible in sharing customer data, and it is therefore critical that they achieve a balance between how flexible data sharing can be while also maintaining its privacy. Recently, the “BCG Global Consumer Sentiment Survey” findings concluded that “credit card and financial information’ are the most private types of data, globally.

Globally, there is a paradigm shift in the way the banking is being conducted. The ‘brick & mortar’ type of banking business is being dispensed with through the rapid adoption of digital technology. Increasingly, banks are moving from an ownership model to a cloud infrastructure. In the channels arena, the initiation processes are being regulated directly by the customer (e.g., Internet banking, Cards Platforms, Point of Sale Terminals, etc.) with appropriate security features. There is a visible transition in the banking environment, with the banks (including local cooperative banks) using their front offices for sales promotion, cross selling, upselling and customer service.

There are three emerging trends in data privacy that are being witnessed in the wake of data breaches, i.e., data breach evolution, regulatory focus and technology. Evolving data breach threats are forcing sweeping regulatory changes. With the help of technology, banks are developing and implementing operational and procedural changes in order to comply.

When it comes to data privacy regulation, there rarely is a universal law that is applicable to all. Oftentimes, there is a significant variation between data privacy regulation and enforcement

Data breach evolution

- Increasing threat of external malware programs.
- Growing data breach events due to malicious ‘insiders’
- Breaches due to unintentional user mistakes.

Regulatory evolution

- Increased regulatory focus.
- Harmonization of data protection standards across geographies
- Outsourcing destinations adopting privacy laws

Technology adoption

- Focus on simplifying data protection and controlling costs
- Increasing use of identity and access management solutions
- Using smartphones for cyber security (e.g., Alerts, OTP, etc)

harshness, which makes cross-border data transfers burdensome. While regulations are being adopted by different countries, the degree of intensity varies (i.e., from the most stringent to the least or sometimes, no regulations at all).

In this regard, it is pertinent to make a mention of the European Union’s (EU) Global Data Protection Regulation, commonly known as GDPR, which was finalized after a series of amendments and will be effective from May 25, 2018, thereby replacing the old Data Protection Act and other national data protection laws. The regulation, which aims to provide a legal framework for protection of personal and sensitive data to all natural people based in the EU, irrespective of their citizenship and where the data is processed, will impact all industries that rely heavily on the usage of natural, people related data.

New Requirements in the Data Privacy Regime

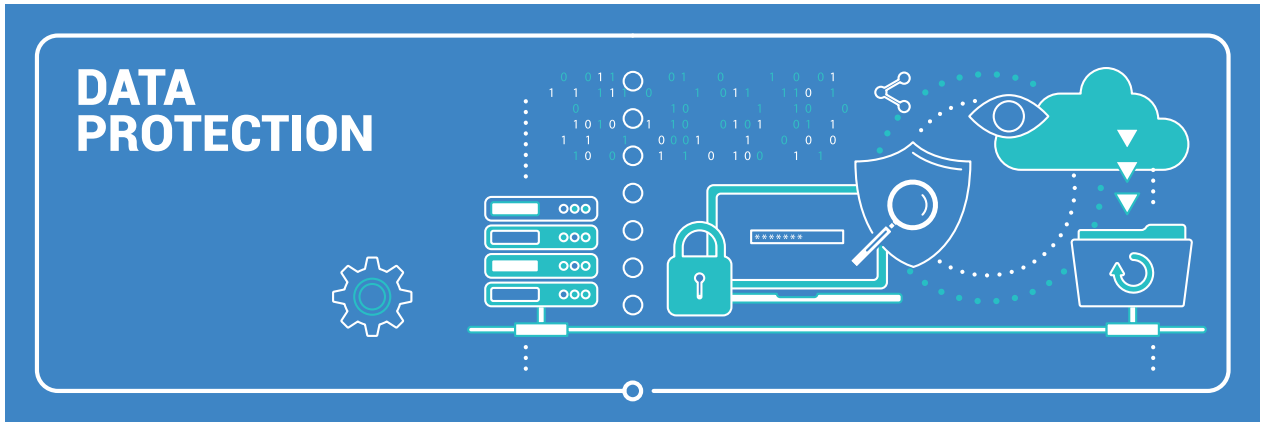
The essence of evolving privacy laws is on the protection and maintenance of a customer’s personal information. It is fair to assume that privacy laws in other regions will also be on similar

lines, focusing on the rights of data subjects and enhanced scrutiny of data handlers. To give a sense of the direction that new data privacy regulations will take, some of the key requirements as envisaged under the EU’s Genral Data Protection Regulation (GDPR) are summarized in chart 1.

OFTENTIMES, THERE IS A SIGNIFICANT VARIATION BETWEEN DATA PRIVACY REGULATION AND ENFORCEMENT HARSHNESS, WHICH MAKES CROSS-BORDER DATA TRANSFERS BURDENSOME.

Chart 1

Chapter	Category	Requirements
1	General Provisions	<ul style="list-style-type: none"> This regulation lays down rules relating to the protection of natural people with regard to the processing of personal data and rules relating to the free movement of personal data. GDPR applies to data processing of EU citizens in their country of residence or a foreign country. Data exchange is allowed only if a country or counterparty is compliant with GDPR.
2.	Principles	<ul style="list-style-type: none"> Explicit consent from customers to process their data. Demonstrate content from customer data both initially and after any correction/ deletion in a structured format, ensuring that there is an audit trail. Special protection for the personal data of children. Data subjects must be informed about the right to withdraw their consent at any time (consent must be as easy to withdraw as to give). Audit log for future references by stake holder/ enquiry/ delivery of data. Data encryption or "pseudonymization" to prevent data breaches.
3.	Rights of the Data Subject	<ul style="list-style-type: none"> Electronic formats and the process of capturing customer consent. Collection of customer data in standard questionnaires to align customer data as well agreements for further processing, e.g., KYC, fraud, marketing. In any case, data is required for KYC, fraud to prevent customer loss and compliance. Automated and secure Information of the data subject in an electronic or paper format Support customer requests for information, correction, and erasure within a month. Notification about subject information in case of requests for information, correction, deletion in a structured form, allowing the channel to process this automated information. Audit trail of notifications for data subjects.
4.	Obligations of Controller & Processor	<ul style="list-style-type: none"> Data mapping is required to be able to determine compliance with GDPR. Gap analysis based on data mapping with GDPR level of compliance. Governance and policies for data protection. Data protection by design and by default. Prevention of attacks via encryption, "anonymization", "pseudonymization", controlled access & data minimization. Accountability, by documenting process flows, privacy controls and decisions made for data protection. Ensure security of processing. Notification of data breaches.
5.	Transfer of personal data to third-party countries or international organizations	<ul style="list-style-type: none"> Standardized reports for use by customer. Restrict transfers of data outside EU with appropriate system validation. Audit logs of data transfer for traceability. Secure transfer mechanism to prevent data loss and its falsification.



Data Privacy Framework

Compliance to data privacy regulations will require a structured approach. Organizations will need to

- Define and roll out a robust governance model to implement data privacy programs
- Review, design and implement a target operating model
- Review current capabilities

of information systems, remediate and roll out upgraded information security systems

To facilitate the above, the program will need to assess current policies and frameworks, processes and IT systems. This will need to be followed by design and development of new policies and processes and, lastly, implemented and monitored through a well-designed program.

Designing Data Security Laws and Governance

Financial services organizations will have to overcome a number of challenges in implementing data protection practices.

Firstly, the key to successful implementation of any data privacy regulation lies in winning trust of customers through a well-defined data security architecture

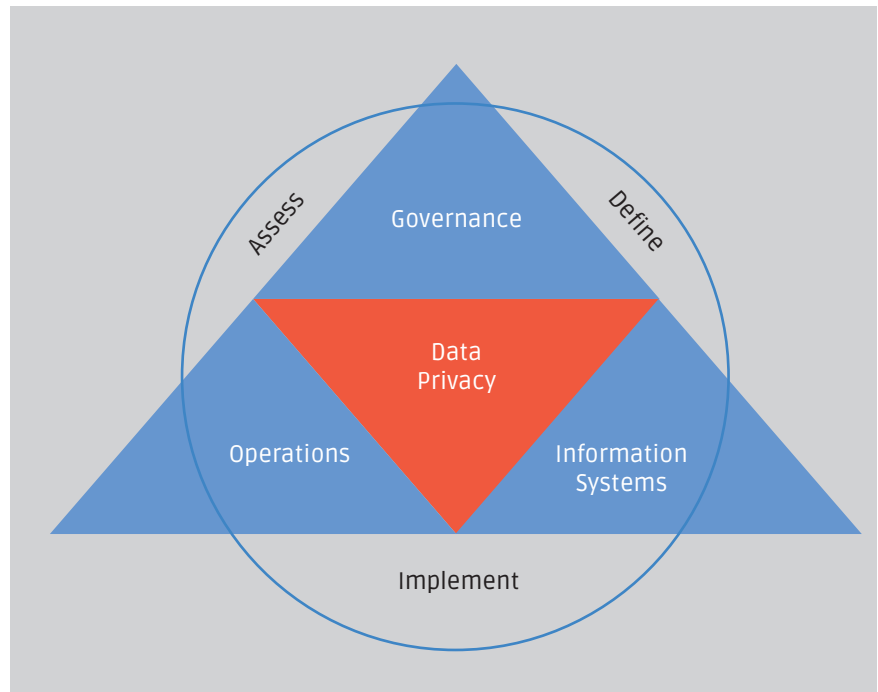


Figure 1: A Data Privacy Framework

Chart 2

Areas	Data Privacy Activities
Governance	<ul style="list-style-type: none"> • Define and implement a data privacy program. • Re-define data governance policy framework, data principles and integrate them within existing functions. • Re-define reporting needs for requisite senior management focus. • Appoint data protection officers. • Design and develop privacy impact assessments. • Review and update partner Agreements for data privacy clauses. • Define and review supplier relationships. • Create awareness across functions within the enterprise. • Develop and roll out a role-based induction program. • Conduct privacy assessments regularly and as and when new products /processes are launched.
Operations	<ul style="list-style-type: none"> • Define templates for data privacy notices. • Define processes for recording consent, withdrawal of consent, correction of stored data, data erasure and portability. • Define a policy for retention and disposal of data. • Integrate security solutions with regular operations. • Establish data audit trails. • Maintain system activity report logs, templates, response records of data subjects. • Maintain data sharing logs, policies, protocols and disclosures.
Information Systems	<ul style="list-style-type: none"> • Assess IT systems' data privacy architectures for new requirements such as consent management, data privacy notices, data erasure, portability and breach notifications. • Remediate and re-design applications to enable prevention controlled access and data minimization. • Define access control points. • Implement automated compliance controls. • Maintain incident logs. • Conduct regular compliance, audit and vulnerability tests.

without compromising on the advantages and benefits of data access and networking. This will pose a significant challenge in implementing data protection by design. Who needs to see the data and to what extent, and who does not need to when carrying out regular tasks will play a key role in designing these laws. Encryption, "anonymization" and "pseudonymization" will assume

significance in deciding the data security design at various levels across the chain. Organizations will also have to balance the needs of shared data access with that of data security.

Secondly, there have been a number of data breach incidents in the recent past where customers' data has been stolen, and this has added to the urgency in revising

data protection laws globally. The EU has taken the lead in repealing older versions, which will be effective from May 2018, and other regions and countries are expected to follow suit. Given the multinational nature of most businesses, especially in the banking sector, the challenge will also lie in stating a multitude of such laws in various forms and understanding the nuances for each



region. Data protection in the EU could be quite different from laws in the USA.

Thirdly, in an environment where outsourcing is the norm, fixing responsibility for liability in circumstances where personal data has been disclosed to various recipients, including third-party countries or international organizations, will prove to be a challenge. The legal agreements between data controllers and data processors will have to review and reflect any changes as per the new data protection regimes.

Finally, lack of awareness among people handling data at various levels is another challenge. People need to understand the importance of data security and own it at all levels. Any data protection compliance program

when implemented will only be successful if people are made adequately aware and educated about its importance.

In Conclusion...

As the dependency of banks on technology is increasing, banks are facing exponentially increasing privacy and security risks to their valuable assets. With this, the cyber-crimes related to banks have also increased manifold even as security mechanisms employed by banks are no longer optimum. A robust data privacy framework is required to provide a safe banking environment to users. As customers become wary of the data security risks, this could also be seen as a key differentiator for banks as they look for growth opportunities. The focus on data privacy will definitely be a key factor in winning customer trust.



Yogesh Sharma
Product Specialist
TCS Financial Solutions (TCS BaNCS)



Nageshwaran R
Product Specialist
TCS Financial Solutions (TCS BaNCS)





APPLICATION OF DATA ANALYTICS IN CAPITAL MARKETS

More businesses today are riding the Big Data analytics bandwagon with the objectives of converting insights---gleaned from huge piles of data--into genuine business advantage. In the retail banking space, unstructured data collected from a broad range of social media sources has resulted in advanced customer profiling and

in-depth analytics that in turn are helping enhance customer loyalty and experiences. However, in capital markets so far, firms have traditionally dealt with structured data sets from limited and pre-defined sources. Big data strategies have now begun to impact a select few areas in capital markets firms over the

recent years, including sentiment analysis for trading, risk analytics, and market surveillance. Data management is now a strategic function within most financial institutions, and regulatory, customer and internal drivers have resulted in firms re-evaluating data related to trading, risk management and operations.

Big Data in the Context of Capital Markets

Capital markets areas typically generate large volumes of data—be it through trading, transactions or operations. However, computing efficiencies and cost constraints limited the management of such data in the past. Today, advanced computing powers coupled with new technologies like Hadoop, Spark, and others have made it possible to have integrated views of data. Regulatory changes, advanced trading strategies, tighter risk management and compliance, complex processing and stricter timelines for reporting are fast paving the way for the adoption of Big Data.

Typically, data strategies can be applied to a whole range of

functions, ranging from front-office trading to back-office processing, surveillance, reference data and support. Many firms today are focused on data-driven initiatives, and are looking to discover unique ways in which data can address prevailing problems or give them a competitive advantage.

Regulatory mandates demand that firms eliminate silos, and this means combining isolated data sets with heterogeneous assets, products and such. In many ways, such strategies are analytical tasks. Audit trails for data underlying risk analytics or pricing of trades are necessary for investors and regulators. The need for transparency in financial markets means that data must be stored and analyzed in a comprehensive

manner, while also keeping costs of managing it low.

Application of Data Analytics in Capital Markets

Big Data projects tend to be implemented in a sporadic manner across capital markets firms. Key areas of focus, keeping in mind the goals of revenue optimization, cost reduction and reporting, are:

- Client Relationship Management
- Market Data
- Risk Management
- Post-trade Processing
- Trading
- Surveillance
- Research

These applications find use in three critical areas - those focused



Figure 1

TYPICALLY, DATA STRATEGIES CAN BE APPLIED TO A WHOLE RANGE OF FUNCTIONS, RANGING FROM FRONT-OFFICE TRADING TO BACK-OFFICE PROCESSING, SURVEILLANCE, REFERENCE DATA AND SUPPORT.

on revenue generation, those aimed at meeting compliance or risk requirements, and those concentrated on cost reduction and operational efficiency.

Revenue Optimization

Trading Analytics

A good example of the revenue generating intent of Big Data analytics is in sentiment analysis. A Big Data strategy can be used to gather and process information surrounding specific markets to create a clear understanding of sentiments that drive front-office trading strategies, as well as to determine the valuation of individual securities. Using this information, traders are able to determine whether various market participants and commentators, including those on social networks such as Twitter or blogs, are bullish or bearish and can then formulate investment strategies accordingly. On a microeconomic level, sentiments and news surrounding an individual organization can be incorporated into valuation methodologies to produce a

fundamental price for a security. By comparing this to the market value, investors can more effectively gauge whether a security is undervalued or overvalued, thereby highlighting potential opportunities for arbitrage.

Trade analytics includes application in areas such as sentiment analysis, High Frequency Trading (HFT), pre-trade decision making, and transaction cost analysis, among others. Due to a cost-driven trading environment, fund managers and buy-side traders are forced to watch every penny involved in transactions, and therefore the increased demand for computerized algorithms. Demand is not limited to mere post-trade Transaction Cost Analysis (TCA); therefore, pre-trade analytics are being used to cover a range of needs, for example, through the analyses of historical, current price and volume data, clients can determine where and when to send orders or realize lost opportunity costs.

HFT is a branch of algorithm trading wherein order execution is conducted at exceedingly high

rates. Here, a burst of small sized orders are sent at very high speed in response to an event. Apart from the built-in memory that is inherent in hardware, it is the algorithm that helps recognize and respond to such nano-second events. With the help of machine learning, historical data is used to find patterns to predict the future, form clusters and perform classification, thereby, identifying particular traits of an event. Proprietary HFT desks try to make profits by acquiring positions that they predict will be profitable based on price movement forecasts. It is the speed coupled with robust and agile data analytics, which provides true competitive advantage in securities trading.

Research

Data analytics can aid the research by generating trading signals (Please see Figure 2) using Time Series Analysis and simulations. Sentiment analysis is used to gather and process information surrounding specific markets

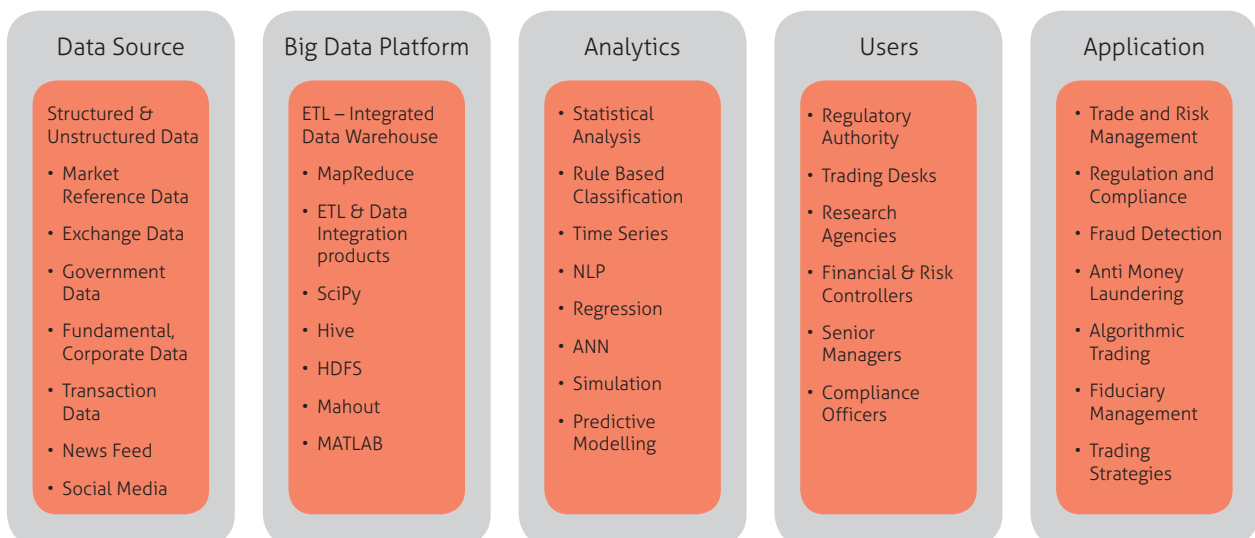


Figure 2: Application of Big Data in Capital Markets Firms

and stocks to formulate trading strategies, as well as to determine the valuation of individual securities. Using information available on news channels, social networks and websites, it is possible to formulate investment strategies. One can evaluate stock placement by comparing created and existing stock prices, resulting in better buy/sell decisions. Being able to provide high-quality research is a service that has helped reinforce client relationships and generate revenue. By the application of analytics and combining natural language inputs with unstructured data engineering across economic reports, monetary policy changes and political events, organizations are gaining the ability to automate manual knowledge-based work. Questions that would once have taken days to research and study can now be answered and visualized in minutes, providing organizations with an automated quant capability.

Client Relationship Management

A single view of the customer can make an immense difference to customer satisfaction levels, thanks to consolidated, rich, relevant and insightful data. A 360 degree view can be obtained by applying analytical insights to data captured at various touch points in the client management lifecycle. This involves classification of clients into pre-defined segments and using of predictive data models to evaluate future client behavior. In addition, advanced analytics can be used to identify subsets of clients-- those which contribute maximum revenue, those that are not served to their full potential or have a high future potential, or for whom there may be no viable economic case for

retention. Analytical data can also identify client behavioral trends such as their propensity to use a particular mode of communication (phone or email rather than post-trade portals) and make last-minute changes to account allocations, thereby, personalizing services and offering dynamic fee packages. Advanced analytics on position and transaction data can identify patterns and trends that inform the next best course of action.

Reporting Requirements

External Surveillance

Though regulators across the world have agreed on the key areas of regulatory design that need reforming, it varies from region to region. Prominent regulations that have an impact in two regions have been the Dodd-Frank Act, Basel III, MiFID II, Solvency II, FINRA Guidelines, FATCA, EMIR, UCITS IV and the FRS9 Standard. Large capital market firms with a cross-border presence face a series of regulations which can be categorized by country, region, international standards and product line regulation. For example, capital market firms in the USA are affected by the Dodd-Frank Act, FINRA guidelines (specific to securities), the Volcker rule and the Consolidated Audit Trail (CAT), and those in Europe by EMIR and MiFID II.

Big data is gaining a strong hold due to the increased scrutiny of data quality in regulatory and ad-hoc market reporting and the need for speed and accuracy. As trading increases and regulators demand tighter scrutiny, the volume of data being created also rises dramatically. Multiple siloed systems can create contradictions and inaccuracies,

further complicating reporting tasks and increasing the cost and timelines involved in generating consolidated regulatory compliance reports. The Dodd Frank regulation requires trade reconstruction reporting for regulatory investigations within a 72-hour period, and this data may be residing in unstructured formats such as voice or text, making Big Data analytics a must. In short, with Big Data analytics, financial institutions are better able to meet compliance requirements, be it in the form of managing unstructured data contained within mails via text mining for surveillance, or the cross-referencing of internal data sets.

Internal Surveillance

Internal surveillance is performed in areas related to fraud and AML/ KYC, market and credit risks, unauthorized trading, employee surveillance, and in continuously monitoring asset performance in businesses that are delivering a higher risk adjusted return on capital investment. This can help evaluate the potential risks and internal and external factors which have an impact on an investment. Data analytics can accurately identify risks and exposure across a trade life cycle and the organization.

Trade surveillance uses pattern based analytics to identify front running and insider trading by gleaning information from various data sources and feeds. Similarly, Anti-Money Laundering and fraud detection can be dealt with models based on pattern identification. Credit scoring, which is a statistical method for evaluating risk of a loan applicant, is another area where Big Data analytics is being applied. As a wide range of information can be generated, multiple variables



can be integrated into more traditional credit rating models to identify hidden patterns that can lead to better and more accurate predictive abilities regarding creditworthiness.

Cost Reduction

Risk recognition

Cost rationalization can occur when fraud and risks are detected in a timely manner. Big Data analytics enables firms to overlay existing information such as client transactions with data gathered from unstructured and semi-structured sources to deliver deeper insights into fraud. Moreover, it is essential for these firms to define a standard for 'normal', so that they can easily flag anomalous behaviour; although, the entire Big Data set is necessary to be able to do this. For example, some irregular activity

can be identified by studying a few weeks of transactions, but with the majority of the cases, coherent patterns emerge from mining months or years of data, making the ability of Big Data to handle large volumes and datasets vital.

Cyber security is another area that can be strengthened by the application of data analytics, by classifying intrusions using data mining and neural network approaches.

Post-trade Processing

Predictive analytics in post-trade processing can help with pre-emptive actions to prevent settlement failures, reducing opportunity costs associated with settlement delays. Analytics-driven failed settlement identification and mitigation can reduce Basel III capital provisions for operational

risk. This in turn can reduce interest rate charges on regulatory capital provisions. Similarly, back-office operational costs can be reduced by identifying patterns, or manual jobs that can be automated; so also, by predicting volumes of trade and trend analyses--all leading to more efficient operations, better resource planning and customer service.

Market Data Management

Data storage for historical trading, internal data management and overall control of reference data are all big tasks in financial services. Inconsistent, incomplete or inaccurate reference data can deter the Straight-Through-Processing rate and create lags in transaction settlement. A large portion of a trade record is composed of reference data, and a significant amount of transaction breaks are caused by

its poor quality. The cost to repair trades and incorrect mismatching are significant, which increases as errors pass through front- to middle- to back-office systems. Organizations have to merge historic and new data to generate insights about delivering better and more cost-effective solutions. Effective reference data management paves the way for developing "golden copies," or single versions of the truth, thus doing away with inconsistent data. It improves the quality and accuracy of data and reduces the need for manual intervention. Consistent data when sent to business units in an organization, can offer a complete and correct picture of financial instruments and their entities.

There are many more areas in which analytics can help, and they are:

- Data quality discovery and profiling - Real-time monitoring and analyses for possible errors from upstream systems
- Data quality management, to continuously maintain the trustworthiness and standards of data
- Data management cycles, where advanced analytics can generate insights in running core operations, for example, in backtracking of costs incurred due to the use of 'bad' data

Conclusion

Growing complexity in the marketplace and the persistent need to comply with a swathe of regulations, is making it necessary for financial institutions to invest in Big Data analytics. The significant role it plays in generating revenue, augmenting the effectiveness of front-office sales and client

retention doesn't require further argument. When implemented in its entirety, Big Data can help institutions go beyond improving risk management, reporting compliance, and operational efficiency, but also in devising better pre-and post-trading methodologies. In short, we believe that there is absolutely no doubt that a revolution in this field is fast imminent.

References

- "Big Data in Capital Markets: At the Start of the Journey", Prepared for Thomson Reuters by Aite Group, June 2014 http://share.thomsonreuters.com/general/PR/Big%20Data%20IB_White%20Paper_Aug2014.pdf
- Big Data and Data Management in Capital markets", Banking Technology, May 19,2014 <http://www.bankingtech.com/221932/big-data-and-data-management-in-capital-markets/>
- Analytics: A Catalyst for Capital Markets <https://www.actian.com/wp-content/uploads/2017/04/SB03-CapitalMarkets.pdf>
- Analytics: Broader Role, Deeper Insight in Today's Capital Markets, Financial Services Strategies and IT Investments, March 2011
- <http://docplayer.net/20127629-Analytics-broader-role-deeper-insight-in-today-s-capital-markets.html>
- Top Ten Trends in Capital market 2017, What you need to Know
- https://www.capgemini.com/resource-file-access/resource/pdf/capital_markets_trends_2017_web.pdf
- Big Data in Capital Markets, International Journal of Computer Applications (0975 – 8887) Volume 107 – No 5, December 2014
- <http://www.ijcaonline.org/archives/volume107/number5/18751-0008>



Ruchi Chauhan
Product Specialist
TCS Financial Solutions (TCS BaNCS)



Mukesh Pandey
Product Specialist
TCS Financial Solutions (TCS BaNCS)





IDFC Bank wanted to diversify its portfolio and increase its urban and rural customer footprint. They found a certain way.

IDFC Bank, a new age bank with headquarters in Mumbai, India, wished to set a new standard in customer experience, using technology and a service-oriented approach. It wanted to diversify its portfolio from corporate to retail banking, targeting both urban and rural under-banked customer segments in India through differentiated services, thereby making banking simple and accessible to all. Tata Consultancy Services (TCS) implemented TCS BaNCS for Core Banking along with a host of additional solutions, including Corporate Loans Origination, Global Limits Management and a Financial Inclusion Gateway. All of this, along with supporting systems such as a micro-ATM helped IDFC Bank achieve its goals, re-imagine its banking services and cater to a broad spectrum of both rural and urban customers. As one of the world's leading financial technology providers, TCS enabled the bank to launch over 11,672 micro-ATMS, increase profits by six times within a year and, thereby, help IDFC Bank live up to its philosophy of delivering banking anytime, anywhere.

Visit www.tcs.com/bancs to learn more or write to us at tcs.bancs@tcs.com



IT Services
Business Solutions
Consulting

TATA CONSULTANCY SERVICES

Experience certainty.



VIEWING CONNECTED THINGS THROUGH A SECURITY LENS



Back in 1999, Kevin Ashton, while working as an Assistant Brand Manager for Procter & Gamble, wondered why a certain cosmetic product always showed “out of stock” on grocery store shelves. This led him on to think of the possibility of a wireless network that could snatch data off a tiny “radio-enabled” chip on, say, a lipstick pack from a warehouse and keep store managers better informed about their inventory. He soon

coined the term “Internet of Things” (IoT) and made a presentation about embedding everyday objects with sensors that were powered by the Internet. Nearly two decades on, human kind hasn’t even begun utilizing IoT to its fullest potential, mainly due to two challenges – privacy and security. Technology has grown to gain insights from data in real time for business outcomes, yet human beings are apprehensive over breach of security and

concerns over confidentiality, integrity, availability and most importantly, the abusive control of personal data. (Trust remains the business currency for the new-age consumer.)

IoT devices have permeated industries, from consumer products to manufacturing processes and public services; however, the banking domain remains at the cusp of influencing consumer financial

behavior today. Who would have imagined the surge of the Quantified Self Movement fuelled by the IoT and wearables industry, collecting raw data continually on various vital parameters and churning them into meaningful insights related to consumer health and fitness, insurance claims processing or flexible interest rates? Many more autonomous banking related IoT use cases have been identified since, such as a cars making payments on user authorization or underwriting decisions influenced by IoT monitoring.

Cross-disciplinary functions seamlessly blend in an IoT-connected ecosystem. It is no paradox to state that the next big thing will actually be multiple, small heterogeneous "powered-things" without a visible user interface, that can handshake data and create a sensor-driven marketplace to drive decisions. Several vendors will offer devices at lower prices, driving the market; however, security and privacy discipline by IoT manufacturers and integrators will have to instil confidence and promote adoption of these ubiquitous devices in mass-market and niche segments. Understanding the threats involved should begin with a breadth- and depth-first approach that can create a security lock as demonstrated in Figure 1.

Banking IoT Use Cases

Corporate Lending – Loan Risk Avoidance

In the corporate lending business, there are multiple functions that qualify for automation such as loan underwriting, reviews and audits, risk analysis and foreclosure avoidance, which are all cost centers for banks. Tech-savvy banks

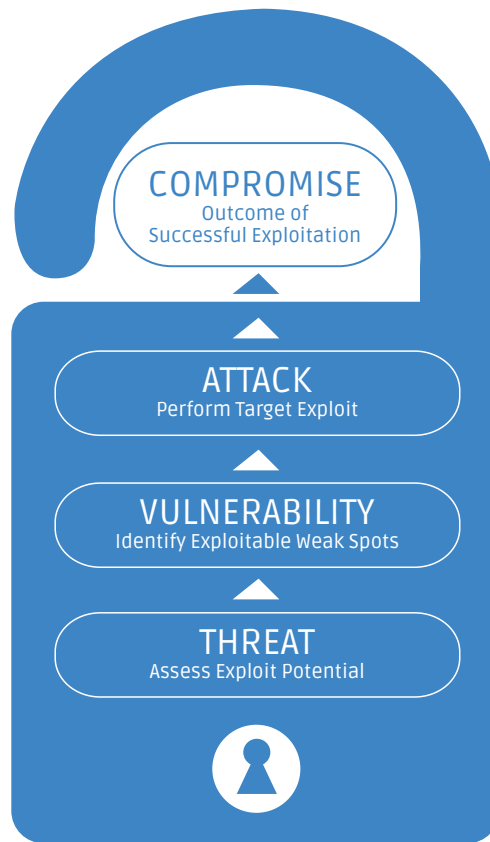


Figure 1: Unlocking the anatomy of an attack

are looking for ways to avoid loan default scenarios (wherein unpaid loan amounts are written off in balance sheets). This is an ideal scenario for IoT that can result in a bank receiving an alert in advance about its Non-Performing Assets. Imagine an industrial scenario where motion, position and GPS sensors are embedded in machinery on which the bank has a lien. Banks can receive alerts indicating stalled industrial production or instances of a plant heading for a shutdown due to being unused. (In some cases, the recipient of the loan may have even planned a resale of the machinery.)

Geo-tagged data can perform risk analysis and stock audit reviews

IT IS NO PARADOX TO STATE THAT THE NEXT BIG THING WILL ACTUALLY BE MULTIPLE, SMALL HETEROGENEOUS "POWERED-THINGS" WITHOUT A VISIBLE USER INTERFACE, THAT CAN HANDSHAKE DATA AND CREATE A SENSOR-DRIVEN MARKETPLACE TO DRIVE DECISIONS.

at scheduled intervals. Movement of stocks hypothecated to a bank can be tracked and credit risk reduced. The purpose of the loan, date of sanction and information about usage can be corroborated to establish the credibility of the customer and their credit score. This in turn can flag off anomalies related to whether a portion of the entire loan amount sanctioned was diverted for unauthorized or fraudulent businesses, or even into tax havens. The system itself can be made to initiate loan instalment payments at periodic intervals with user authorization. Pervasive monitoring can spot financial stress moments at the borrower's end and help with contingency planning.

A question to be asked is whether customers can fool an IoT system by physically tampering with its sensors or intercepting and manipulating them through passive modes, such as scamming with sound waves to feed 'fake' data that can in turn present a scenario where a machine is seeming to be used continuously even when industrial production may have stalled.

Surveillance via Chip-enabled IoT Devices

Possessing a SIM Card is a passport to the land of IoT. There are numerous use cases where SIM cards can be embedded into everyday objects and transformed into IoT devices. Tomorrow, a button, a clip, a binder, a phone cover, a toy, any accessory, gadget or even any part of home decor can be embedded with a chip.

SIM swap scenarios are indicators of a change in ownership of the device, and even fraud. To counter such activities, many banks are experimenting with wafer-thin films stuck onto SIM cards. The film will

install a SIM Tool Kit (STK)-based app, which can be accessed on any mobile even when there is no internet connectivity. Now, imagine this mobile device connected to a wallet that can be dynamically loaded and opened for remote provisioning. SIM cards can come with multi-operator support for enhanced resilience to network outages.

Real-time detection of a SIM swap can block fraudulent use without the need for additional authorization. SIM surveillance can spot users who have evaded loan payments and absconded. But, what happens if the SIM card is cloned? What if one access endpoint is compromised, or the server gets hacked through impersonation and is taken over by a rogue command-and-control center?

Securing in-car Payments with Transaction Authorization across Trust Boundaries

Imagine a common use case of in-car payments at gas stations, parking bays, convenience stores and toll booths. Integration of tamper-proof hardware such as NFCs, embedded secure elements and EMV chips enable cars to make payments by themselves.

A very common attack vector is to encode null bytes into transaction messages that are passed as strings that can get access to system files and resources. What if someone sent a malicious command that took control of the car's bootstrap function and exposed secret keys used for signing the transaction? For an IoT service ecosystem of connected cars, the critical recommendation for a secure endpoint architecture is to implement a trusted computing

WHEN DATA FROM IOT DEVICES IN CONNECTED CAR ECOSYSTEMS ARE TAMPERED WITH, THERE IS A STRONG LIKELIHOOD OF INSURANCE COMPANIES FAILING TO CORROBORATE SENSOR DATA WITH CLAIM REQUESTS.

base to prevent tampering of an application image during Over-The-Air (OTA) firmware updates. It is even more important to establish trust boundaries for separate administrative tasks that can be exclusively accessible with controlled privileges and authorization. Sometimes, car manufacturers can inadvertently expose device identifiers by printing them on the dashboard or etching them on glass windows, leading to metadata harvesting. This could lead to theft of the car or create a loophole in the system, causing unauthorized entry. When data from IoT devices in connected car ecosystems are tampered with, there is a strong likelihood of insurance companies failing to corroborate sensor data with claim requests. Even unsecured Wi-Fi and hotspots in a chain can make so-called secure card payments using tokenization possible, instead of actual cardholder data.

Perimeter Surveillance in Sensitive Environments

In enterprise banking, cash vaults can be installed with IoT sensors to track money movement in a day, including gatekeeper activities. Insider fraud and intrusion can be limited with such perimeter surveillance.

There are several use cases wherein users can hook up IFTTT (IF This Then That) APIs to create automated recipes. Figure 2 demonstrates that the scale of the security risk is as vast as the connections between the Web, mobile, API, cloud, network, data, hardware components, wearables and devices converge. When all of these come together as a chain, albeit a weak one, they can jeopardize the entire system and its participants.

Emerging Focus on IoT Security

Top on the security list is the need to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as impersonating “things” or denial-of-sleep attacks that can drain batteries. Common attacks on IoT include:

1. Denial of Service attacks: Impairs applications, systems and networks by exhausting resources.
2. Malware: Malicious code that interferes with confidentiality, integrity and availability of victim’s data. Examples: Trojan, ransomware, virus, worms, Trojan Horses, logic bombs.
3. Distributed Denial-of-Service (DoS) attacks: Variant of DoS that use bots and distributed hosts targeting a victim’s applications, systems and networks.
4. SQL Injection: Type of database attack trying to lead to unauthorized disclosure of sensitive information via open-ended query constructions.
5. Zero-day Exploit: Represents the window available to an attacker until public disclosure of a security vulnerability.
6. Wiretapping: Without altering information, monitoring or listening to data transmitted over a communication link that can expose sensitive information such as passwords (in clear-text).

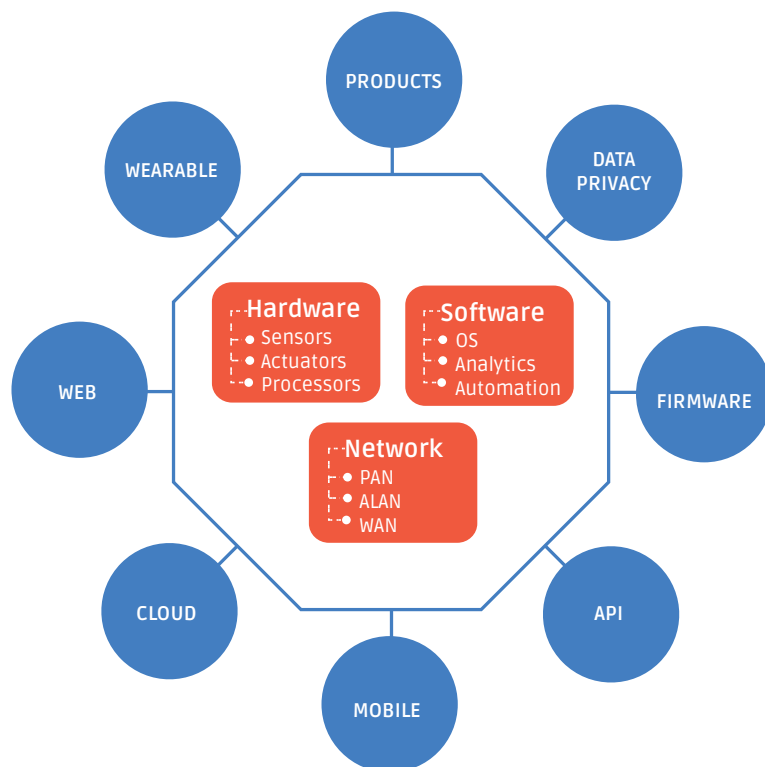


Figure 2: The Scale of Security Risk in an IoT ecosystem

7. War Diving: Use of powerful antennas to search for unsecured wireless networks, as in smart cities, distributed grids or connected-car networks.

The IoT Landscape viewed through a Security Lens

Given the ubiquity of technology and cheap devices available, there is a need for IoT watchdogs to define guidelines to include security as a feature for device/product manufacturers, platform integrators and developers so that the paranoid end consumer of IoT need not be worried about the hijacking of personal data. *(Please refer Open Web Application Security Project (OWASP)'s draft on IoT Attack Surface Areas [4] to understand IoT-driven security challenges.)*

Evolving IoT Security Standards

Several engineers and technologists in working groups have helped evolve security related to the Internet

of Things (IoT) and made privacy recommendations; and, commendable among these include BITAG, OWASP, NISTGSM Alliance, IoT Security Foundation IoT Security Foundation, Industrial Internet Consortium and the Cloud Security Alliance.

IoT Device manufacturers are the custodians of equipment data. Operational data could be raw (JSON/XML) or processed (insights from analytics) inputs from consumers. This data should be protected as per the terms of the license agreement of an IoT contract, and should include who owns what, rights of the licensor and licensee, territorial rights and subjects, rights to sublicense terms, and exclusivity of contractual terms.

From an IoT endpoint device perspective, devices need to possess the following characteristics: low cost and power consumption, longer life and physically accessible endpoints.

OWASP IoT Security Principles

Developing cutting edge security in IoT platforms involves ingrainig confidentiality—integrity-availability elements into the compliance class in products/services and ensuring that manufacturers get their products/services “certified” with prominent marks, seals and icons displayed to the public, and easily understood by the consumer. OWASP’s top 10 IoT vulnerabilities have been available in the public domain since 2014. Every product/service in the IoT system is included for certification and quality assessment. A product/service that fails to comply is declassified and revoked from the market. There is a need to establish procedures for delivery and receipt of personalized security credentials for the devices themselves. *(Please refer to chart 1 that explains the OWASP’s Principles of IoT Security that need to be considered by every component manufacturer in the IoT value chain.)*



Chart 1: OWASP's principles of IoT Security

S No	IoT Security Principles	What they mean
1	Assume a Hostile Edge	Pervasive Monitoring is a threat; assume that attackers always have the edge.
2	Test for Scale	Assume DoS attacks; availability is at stake. Even simple bootstrapping needs to be secure proof.
3	Internet of Lies	Imagine the effect of "Chinese whispers". Misinformation can be be convincing.
4	Exploit Autonomy	Though, this may be the end of human monotony, powered devices now have the full discretion to make decisions on their own.
5	Expect Isolation	Whether connected or disconnected, security as a feature must never diminish under isolation. Devices should function even if the Internet is disrupted. Unplug and quarantine devices, if found infected.
6	Protect Uniformly	Data and metadata are at risk. Protect data in transit, at rest, and in use, always. Every component needs a unique identifier.
7	Encryption is Tricky	Choice of cipher suites, algorithms, key sizes and management throughout the lifecycle have to be considered.
8	System Hardening	There is a need to establish minimum viable attack surfaces; disable unknown ports, unnecessary services; and, delete default passwords.
9	Limit what you can	Deny by default, restrict usage and limit unwanted exposure that is subject to abuse. Provide layered security and access control.
10	Lifecycle Support	Consider on-boarding to recycling, include decommissioning, and full lifecycle definition for all components that are party to a connected system.
11	Data in Aggregate is Unpredictable	Data stewardship responsibility must be defined. Data may seem innocuous, but can prompt unauthorized usage when in the wrong hands.
12	Plan for the Worst	Disasters can be managed if planned for well ahead – Include capabilities that can help re-issue credentials, reset systems, exclude participants, distribute security patches and updates, and so on, even before they become necessary.
13	The Long Haul	Aging of components, extending lifespan, replacement, wiring in a brownfield environment and evolving of standards and technologies.
14	Attackers Target Weakness	Abide by the principle: 'The strength of the chain depends on its weakest link'. Enforce strong authentication and trust throughout the value chain.
15	Transitive Ownership	Sale and transfer of ownership of components should be possible.
16	N:N Authentication	Each component has multiple roles, actors, user privileges and entitlements; Always consider N:N for complex trust, authentication/authorization schemes.

Juxtaposition of Constrained Environments & Stronger Authentication

A deep dive into RFC 7744 [27] (Use Cases for Authentication and Authorization in Constrained Environments), published by the Internet Engineering Task Force (IETF) can enlighten the security

requirements for use cases for varied industries and the same extrapolated to the banking industry.

Golden Rule – Consumer Awareness

Simple human negligence can make artificial or machine intelligence processes vulnerable. An IoT enabled stuffed toy can leak audio/

sound prints of a user, and a hacked lightbulb can break Wi-Fi security. Devices, firewalls or governments cannot be held accountable for a data breach, except for the human beings who have designed them for use. Software patches are a reflection of an afterthought stemming from poor security design. Software can be cracked;



networks can be stalked; platforms can be attacked; and users can be tricked. The insecure web of connected things dons no cloak of invisibility and cyber-attacks are imminent when human beings trade security over convenience.

Building security begins at the top and it is everyone's responsibility – be it an IoT device manufacturer, service developer, product configurator or a platform. End consumers need to be aware of the threat of vectors that seem like invisible data; but, a targeted hijacking could be more damaging than a systemic hack. Consumers and enterprises have fast realized the need for trust as a currency, and products/services teams need to build systems of high reputation and brand value.

Bruce Schneier brilliantly summarizes the necessity to build secure systems: "Amateurs hack systems, professionals hack people".

References

- <http://www.howtoflyahorse.com/beginning-the-internet-of-things/>
- <http://spectrum.ieee.org/tech-talk/telecom/security/smartphone-accelerometers-can-be-fooled-by-sound-waves>
- OWASP Internet of Things Project https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- "Internet of Things (IoT) Security and Privacy Recommendations", Broadband Internet Technical Advisory Group, Nov 2016. [http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf)
- "IoT Security Guidance", Open Web Application Security Project (OWASP), May 2016. https://www.owasp.org/index.php/IoT_Security_Guidance
- NIST Initiatives in IoT <https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot>
- "Internet of Things Security Companion", Center for Internet Security, Oct 2015 <https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf>
- "Strategic Principles for Securing the Internet of Things (IoT)", US Department of Homeland Security,

- Nov 2016. <https://www.dhs.gov/securingthelot>
- GSM Alliance, Feb 2016.
<http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.11-v1.1.pdf>
<http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.13-v1.0.pdf>
- "Establishing Principles for Internet of Things Security", IoT Security Foundation, undated.
<https://iotsecurityfoundation.org/wp-content/uploads/2015/09/loTSF-Establishing-Principles-for-IoT-Security-Download.pdf>
- "NYC Guidelines for the Internet of Things", City of New York, undated.
<https://iot.cityofnewyork.us/>
- "Principles, Practices and a Prescription for Responsible IoT and Embedded Systems Development", IoTIAP, Nov 2016.
http://www.iotiap.com/principles-2016_12_02.html
- "IoT Trust Framework", Online Trust Alliance, Jun 2017.
https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
- "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium, 2016.
http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
- "Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products", Cloud Security Alliance, 2016.
<https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf>
- S Gerdes et. al, "RFC 7744: Use Cases for Authentication and Authorization in Constrained Environments", 2016.
<https://tools.ietf.org/html/rfc7744>

FROM AN IOT ENDPOINT DEVICE PERSPECTIVE, DEVICES NEED TO POSSESS THE FOLLOWING CHARACTERISTICS: LOW COST AND POWER CONSUMPTION, LONGER LIFE AND PHYSICALLY ACCESSIBLE ENDPOINTS.



Annie Thomas
Product Specialist
TCS Financial Solutions – TCS BaNCS





Preparing your enterprise to be available anytime, anywhere

Improved operational efficiency

Optimized costs

Enhanced user experience

Shortened time to more markets

Build your Own Apps

Design. Configure. Brand. Test. Launch.



Domain-aware widgets

Rapid time to market

Low TCO and dependency on IT skills

Easy integration with back-end systems