

DIGITAL CONVERGENCE

From Technology of THINGS to Analysis of THINGS: A Review

CA Vinod Kumar Sharma

Dean, Faculty of Commerce & Management, Rama University, Kanpur

Imagine!

You're on your way home from work and you get an alert from your refrigerator reminding you to stop by the store to get milk and even gives you the directions and also check for the availability of milk in that store

or

Your home security system, that enables you to remotely control your locks and thermostats, can cool your home and open your windows, based on your preferences while you are on your way back home.

All these possibilities and much more are the evolving technological realities that are creating a **DIGITAL ECOSYSTEM (DIGITAL CONVERGENCE OF TECHNOLOGIES)**.

Digital technologies have profoundly changed the ways we do business, buy, work and live. They have altered our society and continue impacting virtually all business functions and industries. It's partially what digital business is about.

With BIG DATA, IoT, Security Intelligence, Neural Networks, Artificial Intelligence and Machine Learning it is very likely that in times to come we may have social media for machines.

Digital technologies that have intensely impacted our interaction with things and devices like never before can broadly be put under the three interrelated and interdependent domains.

- 1. Internet of Things (IoT)**
- 2. Security Intelligence (Big Data)**
- 3. Machine Learning**

1. INTERNET OF THINGS (IoT)

The Internet of Things is the concept of everyday objects – from wearable devices to industrial machines using built-in sensors to collect data and take action on that data across the network. In a way Internet of Things refers to the global network of connected people and devices.

Internet of Things is one of the most important and fundamental technological transformation. The way Facebook has defined the SOCIAL GRAPH, Internet of Things is definitely going to redefine the PHYSICAL GRAPH as one can monitor and control anything virtually from anywhere.

Internet of Things is about intelligent interactions between humans and things for information exchange with a purpose to create value. The Intelligent interactions that make things and devices SMART are driven by 3 things

1. Sensors
2. Connectivity and
3. People

At Consumer level we have

SMART TV, SMART PHONES, SMART WATCHES, SMART CARS, SMART LIGHTS and much more

At Industrial level we have

SMART RETAILING, SMART LOGISTICS, SMART TRANSPORTATION, SMART HEALTHCARE and much more

Not only that we now have SMART HOMES, SMART BUILDING and SMART CITIES

All converging to evolve into a DIGITAL ECOSYSTEM

So what exactly the words SMART means?

If we break the word **SMART** into **SM + ART**

SM stands for SELF-MONITORING and

ART stands for **ANALYSIS** and **REPORTING TECHNOLOGY**

Things that have word SMART prefixed to them like SMARTPHONE or SMART WATCHES have the ability to monitor analyze and report data in real time all that is possible with the presence of sensors and connectivity.

Internet of Things is fast emerging as the most promising reality with tremendous opportunities and possibilities for scaling new horizons in almost every domain.

Experts believe that **by 2020 there will be more than 50 billion IoT things and** devices in operation. This simply means roughly 6 IoT devices for every person on this planet

CISCO estimates market size for IoT to be as big as 14.4 Trillion USD dollars.

Internet of Things beside convenience, optimization, and efficiency offers new sources of data and business operating models that can boost productivity across industries.

Health Care

Wearable devices help in monitoring exercise, sleep, and other health concerns. Patient monitoring devices, electronic records, and other smart accessories offer tremendous potential and can help save lives.

Manufacturing

Manufacturing Industry benefits from IoT the most. Data-collecting sensors embedded in machinery or warehouse shelves can communicate problems or track resources in real time, making it easy to work more efficiently and control costs. Smart Machine monitoring sensors diagnose and predict maintenance issues.

Telecommunications

The telecommunications industry will be significantly impacted by the IoT as connectivity is the basis of IoT operations. Smartphones and other personal devices need to maintain a reliable connection to the Internet for the IoT to work effectively.

Retail

Retail Stores are using IoT for inventory tracking and security purposes and much more to deliver consumers great shopping experience.

Transportation

Smart & Intelligent transport solutions speed up traffic flows, reduce fuel consumption, prioritize vehicle repair schedules and above all save lives. Logistics service providers can track their vehicles using GPS solutions.

Understanding the potentiality of Internet of Things, the next BIG Question is how to analyze this huge volume of data streaming nonstop from sensors and devices across the globe in real time (24x7) potentially so called the BIG DATA.

This Big Data needs to be processed automatically using data analytics to decipher the data, all while IoT devices continue to emit and receive data before it is being stored

To assess the possibilities using these data streams high-performance technologies are needed capable of identifying the data patterns as they occur. Based on the recognition of Data patterns, metrics are embedded into the data stream automatically and adjustments in connected systems

are implemented to the extent that they become capable of initiating alerts for immediate actions and informed decisions.

Essentially, this means with IoT in place we are moving beyond monitoring conditions and inceptions to assessing plausibility of events that might unfold in future and accordingly planning for innumerable **what-if scenarios (PREDICTIVE ANALYSIS - SCENARIOS)**

Is it not very challenging and even dangerous?

Yes, it is indeed as it raises issues related to SECURITY & DATA MANAGEMENT

With **more than 50 billion IoT things and** devices in operation by 2020 and with such massive connectivity SECURITY is going to be a major concern.

So to make the **Internet of Things useful, we need an Analytics of Things.**

We need new data management and integration approaches, and new ways to analyze continuously streaming data.

That brings us to the next level of technological Intelligence to protect the large volume of DATA being produced by Internet of Things.

2. SECURITY INTELLIGENCE – (BIG DATA)

Security intelligence is the real-time collection, normalization, and analysis of the data generated by users, applications, and infrastructure that impacts the IT security and risk posture of an enterprise. The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization.

The data volumes are exploding phenomenally. Data is growing faster than ever before and by the year 2020, about 1.7 megabytes of new information will be created every second for every human being on the planet.

By 2020 our accumulated digital universe of data will grow from 4.4 zettabytes as of today to around 44 zettabytes, or 44 trillion gigabytes.

To understand the magnitude of BIG DATA let's take a quick look at the following facts:

People perform 40,000 search queries every second (on Google alone), which makes it 3.5 searches per day and 1.2 trillion searches per year.

Facebook users send on average 31.25 million messages and view 2.77 million videos every minute.

Video & Photo streaming are reporting massive growth every minute up to 300 hours of video are uploaded to YouTube alone and it is believed that by 2018, nearly 80% of photos will be taken on smartphones.

By 2020, there will be over 6.1 billion smartphone users globally and **50 billion** smart connected devices across the world, all developed to collect, analyze and share data.

Distributed computing (performing computing tasks using a network of computers in the cloud) is going to be the next BIG reality.

Emerging Economies are the largest contributors to the BIG DATA.

US – contributes 23%, China 21%, India – 6%, 15 % Western Europe and 35% comes from the rest of the world.

Every day 2.5 quintillion bytes of data is produced (2,500,000,000,000,000,000) meaning thereby 10 million Blue-ray discs when stacked on top of one another would measure height of 4 Eiffel Tower



By 2020 it is expected to have 50 Billion IoT things and devices in operation. Imagine the amount data that will be generated by these devices. We are at the verge of digital explosion. This enormous amount of DATA offers both opportunities to increase efficiencies and explore new possibilities as well as **THREAT** for getting the vulnerabilities exposed.

90% of the DATA coming from estimated 50 billion devices is unstructured and nearly half of this data is unprotected making it more vulnerable to people with malicious intent.

All this explosion of data is going to create lots of DATA NOISE, so the Big Data generated by Internet of Things needs to be processed automatically with data analytics and high-performance data streaming technologies that can identify the data patterns as they occur and recognize data patterns so that the metrics can be embedded and accordingly adjustments are implemented in connected systems so that they can initiate alerts for immediate actions and informed decisions.

That is what exactly **PREDICTIVE ANALYSIS**.

PREDICTIVE ANALYSIS lays its foundation on **MACHINE LEARNING**.

3. MACHINE LEARNING:

Machine Learning appears to be more concerned with machines but Surprisingly Machine learning is not about machines rather it is a formula, a calculation, algorithm or a model that has the ability to learn patterns in data and then predicts similar patterns in real-time data.

The iterative aspect of machine learning exposes data models to new data to independently adapt. They learn from previous computations to produce reliable, repeatable decisions and results. It's a science that's not new – but one that's gaining fresh momentum

To make the things clearer let's take few examples

Most of us use Facebook and must be familiar with the Facebook recommendations for People we might know aka friend suggestions.

Another Example of Machine Learning is **BEHAVIOURAL ADVERTISING**. Google and other agencies track the links we click and the products or contents we search or read for on the internet and consequently the related company products are displayed as advertisement along the web pages we visit.

Online recommendation and offers like those from Amazon, Facebook are Machine learning applications for everyday life.

Knowing what customers are saying about you on Twitter, that is Machine learning combined with linguistic rules.

All this mean it's now possible with **MACHINE LEARNING** to quickly and automatically produce models that can analyze bigger, more complex data and deliver faster, more accurate results on a very large scale resulting in High-value predictions capable for better-guided decisions and smart actions in real time **without** human intervention.

Machine learning is not new but got impetus in recent times because of the affordable processing and inexpensive storage costs.

Industries operating with a large amount of data, in particular, the Financial Services, Health Care, and Transportation have realized that by glistening real-time data insights they can be more efficient in their operations with tremendous cost saving potential.

The Way ahead

Internet of Things, BIG Data and Machine Learning offers tremendous potential and opportunities, however, our ability to produce data is exceeding far by our ability to produce chips that can process the voluminous data streaming live (24X7) thereby creating a lot of DATA NOISE with less actionable insights. If we look at what happened during 9/11 in America, there were lots and lots of intercepts if reports were to be believed (DATA NOISE) but all that data could not lead to actionable collated information.

With Data explosion and emergence of DIGITAL ECOSYSTEM, Security is going to be a major concern.

References:

- The Statistics Portal. (2017). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). [Online]. Available: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
- IDC. (2016). Internet of Things Market Statistics. [Online]. Available: <http://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/> [3] Bigthink Edge.
- Chen, Daming D., et al. "Towards Automated Dynamic Analysis for Linux-based Embedded Firmware." Network and Distributed System Security Symposium. 2016.
- Schulz, Patrick Koeberl Steffen, Ahmad-Reza Sadeghi, and Vijay Varadharajan. "Trustlite: A security architecture for tiny embedded devices." EuroSys. ACM, 2014, pp:1-14
- Scheel, Ryan A., and A. Tyagi. "Characterizing Composite User-Device Touchscreen Physical Unclonable Functions (PUFs) for Mobile Device Authentication." International Workshop on Trustworthy Embedded Devices. ACM, 2015, pp. 3-13.
- Guo, Fuchun, et al. "CP-ABE With Constant-Size Keys for Lightweight Devices." IEEE Transactions on Information Forensics & Security 9.5. 2014, pp. 763-771