ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 6, Issue 10, October 2018

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Connectivity and IoT: Choosing right channel is necessary!

Biswaranjan Sethi[1]
Solution Architect,
Wipro Digital,
Bangalore, India.

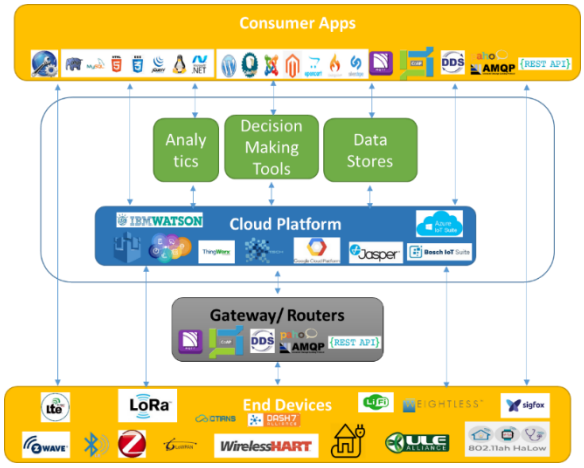
Shreya Solanke[2]
Senior Software Engineer,
Wipro Digital,
Bangalore, India.

Abstract: ***Internet of Things (IoT) is one of the most popular ubiquitous term that has been encompassing wide range of technologies and has a potential to converge the existing ecosystem to a greater degree. When we talk about IoT covering the sky, the backbone of the phenomenon remains the intra and inter connectivity of the entities. A vast and multifarious connectivity models be it traditional short range wireless radios like RFID, BLE, ZigBee, ZWave, Wi-Fi, Li-Fi etc. or the new players like SigFox, LoRa, Thread, LTE Advance, HaLow, Homeplug etc. are trying to establish a place for themselves; the internet service providers are also trying to extend and leverage the already existing network. While IoT talks about everything under one roof, it is essential to understand that one cannot have a single blueprint of the solution that can work in a multitudinous use cases but several reference architectures made against diverse problem statements can co-exist in IoT. To achieve the same, standard working groups of IEEE, IETF and ITU are working to enable technologies matching the rapid growth in IoT. These standards include communication, routing, network and session layers of the networking stack that are being developed just to meet requirements of IoT.***

However, in case of an interoperable seamless mesh of various networking protocol working together, aiming at interconnectivity of Things to things, Things to humans, Things to servers, Things belonging to one module to another frameworks one must consider the challenges too. Interconnected Networks are prone to security breach as well as the autonomy of the networks can be threatened which cannot fit in IoT ecosystem. Another operational aspect of the issue in achieving the same is the specifications of the network's physical components and their functional organizational conflicts for principles and procedures. However, networks being open for interoperation and choices for the right connecting mediums at right places brings the connectivity to a converged point. This can successfully achieve a decentralized, loosely coupled but controlled system architecture. Hence IoT can grow in a better way in case of separate but interoperable contributions rather than one grand plan.

I. INTRODUCTION

The Internet of Things (IoT) is one of the key technology drivers which aims at achieving the interconnection of almost all physical objects to each other and to the humans in order to establish a smarter and efficient ecosystem. What remains at the heart of the system is the mechanisms to connect these objects. There are multiple technologies and standard groups, researchers trying to bring the disjoint systems under one roof and thus avoid redundant developments and design competent solutions. There are many groups who have derived the architecture of IoT. However bringing the entire IoT ecosystem in one pictorial representation is prone to miss most of the integral parts of the system. The architectural framework defined here promotes cross-domain interaction, aid system interoperability and functional compatibility.



IoT Ecosystem: Figure shows a generalized framework of IoT Ecosystem. The bottom most and the top most layers represent end entities of the applications is various domains like smart home, smart health, transportation, smart grids etc. The bottom layer represents the data generators. There can be numerous types of sensors sensing various physical parameters, electric utility meters, wearables, audio and video surveillance devices connected over any of the communication protocol listed. Second layer from the bottom represents the gateway and is a crucial component when it comes to establish connections in between the low power constrained devices to the external worlds. The typical standard communication protocols supported by them are shown in fig. The third layer is a big block which can be considered as the mastermind of the system which is responsible for storing the generated data, consume it for decision making, run some machine learning algorithms and apply data mining techniques in order to make it useful for users etc. The top layer is nothing but a counterpart of the bottom layer who consumes the features built using the data. Based upon the data in cross domains, the patterns are observed and same are available to be consumed by cloud services and thereby to end devices via gateway. Each of the above with the respective communication channels are discussed in details in subsequent sections.

II. Building Blocks of IoT Ecosystem and Factors Affecting Their Choice

1. let us discuss the fig.1 in depth in subsequent sections:

1. End Devices

End devices, edge devices or simply the sensors can be redefined as the data generators of the IoT ecosystem. The data can be value of any measurable quantity such as temperature, humidity, percentage of Hydrogen in air, heartbeats, the number of units of electricity consumed by a particular house etc. Typically these devices are Low power bandwidth constrained devices capable of sending a data of few bytes at regular interval. They ae expected to work with coin cell batteries for several years. Hence, the choice of right communication channel becomes essential.

There are many standard working groups with IEEE, IETF, ITU etc. and industry SIGs that are building standards to achieve highly durable low power connectivity. Along with the new standards, the existing popular standards like ZigBee, Wi-Fi are working towards supporting IoT requirements of the connectivity devices. Lot of new work and lot of rework is happening in order to meet the connectivity requirements of the end devices. Standards like LTE Advanced, ZWave, ZigBee, BLE, 6LowPAN, Weightless, SigFox , LoRA, Li-Fi, WirelessHART, Wi-Fi, Homeplug, HaLow, Thread, DECT, DASH7 etc. gaining popularity in various types of application domains. See **Table 1.1** for a quick comparison at a glance against common parameters like data rate, power consumption, connectivity range, network topology and respective ideal application domains for each.

2. Gateway

Gateway is responsible for aggregating the data received from various devices connected over any of the protocol mentioned in above section and transmit it to either server or cloud storage or any decisive application running over cloud. Since Gateway send this data over internet protocol and IP based communication channel must be chosen with utmost precaution. The communication channel has to be hassle-free, bandwidth efficient capable of working with constrained hardware. It should also be capable working with storing the data for certain interval so that it can send data once connected to Internet in case of energy constrained devices. The footprint of the protocol and QoS are other two aspect that are good to be balanced when we chose communication channel.

With diverse application domain and use cases, there becomes a room for accommodating one or more messaging protocol. In IoT space various messaging protocols like MQTT, CoAP, AMQP, DDS, XMPP, STOMP, Mihini/M3DA, LLAP, LWM2M, SSI, SOAP, WebSocket, Reactive streams, HTTP seems to be suitable for different type of applications.

Refer **Table 1.2** for quick comparison of these protocols against the dynamics listed in above section

3. Cloud

IoT Cloud Platform can be well defined as set of fully managed and integrated services that allow you to easily and securely connect, manage, and ingest IoT data from globally dispersed devices at a large scale, process and analyze/visualize that data in real time, and implement operational changes and take actions as needed. There are multiple factors which play crucial role while choosing a right IoT Cloud Platform viz. device management, Integration, security, protocols supported for Data collection, types of analytics and support for quick visualizations and ease of operations. The IoT Platform must maintain the information about the devices being connected in order to support their intrinsic and extrinsic operations. Another important aspect when enormous number of devices, managed under different categories, are data privacy and security. Security at both, data in transit and data at rest is equally important and there must be techniques supported to achieve both.

Most of the IoT Platforms do support Basic operations and comparisons over the data. However, with the growing intelligence and demand, Support of analytics services is very important. Based upon the domain and use case, one may be interested in either real-time analytics or batch or predictive analytics or even in interactive analytics. The continual learning of the analytics algorithms is essential. **Table 1.3** gives an insights of major IoT Platform service providers and their comparison against above discussed parameters. Many Open source IoT Platforms like Kaa, Devicehive, The Things network etc. are also providing services that are essential to build (See **Table 1.4)**

.Consumer applications

IoT embodies convergence of the virtual and physical worlds. It is a vital nerve between device-oriented sensor network and data-oriented applications facilitated by Internet connectivity. One of the major goals of IoT remains instituting connectivity and smartness amongst the physical entities in surrounding, may or may not be internet enabled as of today. The connectivity and data collection becomes passive and dumb if not visualized and utilized in real-time or near real-time frame. The system has to facilitate remote monitoring and control to the end user and consumer.

Consumer applications are tightly coupled with cloud platform chosen in system as for most of these applications, data available in cloud; be it raw, processed or analyzed; is source. Depending upon the use case, deployment environment, data confidentiality, security visualization of data can be made available in the form of dashboards or mobile applications or intra-web applications etc. In case of critical applications like healthcare, a piece of data can be made available to the doctor and only a certain can be consumed by the patient. Thus, availability of the data over public channels or private channels dominates choice of communication protocol.

III. Factors Impacting Choice of Right Communication Channel While Building an IoT Solution

IoT is all about establishing communication between various entities in the ecosystem of particular use case. For example, in case of a Smart home solution, the ultimate aim becomes to be connected to home from anytime, anywhere. While achieving this goal, one has to choose how are end devices connected to the home gateway, how is home gateway transferring data to the cloud, what cloud is being used, how is the cloud data being made available for the user and how are the actions suggested by the user are being communicated to the actuators and devices at home premises. At every step, one must choose communication channel wisely. Both intrinsic factors and extrinsic factors are of equal importance while making choice.

Depending upon the layer of connectivity, the network autonomy and necessity for security factors impacting the choice of communication channel differ. In case of end devices, communication among the on premises devices, predominantly end devices, gateways and associated application services, the communication may occur in ad-hoc or timely manner. However, most of these devices are resource constrained. Thus, dynamics like processing necessities, power consumption, and bandwidth requisites are dominant while choosing the right device. However, the external factors like field of deployment, probability of interferences, number of end nodes to be deployed to collect all vital data and to cover full premises are very decisive. Along with these factors, design must consider need for strong security and autonomy of operation. For example, a manufacturing plant of medical equipment. Gateway can appear complex choice for many of the factors playing a vital role. Gateway can be constrained resource with limited storage, power and processing capability or may be a hi-end powerful processor with continual power support. There has to be heterogeneity as the choice of the gateway is more use case and domain centric. The choice of messaging protocol, for establishing communication with cloud and the other counter entities, is most affected by the security implementation of the protocol. As the data may be travelling over private or public channel, it is prone to theft in either of the cases. Thus a gateway must be chosen keeping these critical parameters and scenarios consideration.

The third side of the pillar is interoperability of the communication channels avoiding all the possible interference and bandwidth overlap. Many of the solutions are vendor specific as of today which soon will transform into interoperable and flexible systems. While choosing the communication channel in any end to end IoT solution, it is good to follow the principle of neutrality. The principle of neutrality essentially points to the freedom of actions instead of promoting any perspective. That what is a building block of intelligent and self-dependent networks which also makes a major impact on data privacy and protection.

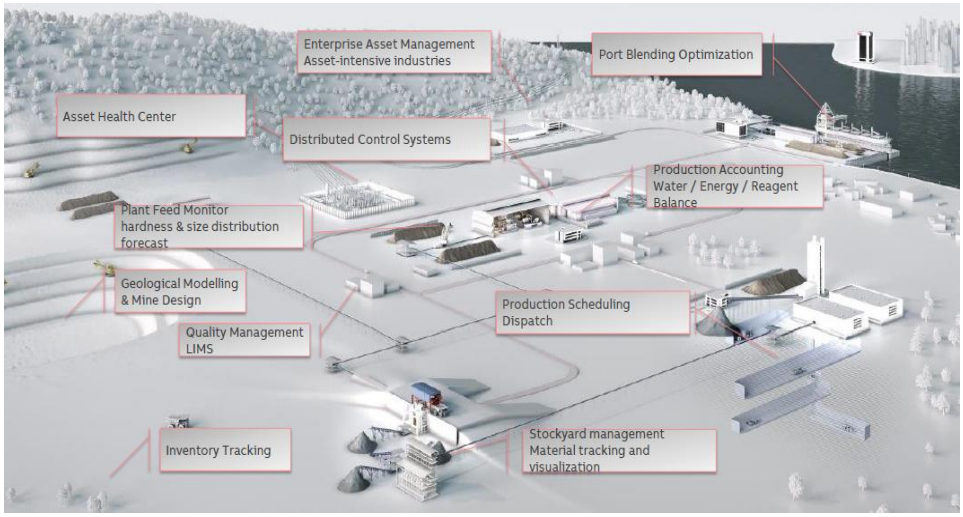
IV. Case Studies

ABB's Ability IoT Solution in Mining Industry

The Internet of Things is a primary catalyst for transformation in many fields like Home automation, healthcare, industrial IoT etc. Mining Industry is no exception and is aiming at leveraging the benefits of IoT. Mining can be done both surface and underground. It involves multiple operations and processes depending upon the ore extracts and the subsequent process. Many Tech giants like Rino Tinto PLC, Montego Resources, and Angelo American are enhancing the mining to be done in smarter way than harder way. The major problems faced by mining industry as per one of the surveys by ABB Group are harsh climatic conditions, safety issues, lower grades, energy costs, remote locations, islands of automations and value chain gaps. From IoT perspective the major challenges is establishing the connectivity between the remotely scattered mining plants and their operation centers.

The ABB's Ability IoT solution for mining not only aims at seamless connectivity between the workers in the fields, sensors at premises, giant machineries via usage of right communication protocols at right places but also utilizes this data for predictive maintenance, effective asset monitoring. The solution enhances security standards of the people working at the field, makes their lives smarter and also welfares the business. It also takes care of diagnosis and process optimization in mining lift

operations thus increasing productivity. Figure below shows various part of system that the solution implements among various nodes in mining is achieved using ABB's Ability solution.



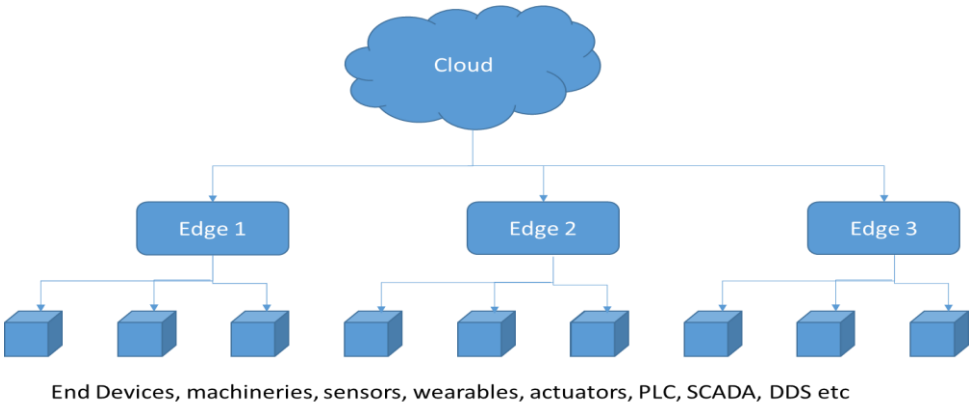


Figure 2

However, in most of the solutions shown above implement the basic connectivity mechanism as shown in fig 2. The connectivity amongst the end devices and edge gateways can be achieved using either of the suitable communication protocols stated in above sections. ABB Ability also allows Intercloud communication with many popular platforms like GE Predix, AWS Lambda etc.

2: How Verizon's strategy of connectivity is helping it to grow business?

With the already existing wide range of connectivity, Telecomm service providers like Verizon are making their way to sustain in market in profitable way. As per the Q3 17 reports. Verizon's revenue from IoT services increased by 17.4% YoY to reach approximately $229 million. According to the CEO, 5% of the IoT revenue comes from connectivity services offered by Verizon. They are number one in market with practically achieving connectivity

For Instance, in city of Columbus and Ohio, it has been able to create seamless connectivity of yellow taxis by providing a dedicated mobile app that connects to nearby taxis using cellular network. Where it only leverages software solution in this case, in the city of Sacramento, California, it provides free Wi-Fi across city. The other Connectivity services of Verizon like facilitating a dedicated private network in order to achieve secure connection to cloud in case of crucial applications like healthcare, are gaining popularity and many non IT industries are happily adopting these services.

V. CONCLUSION

IoT ecosystem has capacity to incorporate different type of reference architectures as per the desired use case. It also accommodates multiple connectivity protocols at multiple layers like end devices, Gateway and cloud. However, choosing a right communication partner becomes essentially important in order to achieve resource optimization and enhanced security. There are various intrinsic and extrinsic Factors that dominate the choice of the communication channels. These factor vary based upon the communicating entities and respective requisites of those.

References

1. https://new.abb.com/docs/librariesprovider78/eventos/jjtts-2017/presentaciones-peru/(edgard-de-olazabal)-digital-mining-integraci%C3%B3n-de-activos-y-procesos-en-mineria-en-la-era-iot.pdf?sfvrsn=2
2. https://www.youtube.com/watch?v=UzHbS63JMHQ
3. https://www.youtube.com/watch?v=He7kqk6rv6Q
4. https://www.irjet.net/archives/V3/i12/IRJET-V3I12239.pdf
5. https://sigport.org/sites/default/files/Enabling%20Heterogeneous%20Connectivity%20in%20Internet%20of%20Things%20A%20Time-Reversal%20Approach.pdf
6. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1750

Appendix A: List of Tables

Table 1.1: Comparison of messaging protocols

Protocol	Abbreviation	Functional model	Typical header size	Security	QoS	Silent Features
MQTT	Message Queue Telemetry protocol	TCP based Pub/Sub model	2 byte	TLS/SSL	QoS 0 (At most once) QoS 1 (At least once) QoS 2 (Exactly once)	low bandwidth, high latency, data limits, and fragile connections Small footprint
CoAP	Constrained Application Protocol	UDP Based Unicast/Multicast/Broadcast request response oriented model	4 byte	DTLS	Quality of service with confirmable message	M2M communication in constrained environment, security, low header overhead and parsing complexity, URI and content type support,
AMQP	Advanced Message Queuing Protocol	Message oriented Pub/Sub model	8 byte	SASL or TLS	QoS 0 (At most once) QoS 1 (At least once) QoS 2 (Exactly once)	Efficient, portable, multichannel and secure
XMPP	Extensible Messaging and Presence Protocol	XML based data transfer	NA	Hop-by-hop end-to-end Encryption	NA	Access control, a high measure of privacy, hop-by-hop encryption, end-to-end encryption, and compatibility
SOAP	Simple Object Access Protocol	Web services enabled XML based messaging service	One or More	WS-I Basic Profile	NA	can also be used over SMTP, JMS and message queues, allows tunneling,
WebSocket	NA	TCP based bidirectional full duplex protocol	NA	TLS	Origin model used by web browsers	Efficient, portable, extensively used and secure

Table 1.2: Comparison of Communication protocols used by end devices predominantly

	Standard	Operating Frequency	Range	Power Consumption	Data Rate	Network topology	No of nodes that can be connected	Ideal Application domain
LTE Advance	IEEE 802.16	1850MHz to 3800 MHz	Few miles	High	~1Gbps	HetNet	Few hundreds	Smart City, field specific networks
ZWave	ITU G.9959	900MHz	~30 meters	0.71uW/bits	~100Kbps	Mesh network	232	Smart homes
ZigBee	IEEE 802.15.4	2.4GHz	~100 meters	185.9uW/bits	~250Kbps	Star Cluster Mesh	65000	Smart homes, Smart meters
BLE	IEEE 802.15.1	2.4GHz	~30 meters	0.153uW/bits	~1Mbps	Star Clusters	One to Many	Smart homes, ecommerce
6LowPAN	IEEE 802.15.4-2003	2.4GHz	Upto 2kms	185.9uW/bits	~250Kbps	Star, peer-to-peer, mesh	One to Many	Smart City
Weightless	Weightless SIG	sub-1GHz frequency bands	Upto 2Kms	~50mW	~100kbps		~2769	Smart Meters
SigFox	ETSI	868 to 869 MHz and 902 to 928 MHz	N/A	N/A	~600 bps	LTN	~10+ millions messages /day	Health, Energy Home
LoRA	LoRa Alliance	sub-1GHz frequency bands	15 to 20 kms	Few uW/bits	~50Kbps	Hybrid	Millions of nodes	Smart city, Smart Agriculture, Smart Intustry
Li-Fi	IEEE 802.15.7r1	2.4GHz	Upto 32meters	~1uW/bits	~1Gbps	Hybrid	Point to point	Secure Communications networks
WirelessHART	HART Communications Foundation (HCF)	2.4GHz	228 m	~10mW/bits	250 kbits/s.	Star, Mesh	~100	field device networks
Wi-Fi	802.11	2.4GHz, 5GHz	Upto 150 meters	~0.000525uW/bits	~1Gbps	Star, Mesh	250/access point	Smart Homes, Smart Industries, Smart Cities. Smart Health etc.
Homeplug	IEEE 1905.1	83.16MHz	Upto 30 meter	~0.5uW/bits	~85Mbps	Star	NA	Home Automation
HaLow	802.11ah	900MHz	> 15 meters	~1uW/bits	~1Gbps	NA	NA	Home Automation
Thread	IEEE 802.15.4	2.4GHz	Upto 30 meters	~11.7uW/bits	~250 Kbps	Mesh	300	Smart Asset monitoring
RFID	IEEE 802.15.4f	2.4GHz, 5GHz	~2meters	~1uW/bits	~640Kbps	Hybrid	One to Many	Smart Asset monitoring

Table 1.3: Comparison of Open Source IoT Cloud Platforms

Platform	Data Modelling	Information Security	Data Collection Protocols	Types of analytics	Support visualizations?
Kaa	Yes	Yes. 1.TrustfulVerifiers 2.Google/ Facebook/Twitter+ Trusted	MQTT	Real time, batch	Management console available. UI development not supported
AllJoyn	Yes	Applied at Endpoints and not in framework	Router: Wifi, PLC,BLE Router to cloud:	Depends upon cloud component chosen	Depends upon cloud component chosen
Devicehive	Yes	JWT	HTTPS, WebSocket	None	Yes
The Thing Networks	Yes	128-Bit AES Encryption	MQTT	None	Yes

Table 1.3: Comparison of IoT Cloud Platforms

IoT Software Platform	Device management	Integration	Security	Protocols for data collection	Types of analytics	Support for visualizations?
AWS IoT platform	Yes	REST API	Link Encryption (TLS), Authentication (SigV4, X.509)	MQTT, HTTP1.1	Real-time analytics (Rules Engine, Amazon Kinesis, AWS Lambda)	Yes (AWS IoT Dashboard)
Microsoft Azure IoT	Yes	REST API and storage-adapter	Link Encryption (TLS, SASL), Authentication (SigV4, X.509), Custom device authentication	MQTT,AMQP, HTTPS,	Stream Analytics, Data Lake Analytics, Enterprise grade analytics	Yes (Microsoft Azure Dashboard)
IBM IoT Foundation Device Cloud	Yes	REST and Real-time APIs	Link Encryption (TLS), Authentication (IBM Cloud SSO), Identity management (LDAP)	MQTT, HTTPS	Real-time analytics (IBM IoT Real-Time Insights)	Yes (Web portal)
Google Cloud Platform	Yes	Firebase SDKs, App Engine, REST	Link Encryption (TLS), E2-factor authentication	MQTT, HTTP	Stream Analytics, Data Lake Analytics	Yes (Web portal), web console
Bosch IoT Suite - MDM IoT Platform	Yes	REST API	ESCRYPT	MQTT, CoAP, AMQP,STOMP	Bosch IoT Analytics	Yes (User Interface Integrator)
GE Predix	Yes	Micro Services, REST API, SDKs	SAML	OPC-UA, Modbus, and MQTT	subscription analytics, non-subscription analytics	No
Ericsson MDM IoT Platform	Yes	REST API	Link Encryption (SSL/TSL),Authentication (SIM based)	CoAP	*Unknown	No
EVRYTHNG - IoT	No	REST API	Link Encryption (SSL)	MQTT, CoAP, WebSocket	Real-time analytics (Rules Engine)	Yes (EVRYTHNG IoT Dashboard)
PLAT.ONE - end-to-end IoT and M2M application platform	Yes	REST API	Link Encryption (SSL), Identity Management (LDAP)	MQTT, SNMP	*Unknown	Yes. Management Console
ThingWorx - MDM IoT Platform	Yes	REST API	Standards (ISO 27001), Identity Management (LDAP)	MQTT, AMQP, XMPP, CoAP, DDS, WebSocket	Predictive analytics(ThingWorx Machine Learning), Real-time analytics (ParStream DB)	Yes (ThingWorx SQUEAL)

AUTHOR(S) PROFILE

Biswaranjan Sethi, received the Master's degree in Computer Application and MBA degrees in International Trade from Symboisis Institute of Management in 2000 and 2007, respectively. During his service of 17 years in Information and Technology Industry, he has worked with many tech giants like Wipro technologies, IBM, CGI, and Integra systems etc. He has been part of many hi-tech projects predominantly in Banking and healthcare domain.

Shreya Solanke, received the Bachelor's degree in Electronics Engineering from Walchand College of Engineering, Sangli in 2013. She has an industry experience of around five years and have been part of research and development sector of the organizations like Wipro Technologies Dell International Services and TCS. Her overall experience remains in IoT Space.

