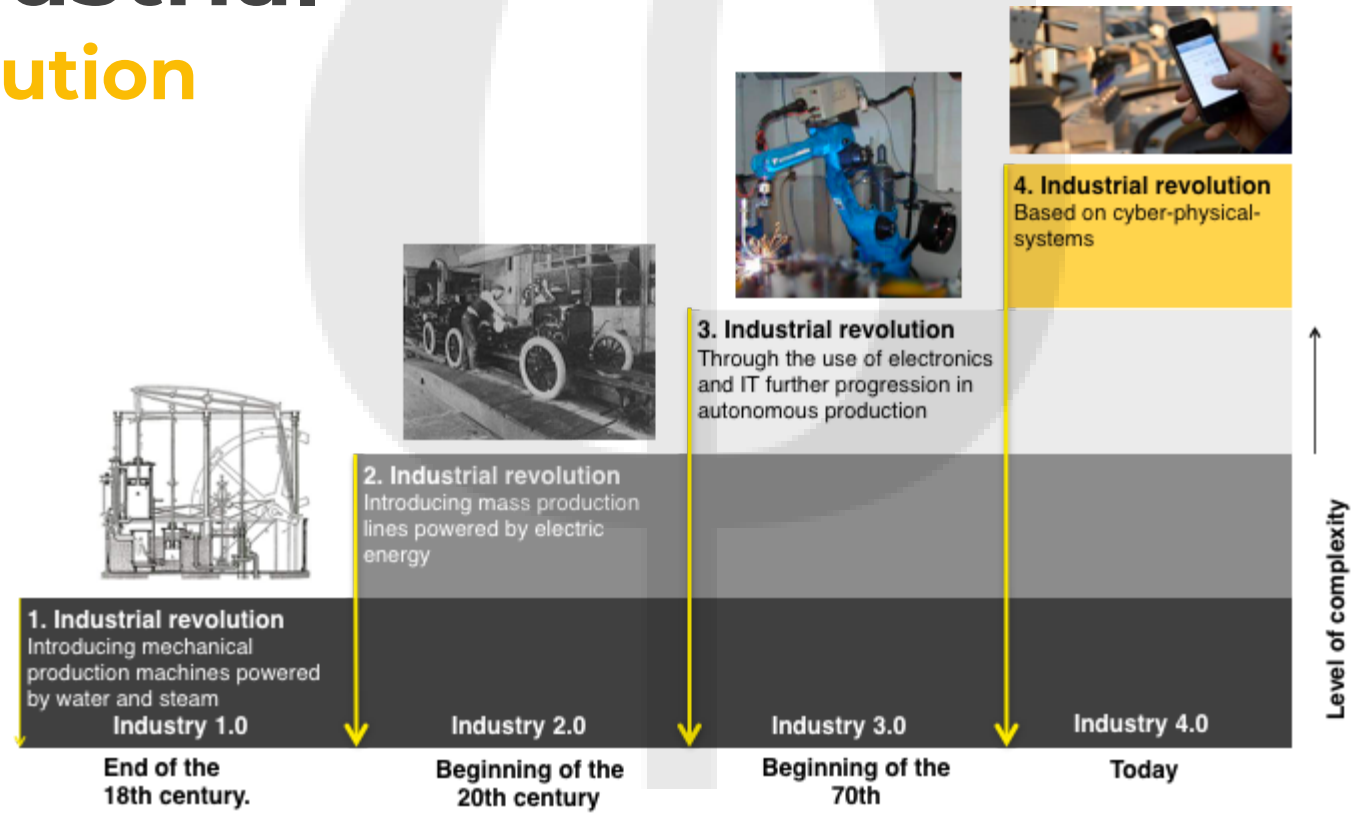
ΦFAI

Federated Artificial Intelligence

Industry 4.0 - Digitization

Need for Cyber Security

Industrial
Evolution



Industry 4.0

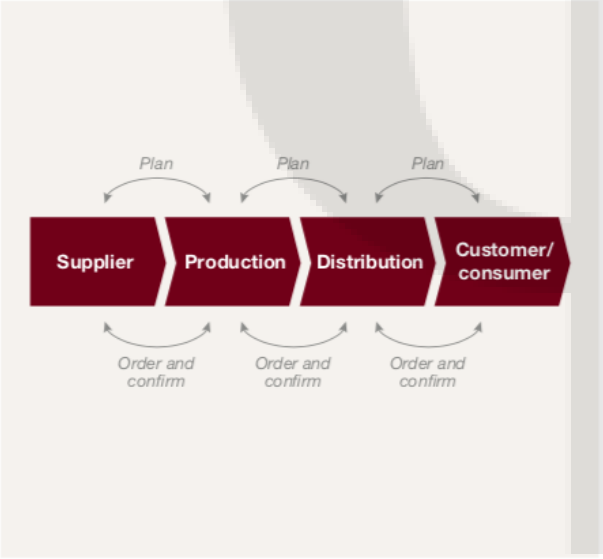
Why Digitization

- **Marketing analyzes customer demand**
- **Predict sales for the coming period**
- **Manufacturing orders raw materials, components, and parts for the anticipated capacity**
- **Distribution accounts for upcoming changes in the amount of product coming down the pipeline**
- **Customers are told when to expect shipment**

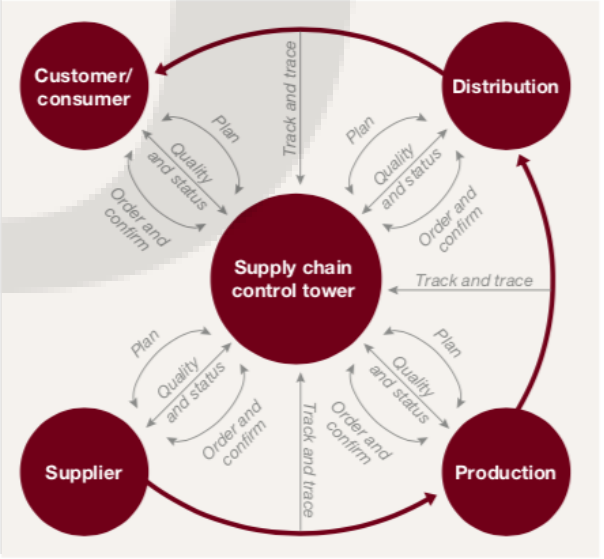
Industry 4.0

Why Digitization

Traditional supply chain model



Integrated supply chain ecosystem

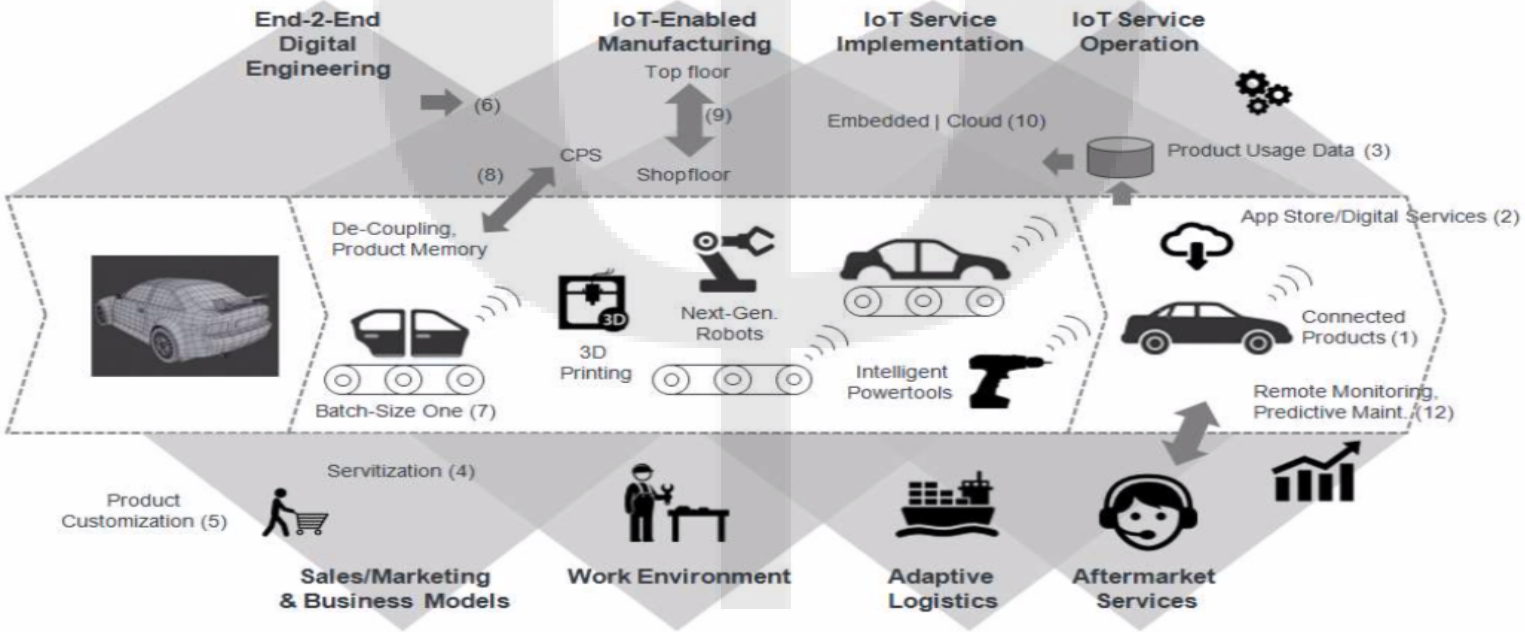


Source: Strategy&

Federated AI

Industry 4.0

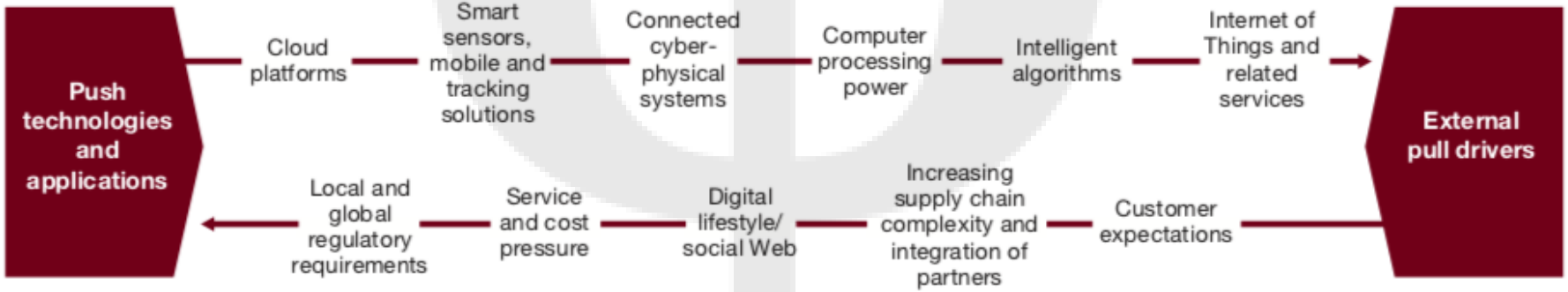
Digitization in Supply Chain Management



Source: EY

Industry 4.0

Pull/Push Drivers

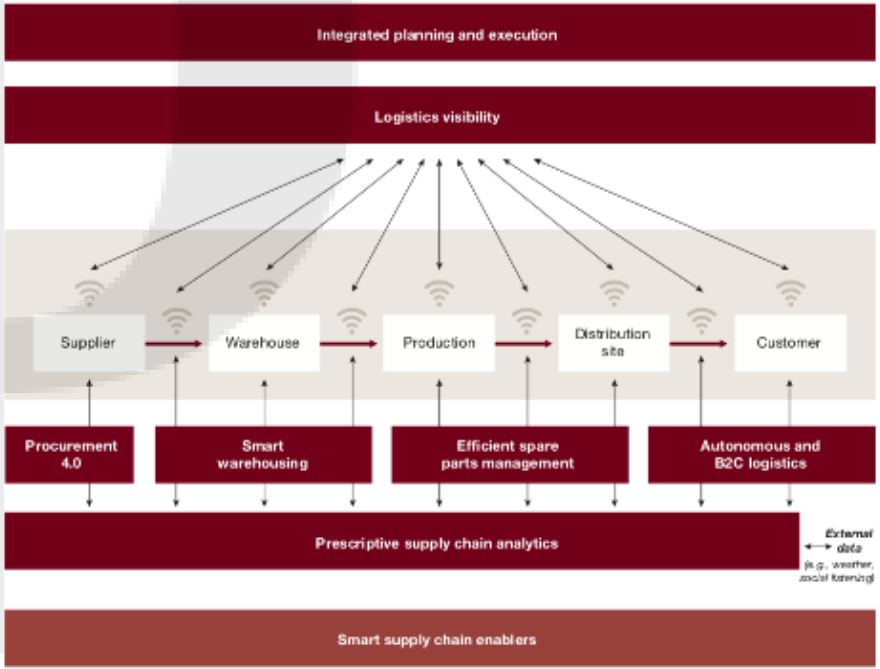


Source: Strategy&

Industry 4.0

Digitization Elements

- Integrated planning and execution
- Logistics visibility
- Procurement 4.0
- Smart warehousing
- Efficient spare parts management
- Autonomous and B2C logistics
- Prescriptive supply chain analytics
- Digital supply chain enablers



Source: Strategy&

Industry 4.0
Digitization

Federated AI

What does it mean ?

- Primarily merges automation with advanced manufacturing to reduce direct human effort and resources.
- Make the manufacturing system a “smart networked factory”, where all activities are digitally controlled and are thus, immutable.

Where it is applied ?

- Catalyst for changes happening in different fields like governance, management and administration of smart cities and other applications.

Why it is adapted ?

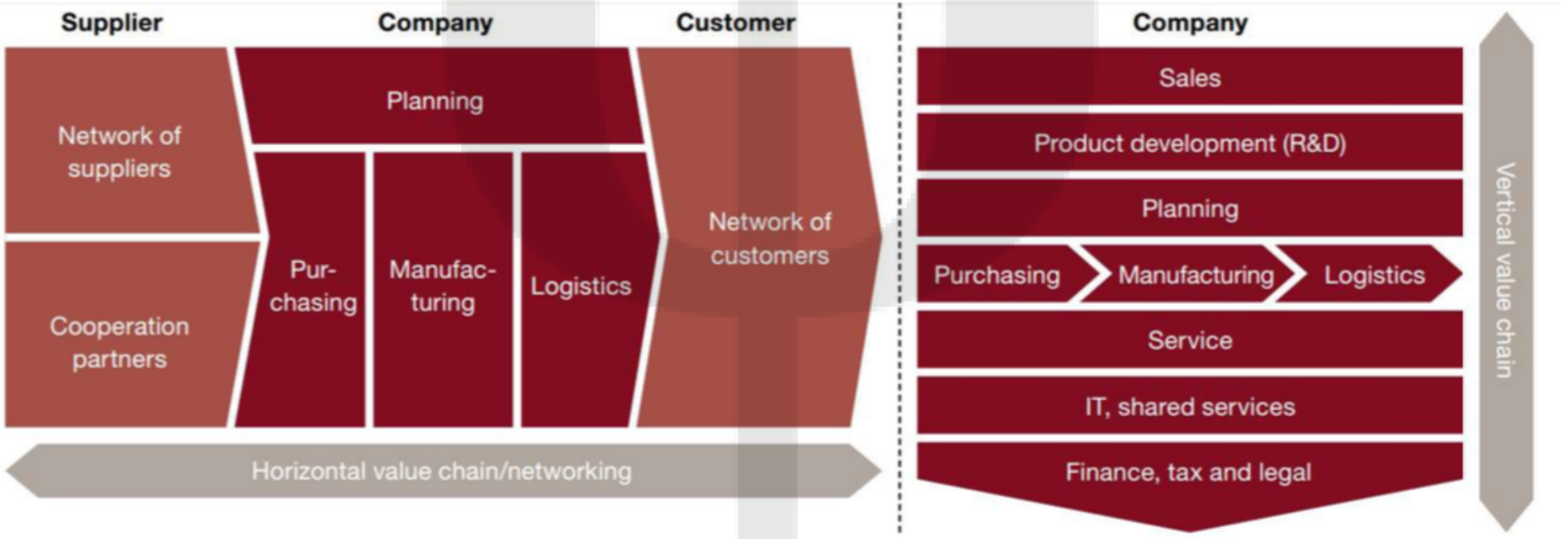
- Organization increasing their digital footprints and adapting the technologies and engagement environments to remain competitive and relevant.

Source: Strategy&

Federated AI

Industry 4.0

Digitization in Vertical & Horizontal Values



Source: Strategy&

Industry 4.0

Cyber Security

Federated AI

Why it is required ?

- As information and assets owned or used by the organization become another node in the network, the attack surface area increases exponentially.

Where it is applied ?

- Should no longer be viewed as a function of information technology or information security alone. It needs to form an integral part of culture and strategy of the organization.

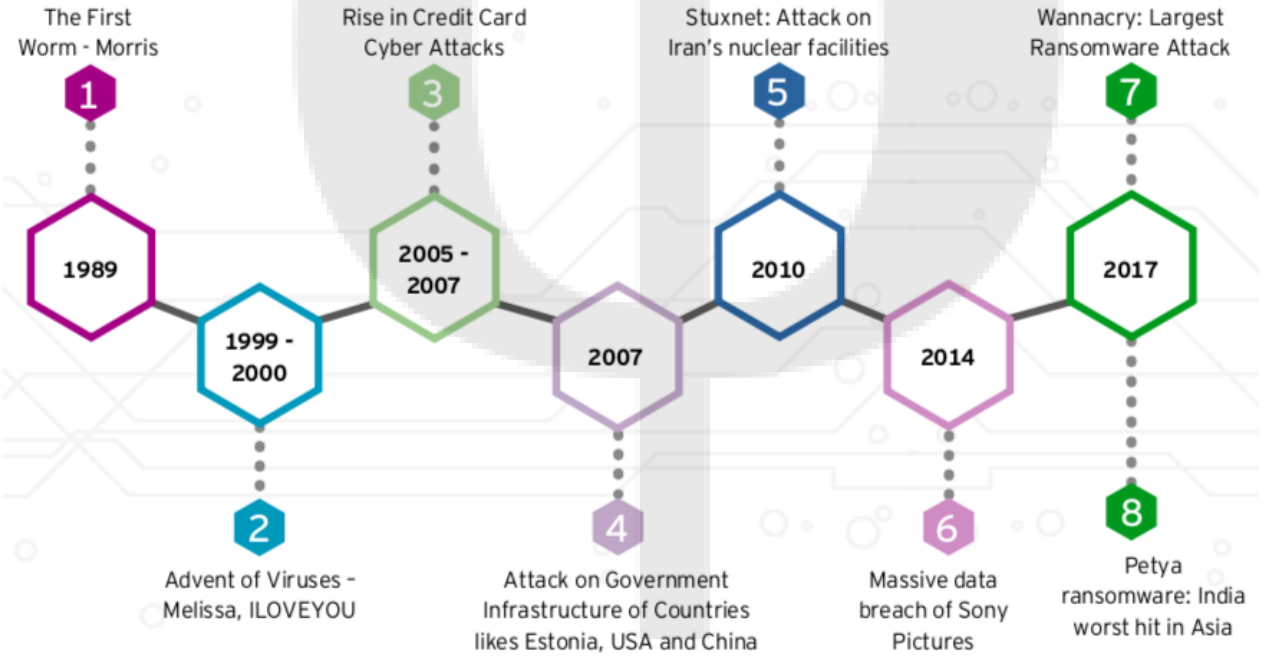
Why it is adapted ?

- Organizations with well-crafted risk management and cyber security strategies are more likely to survive and succeed in the long term

Source: Strategy&

Industry 4.0

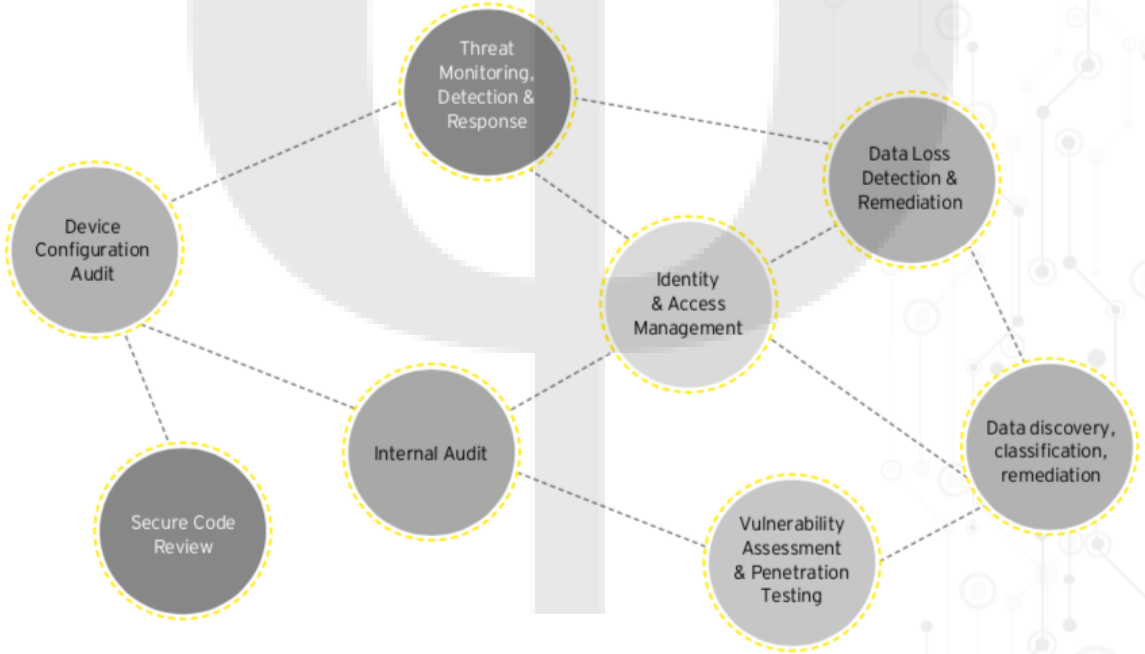
Earlier Cyber Attacks



Source: EY

Industry 4.0

Cyber Security Tasks



Source: EY

Federated AI

Cyber Security Tasks

Threat monitoring, detection and response

- **Allow the systems to monitor a wider range of evolving threat vectors.**
- **Can be carried out without human intervention and allow security administrators to respond in near real time to security events and incidents.**
- **Can track anomalous behavior easily and help in predictive analysis of threats and attacks.**

Cyber Security Tasks

Audit

Federated AI

- Can increase efficiency of configuration management, configuration audit and cyber security audits by removing human errors and biases.
- Reduce the risk in internal audits by reviewing a larger data set.
- Ensures the audit completeness and quality reports.

Cyber Security Tasks

Secure code review

Federated AI

- **NLP techniques are utilized in automated code review for better detection and reporting of bad coding practices or security vulnerabilities.**
- **Automating code reviews can help reduce costs, ensure code health and increase productivity by focusing on the most harmful vulnerabilities.**

Cyber Security Tasks

Access management and network monitoring

- **Security of systems, applications and databases can be improved through continuous learning and updation of rules.**
- **Monitoring network traffic and identifying any abnormal activity and raising alarms or taking pre-emptive actions to block any traffic which can harm the networks or applications.**

Cyber Security Tasks

Data discovery, classification and loss detection/ prevention

- **Enhances the typical Data Loss Prevention (DLP) solutions by automating classification, monitoring and prevention of sensitive data loss by using predictive models to identify sensitive personal or health or financial information and tracking access patterns to these data sets from new/unusual activity from existing sources.**

Cyber Security Tasks

Vulnerability assessment and penetration testing

- **Crawls dynamic pages, detect vulnerabilities which otherwise require human intelligence, thereby reducing cost and increasing efficiency and reducing false positives.**

Federated AI

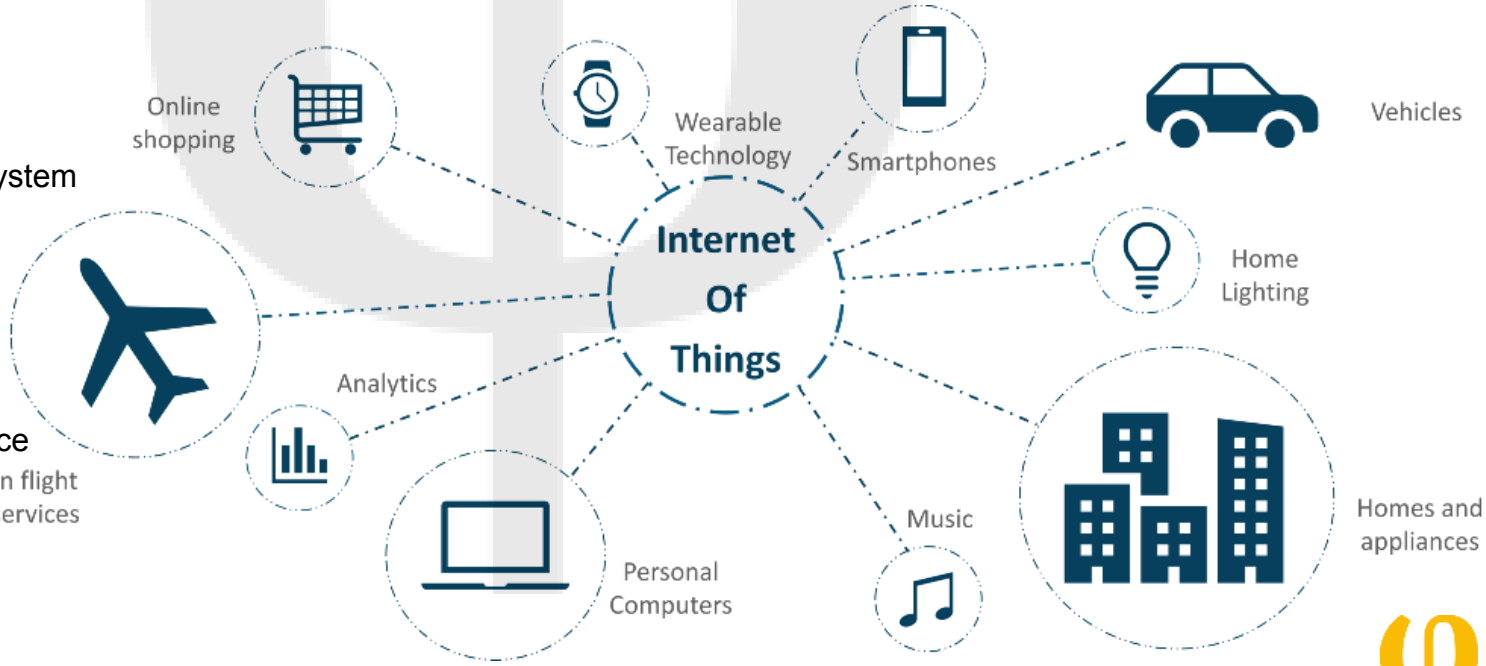
Industry 4.0

AI & IOT perspectives

Applications

IOT - Smart City Project in India

- Smart parking
- Tele-care
- Intelligent transport system
- Citizen safety
- Smart urban lighting
- Smart grid
- Waste management
- Smart energy
- Smart city maintenance



Cyber Security

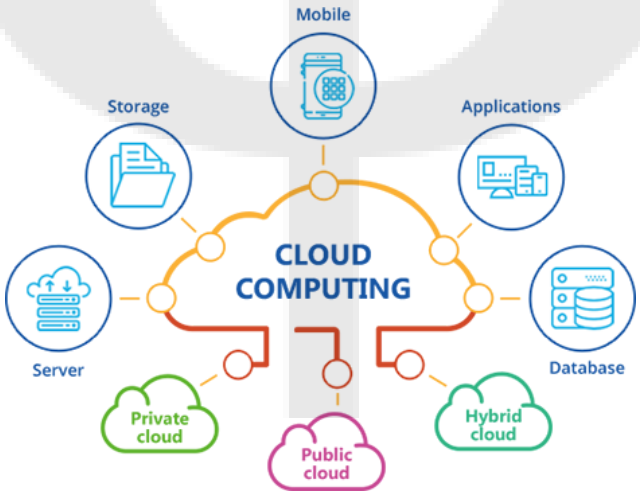
IOT - Privacy and data protection

- The confidentiality of data is often threatened due to lack of adequate security architecture of service providers and lack of user awareness.

Cyber Security

IOT - Cloud computing

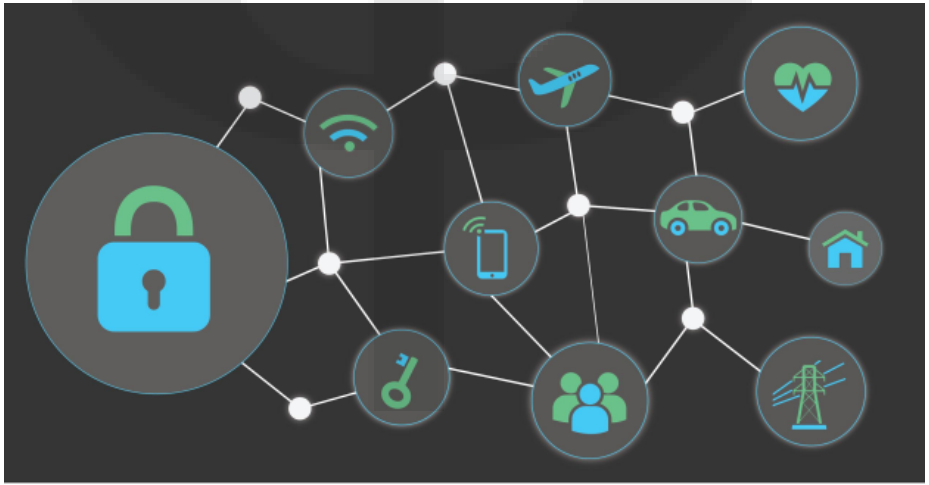
- Cloud provides the platform for devices to be remotely connected and store massive amount of data, hence its security is of a primary concern.



Cyber Security

IOT - Security of devices / Connectivity

- The technology is dependent on physical devices for collection and transmission of data. One vulnerability in a device can compromise the entire network of connected things.



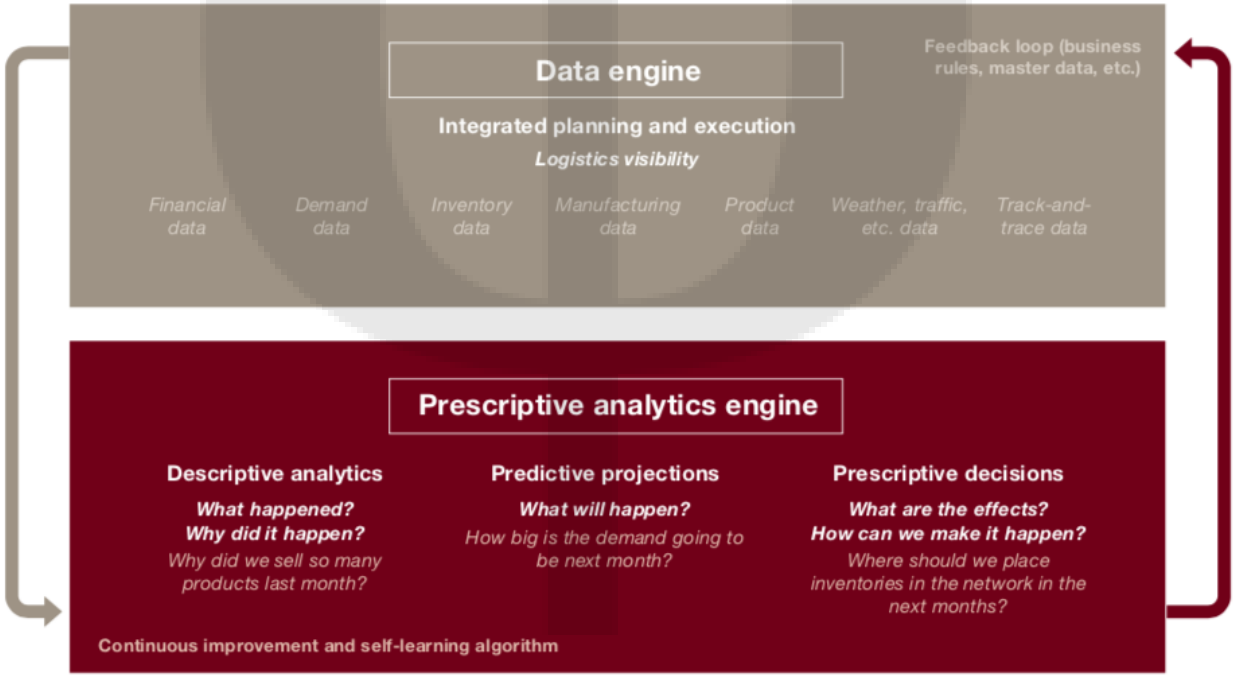
Cyber Security

IOT - Application Risk

- Applications provide another surface area for attack; the weakness in the application can be exploited by attackers.

Cyber Security

AI - Need for it



Source: Strategy&

Cyber Security

AI - Data manipulation

Federated AI

- **AI and Machine learning systems make better predictions by analysing huge amounts of data. But if the learning data sets or algorithms can be manipulated, it can lead to potentially disastrous results for sectors specifically in healthcare, finance, etc.**

Cyber Security

AI - Unauthorized access

- **Lack of strong access control, credential management and privilege account administration can lead to abuse of system functionalities and system availability by accessing the Machine learning algorithm data source and training method.**

Cyber Security

AI - Protection of training data

- **Majority of the training data fed into a system consists of sensitive personal information for services like e-governance, healthcare, finance etc. Hackers can gain access to such confidential data by utilizing reverse engineering.**

Cyber Security

AI - Unmasked PII

Federated AI

- **Personally Identifiable Information in unmasked form being used in an AI platform can lead to compromise of the data. Hence organizations need to ensure masking/ encryption of the PII.**

Cyber Security

AI - Regulatory and compliance issues

Federated AI

- **Although analysis of huge amounts of data leads to more accuracy in providing core services, but getting adequate consent for data collection, processing and storage in order to comply to regulations pose a challenge.**

THANK YOU

hb.bg@fai.services | info@fai.services | +91-7339103001