A SOLUTION FRAMEWORK FOR MANAGING INTERNET OF THINGS (IOT)

Sukant K. Mohapatra[1], Jay N. Bhuyan[2], Pankaj Asundi[1], and Anand Singh[3]

[1]Ericsson, Monroe, LA, USA
[2]Dept. of Comp. Science, Tuskegee, AL, USA
[3]CenturyLink, Monroe, LA, USA

ABSTRACT

Internet of Things (IoT) refers to heterogeneous systems and devices (often referred to as smart objects) that connect to the internet, and is an emerging and active area of research with tremendous technological, social, and economical value for a hyper-connected world. In this paper, we will discuss how billions of these internet connected devices and machines will change the future in which we shall live, communicate and do the business. The devices, which would be connected to the internet, could vary from simple systems on chip (SOC) without any Operating System (OS) to highly powerful processor with intelligent OS with widely varying processing capability and diverse protocol support. Many of these devices can also communicate with each other directly in a dynamic manner. A key challenge is: how to manage such a diverse set of devices of such massive scale in a secured and effective manner without breaching privacy. In this paper, we will discuss various management issues and challenges related to different communication protocol support and models, device management, security, privacy, scalability, availability and analytic support, etc., in managing IoT. The key contribution of this paper is proposal of a reference management system architecture based on cloud technology in addressing various issues related to management of IoThaving billions of smart objects.

KEYWORDS

IoT, SOC, M2M, OMA, SOC, CSP, SLA, CoAP, REST

1. INTRODUCTION

Over the past few decades, there has been tremendous progress and technology innovation in the field of computing and telecommunication. Although, in the past, telecommunication has been more or less focused on human-to-human communication, now with advances and innovation, machine-to-machine communication shall use same communication infrastructure and facilities in a much greater scale. Billions of these smart machines/devices shall connect to the network and significantly impact the way we live and do business. A market survey by Cisco predicts that, by 2020, about 50 billion of these smart devices shall be connected to the internet, far outpacing the world population [1].

Smart devices have been used in various sectors such as the industry, offices, home, and transportation, etc., for years. For example, many offices today have sensors to save energy in the buildings [2], traffic light controller for traffic management [3]. Typically, sensor based smart devices have been used in a closed system; for example, various sensors in an automobile mostly work within the vehicle itself. In a smart home, safety related to fire, unauthorized intrusion, level

DOI: 10.5121/ijcnc.2016.8606

of Carbon Monoxide (CO) in the house, etc., are managed by home monitoring system/application. Thus it operates mostly in the Silo of Things (SoT) model with application specific connected devices, with proprietary interconnection in a closed system. However, connectivity of these devices in an open ecosystem, whether machine-to-machine and/or human-to-machine communication, is already evolving and it would bring much greater value and create a completely new generation of innovative services with tremendous socio-economic impact. These smart devices, in an open ecosystem, shall help build smart homes, smart buildings, smart automobiles, smart industries, and smart healthcare, etc., in a very synergetic manner in a hyper connected world. For example, smart office shall not only conserve energy in the building but also integrate with security, environmental conditionsin the office and their operational readiness in a comprehensive manner. Individuals with smart wearables or bionic skins could provide physiological and health information which could be used for enhanced wellbeing, health and safety of the same individual while at home or working in an office.

As the use of smart devices proliferates with advanced sensors, actuators, processors, and transceivers and get connected, many of the applications will also involve human and things (human-to-machine) to operate synergistically. Human-in-the-loop model has tremendous opportunity in various application verticals like smart healthcare and smart vehicles [4]. However, human-in-the-loop model has its own disadvantages, specifically complexity involved in modelling human behaviour to work with smart devices in a synergetic and predictable way.
In this paper, we discuss various challenges in managing IoT in support of billions of smart devices. We propose a solution framework to manage IoT ecosystem from enablement, operational, and business application support point of view. The proposed architecture provides an open model for development and integration of various innovative applications by 3rd party in supporting and enriching theIoT ecosystem. This will enable innovation and contribution from many subject matter experts in evolving a rich IoT platform and ecosystem. The proposed reference solution framework, which addresses various challenges faced by IoT management, is the main contribution of this paper.

This paper is organized as follows:

Section II discusses transformation of silo of things to internet of things and related research work. Section III highlights various requirement and challenges in managing smart objects that are part of the IoT. Section IV provides a detailed view of referenced solution framework in managing IoT and supporting its ecosystem. Section V describes how the referenced solution framework meets various requirements and helps mitigate challenges, while section VI concludes the paper with reference to potential future work in this area.

2. SILO OF THINGS TO INTERNET OF THINGS (IOT)

The current mode of operation in IoT space is very fragmented and silo based. Application specific connected devices mostly have proprietary interconnection and work in a closed system. For example, the alarm system in a smart home is operated by alarm and security companies with dedicated servers and applications specifically to address security concerns of the home and alert stakeholders in case of a security breach. Again, the same home is monitored for utility usage often by different companies and applications (e.g. water, electricity, gas) in a very independent and uncorrelated manner.

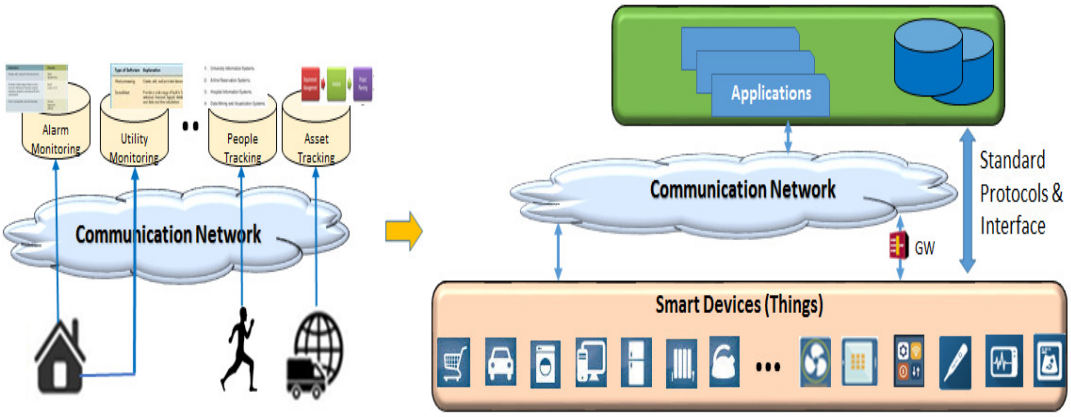

Figure 1: Silo of Things to Internet of Things

IoT has been evolving to meet the challenges of growth of billions of interconnected smart devices in an open system with standard based connectivity for varying capacity and models of smart devices. In an open, non-silo based system, the huge volume of data obtained from smart objects could be used in more intelligent and correlated manner with significant qualitative impact on our daily life, health, communication, and work environment. For example, the food habits of a person in a smart home with data from a smart refrigerator could be correlated with his/her smart health wearable, predicting/inferring appropriate health guidance for the person. Also an open IoT ecosystem shall bring subject matter experts from various domains to effectively contribute and enrich the system. Figure 1 above depicts the transformation of Silo of Things (SoT) to Internet of Things (IoT).

Internet of Things is a very active research area and significantresearch work and publications are available: survey [5], security [6, 7, 8], communication protocols [9, 10], and various IoT vertical domains [11, 12]. This paper focuses on solution framework for the platform in supporting various IoT device management, communication protocols, application verticals, addressing security issues in order to support IoT ecosystem. A solution framework addressing key challenges in managing IoT ecosystems is the key contribution of this paper.

3. REQUIREMENTS AND CHALLENGES IN MANAGING IOT

IoT devices range from simple 8-bit System on Chip (SOC) to powerful 64-bit processor with intelligent Operating Systems (OS), thus requiring support of varying communication protocols, device management methods, pre-deployment testing and integration and monitoring during operation, etc. In this section, we discuss various requirements and challenges while managing IoT devices.

3.1. Communication Protocols and Models

Figure 2presents a pictorial view of ETSI M2M reference architectural model [13].

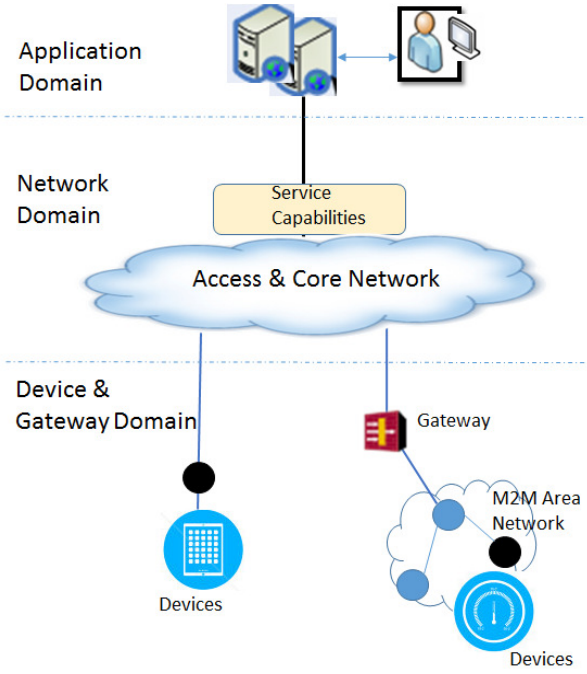

Figure 2: ETSI M2M Reference Architectural Model

The ETSI reference model has three domains: Device and Gateway domain, Network domain, and Application domain. The Device and Gateway domain includes smart devices such as sensors. A gateway typically interconnects to the Communication Service Provider (CSP) network supporting device inter-working and inter-connection. The M2M area network supportsconnection between different smart devices and gateways. The Network domain provides communication service between smart devices (including via Gateway) and servers in the Application domain. It typically includes access and core network of a CSP, which could include fixed as well as mobile networks. The Application domain supports various application services. Application services are rendered by specific business-processing servers where data analysis, various actions, alerts, and reports are handled.

M2M area networks for constrained IoT devices typically include personal area network technologies, such as Bluetooth, Thread, ZigBee Pro, ZigBee SE, and NFC. Constrained devices refer to devices using low power platform and wireless, limited computation and memory, low bandwidth, etc. Constrained devices are expected to use 6LowPAN – UDP – DTLS – CoAP protocols in higher layer. High performance IoT devices are expected to support Wi-Fi, Cellular [2.5G/3G/4G (LTE)], and Ethernet technologies. High performance IoT devices are expected to use IP v4/IP v6 – TCP/UDP – TLS – HTTP at higher layer. Figure 3 provides an overview of protocol stacks for constraint and high performance IoT devices.

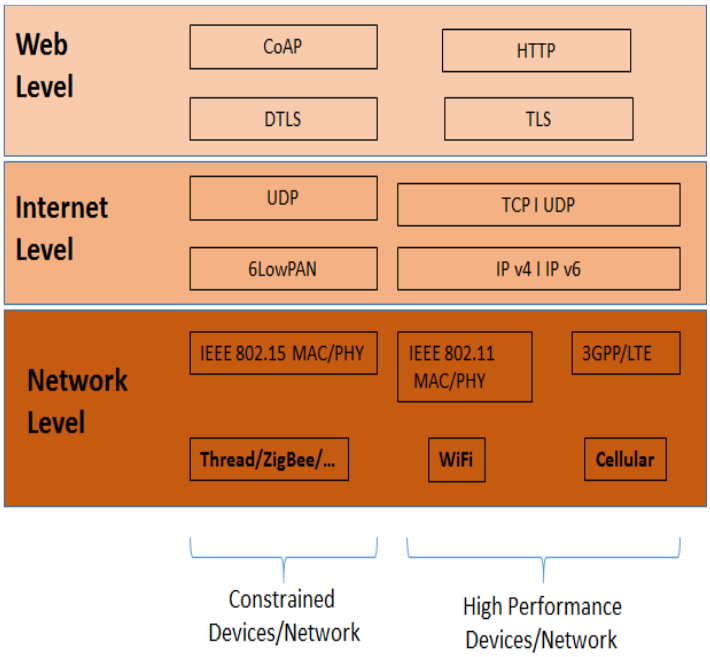

Figure 3: A High Level view of Protocol Stack for IoT Devices

Industrial Internet Consortium document [14] provides detail on IIOT connectivity architecture, stack model, and key system characteristics.

3.2. Device Management Requirements

Paper [15] describes lightweight framework for IoT device management whereas [16] describes IoT device management in a smart home environment. In this section, we highlight the following key device management functionality that a platform needs to support irrespective of different protocol support, which are described in section 3.1.

- The ability to disconnect a rogue or stolen device
- The ability to update the software on a device
- Updating security credentials
- Remotely enabling or disabling certain hardware capabilities
- Remote configuration of device
- Remotely re-configuring network parameters for the device

3.3. Interoperability and Integration

Third party products/solutions have to be added to theIoT platform creating an open ecosystem. This will ensure use of various applications and analytics developed by subject matter expert to add value to the IoTecosystem. The platform must support easy integration mechanism for incorporating such third party solutions by using an open application interface and tools.

3.4. Analytics

In theIoT ecosystem, there will be a collection of vast amount of raw data from smart devices and other systems. It is very important to use this raw data in an effective manner to derive usable knowledge base and provide actionable alerts and intelligence to end user, both in a near real-time as well as non-real-time basis. Action may happen in near real time, so there is a strong requirement for real-time analytics. For example, in a smart home, when data related to level of carbon monoxide in the house exceeds the threshold, the user must be alerted in real-time. In addition, on different occasions, the device should be able to act on analyzed data in real-time. However, in some cases, more powerful devices can also do event processing and action based on embedded logic.

In addition to handling huge amounts of raw data, analytic solution will be able to handle various types of data, varying from text to image, video, and voice in real physical world. The right data model and database should be used for effective grid, stream, graph, big data, and in-memory processing in a distributed environment. It is expected that analytics must have to deal with noisy and sometimes incomplete data. New and advanced inference techniques, rules, and models have to be used by the analytics system in order to deal with such noisy and incomplete data while deriving any inference. In some domains, correlation of various data to derive meaningful intelligence could be challenging.For example, in smart healthcare domain, raw sensor data from an individual's wearable and/or bionic skin patch must be correlated to semantically meaningful activities of the individualand his/her habits.

It is also very critical to derive correct inference and/or predication by the analytics system while dealing with noisy, incomplete data, unknown behaviours.Otherwise, it could lead to some devastating consequences. For example, driving an actuator using wrong inference could create serious safety issues. A probabilistic inference model with specific confidence level may be an approach to address this issue. Analytic systems need to support various models to support different use cases in various business domains. For example, some use case may need correlation analysis, whereas another may need predictive analysis based on historical behaviour. An adaptive model may be necessary to deal with evolving/adjusting behaviour of a smart device and human behaviour specifically with human-in-the-loop environment, often referred as Internet of Everything (IoE).

3.5. Security and Access Control

Security issue for IoT is very critical because smart device may have minimal capacity to comply with complex security need and protocols, easy accessibility of device, and on-the-air communication. Thus IoT devices are prone to security attacks [17]. There are many aspects of security issues from information processing to transmission security [18].

IoT devices are often collecting highly personal data, and bringing the real world onto the Internet (and vice-Versa). This brings following categories of security risks:

- Security risk unique to IoT device (specifically low-end devices)
- Security risk associated with protocol and data transmission by IoT devices
- Security risk inherent with internet
- Security risk ensuring safety of operation of devices like actuators
- Security risk due to incorrect inference

- Security risk due to transient failure of the device

It is very likely that next generation smart devices with powerful processors [19] shall provide enhanced security capability. However legacy devices supporting requisite security functionality shall prove challenging.

It is expected that, IoT platform shall be used by a variety of users starting from system administrator, various application users to 3rd party vendors. It is extremely important that access to the platform should be highly secured using various identification, authorization and authentication techniques and roles based access control to accommodate different users with varying roles and responsibilities [20]. In addition, the platform must be protected from potential security attack and breach [21].

3.5. Privacy Considerations

Though IoThas evolved considerably and provides many potential benefits, it also creates an opportunity for privacy violation of physical objects, individuals, or groups. The challenges are that, unlike the situation where the data owners are an individual ora group, in IoT space privacy for physical entities (things) like smart oven, smart room and its associated owners has to be taken into consideration. Analysis of collected data from smart devices and various inferences could breach privacy of individuals or groups. For example, identification specific ailment of an individual based on smart wearable data could infringe the individual's privacy and his/her health insurance risk.

An effective privacy policy must be devised and enforced by the system. The solution must be able to create and store various privacy policies based on consent of individual, legitimate owners of smart devices, and applicable laws. Privacy policy could be updated dynamically by authorized policy administrators. Once policy is configured, the system shall ensure against breach of any privacy policy.

3.5. Scalability

It is expected that billions of smart devices shall be connected to the internet. It raises many challenges with respect to scalability and reliability of platform in order to handle devices of such massive scale. The solution framework must support various aspects such as access authorization and authentication, connectivity, current and evolving communication protocols, monitoring, control and associated applications while supporting billions of smart devices. The platform architecture must scale, be secured and highly reliable to support potentially trillions of smart objects.

4. REFERENCE IOT- ARCHITECTURE MODEL

This section describes in detail the generic architectural framework for managing IoT. First we describe various components and their functionality and then realization of same in a cloud based architecture ensuring high scalability and availability.

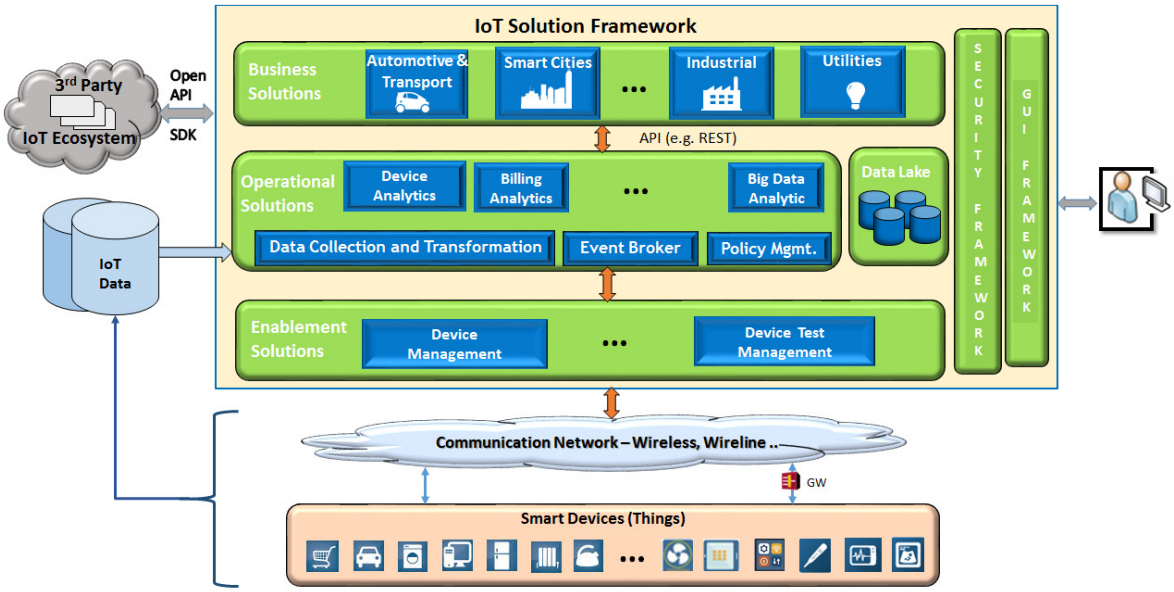

Figure 4: A Reference Architectural Framework for Managing IoT

Figure 4 depicts an overall view of IoT ecosystems in general. Smart devices typically connect to Application domain via a communication network. The communication network could be wireless and/or fixed network generally supported by communication service providers (CSP).

Typically, constrained IoT devices shall be connected with communication network via gateway, whereas high performance IoT devices could directly connect to communication network itself.

In Figure 4, IoT data refers to IoT device communication related data and IoT device usage specific data. This data could be available from different sources. For example, device communication related data could be available from different operation support systems of communication service provider, whereas device usage specific data could be available from application servers supported by application service providers (e.g., alarm/security service providers for smart home/enterprise). Thus IoT data could be very large, varied data type (text, video, message, etc.) and shall be available over different storage mechanisms (different type of database, files, object storage, etc.).

The reference architecture for IoT solution framework is component based model, where various components and sub-components can be added in plug-and-play mode. Also, components could operate logically in centralized way in a distributed manner on a cloud based platform.

4.1. Enablement Solution

This section describes two key modules on device management, device connectivity and testing domain. However, other similar functional blocks can be easily added in a plug-and-play mode.

Device Management: The device management module is responsible for communicating with devices using various protocols, both for constrained and high performance IoT devices

supporting protocols as shown in Figure 3. Key device management functionality supported by this module include:

- Software Management – installation and upgrade of device f/w and s/w
- Device Configuration – including configuration of bearer and proxies
- Disconnect/Wipe stolen and rogue devices – Disconnect misbehaving (rouge) device from network. Remotely lock-in and/or wipe-out of the device when it is stolen or lost.
- Remote enabling/disabling of device capabilities – allows to remotely enable and disable device peripherals like cameras etc.
- Etc.

Among others, Open Mobile Alliance (OMA) specification defines protocols allowing a Device Management Server to configure parameters in a smart device supporting OMA Device Management client. This include support of management objects related to device management [22]. The server and client communication model is depicted in Figure 5.

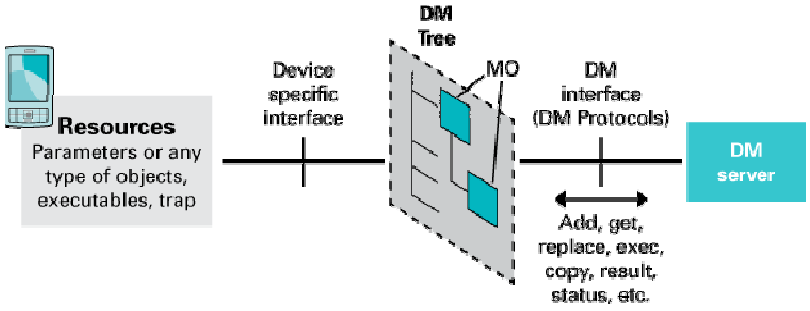

Figure 5: Open Mobile Alliance (OMA) – Client Server Model

Device Test Management: It is critical that IoT devices be tested in pre-deployment, thus assuring that there are no major issues when it goes on-line. Similarly, mechanism for remote testing in post-deployment is necessary in order to diagnose and troubleshoot any problem with device during operation. It is expected that many of the IoT devices shall be deployed in remote location, so remote on-line testing is very critical from the operational cost effectiveness point of view. The device test management module shall support functionality supporting both pre-deployment and post-deployment testing of IoT devices. Open Mobile Alliance (OMA) Diagnostics Monitoring Function Specifications defines standardized management object framework in supporting diagnostic and monitoring information [23].

4.2. Operational Solutions

The Operational Solution layer covers many functional areas primarily supporting operational management support aspect for IoT. It has many supporting software infrastructure components such as data collection, event broker, policy management as well as operational functional module supporting various analytics functions. Analytics solution also includes logic, algorithms, and framework to support rich analytics functions based on machine learning [24], artificial intelligence [25], and natural language processing.

Data Collection, Transformation and Distribution: The Data Collection, Transformation and Distribution Module supports data collection for IoT devices from varied sources, including data from enablement management layer. Primary functionality supported by this module is in collecting various types of data from the underlying systems/environment and making it available to interested applications. Data type could be very varied such as text, video, voice clips, topology graph, and GIS based data. The data would be related to connectivity, session records, flow records of smart object as well as usage data, stats, and KPIs supported by smart devices. An effective collection of all different data in real-time and near-real-time is key to run various analytics functions supporting operation and intelligent inference for proactive management of supported IoT systems. From an architectural perspective, although this module could logically behave in a centralized manner, but couldbe deployed in distributed fashion using cloud computing environment.

Event Broker: Event broker provides common mechanism for the receipt and distribution of autonomous events; the events originating from the managed environment (e.g. state changes of objects, etc.) or from various supported applications that detect events of interest (e.g. abnormal behaviour of devices, connectivity failure, etc.). Events could drive various actions and activities for the supported applications.

Policy Management: Policy Management enables rule-driven behavior of operational framework based on configured/dynamic policy. Policy management also could enforce various rules regarding security management, rules related specific data analysis, etc.

Device Analytics: The Device Analytics component supports all analytics functionality related to smart devices. This includes device connectivity analysis and inferences/alerts related to device communication failure, abnormal behaviour, fault, and SLA violation. Device analytics shall also support device usage related analysis and inferences based on device usages data and its KPI. This module also supports various analysis and intelligence inference with respect to pre-and post-deployment device testing data.

Billing Analytics: Billing of IoT service would be very different from typical billing of voice, video, and data services as supported by service providers. Typical communication service providers may just provide communication services for smart devices, whereas application owners could be different entity. Even 3rd party connectivity service providers could provide device connectivity service using infrastructure of multiple communication service providers across various regions. IoT ecosystem platform could be shared by many vendors and specific functionality can be serviced based on vendor's need, rather than whole platform being owned and operated by each vendor. Thus, the Billing Analytics module is expected to support billing and invoicing models supporting various models and business use cases in a flexible and configurable way.

Big Data Analytics: The big data analytics support analysis of collected data from various sources for intelligence inferences related to specific business application support and monetization. This is primarily non-real-time data analysis. For example, it could use various application data such as energy consumption, water consumption, security data for a smart home and use external data (e.g., weather data) to provide various useful information for resident of home, security personnel, township, insurance company, etc. As an example, by using weather chart, it could provide analysis such as excess water usage by sprinkler system at home, thus enabling user to save on water usage bill. Based on security incidents in various home/offices in a region, the security personnel (e.g., police) in township/county/community could devise a smart

policing plan. The algorithm, logic, and framework of this module could be applied for various application domains such as smart city, smart transport, smart health, etc.

Data Lake: The data lake shown in the solution framework could include data in core and Edge Lake. This component provides a persistence mechanism for both structured and unstructured data that is collected and made available for application analysis. It will leverage some of the Big Data technologies for performing various analytics at the edge (the Edge Lake) and complementing the Big Data Core Lake.

4.3. Business Solution

At the business layer, the IoT ecosystems support total solutions covering applications in various verticals, such as smart home, smart cities, smart grid, smart health, connected automotive, etc., and its use cases. Thus it provides complete solution for operating a specific vertical/domain in a comprehensive manner. For example, a smart city may include many aspects such as smart policing, traffic management, waste management, transportation, etc. Thus the smart city business module supportsall the aspects in managing a smart city, so that the user (e.g., city authorities) can use this business application to manage all major aspects of the city in a comprehensive and intelligent way, thereby providing the best service to city residents in a cost effective and efficient manner.

4.4. Security Framework

The security framework includes Operation, Administration and Management (OAM) and Security Management that supports user administration, authentication, authorization, auditing, and secured communication, etc. [26, 27] for operation personnel. The Security framework shall also support overall security of IoT management framework ecosystem and supported application against security risk and external security attack (such as denial of service attacks).

4.5. GUI Framework

The Web Server based GUI framework provides web-based access to IoT management ecosystem from client workstation. The GUI framework also supports generation of various adhoc reports, and enables communication with users of the system, both online or offline.

4.6. Open API/SDK

It is expected that IoT ecosystem would need expertise in many different domains to leverage the true value of IoT deployment. For example, the domain expertise in smart health and smart city area would be quite different. Thus an Open API/SDK is essential for people/organization with different domain knowledge/expertise to contribute to IoT ecosystem. The Solution frame supports an open API/SDK, so that 3rd party application developer can contribute to IoT ecosystem development and enhancement. The 3rd party interface could be based on Representational State Transfer (REST) Application Programming Interface (API) [28] for interworking with IoT ecosystem. REST API can also be used for interfacing operational application with business layer applications supporting integration.

The IoT platform needs an efficient, reliable, and scalable way to handle connectivity and communication with large number of devices as well as storage, processing and analysis. Cloud

based architecture for the IoT platform is most suitable, when it comes to storing, processing, and analysing data, especially big data. [29], [30] describes platforms for building, testing, and deploying applications for cloud computing.

5. MANAGING THE CHALLENGES OF IOT

It is evident that the proposed solution framework as described in section IV, meets all key challenges in supporting and managing theIoT ecosystem.

The enablement layer of solution framework supports various communication protocols and models using device management component. Device management modules also support key functionality enabling various aspect of device management from software upgrade to handling security related issues for stolen/lost IoT devices.

Open API/SDK module provides interoperability and integration mechanism for 3rd party applications. Flexible and open API enable easy integration with 3rd party applications and using SDK the external application developer could access various relevant object model in the system and develop value added applications.

Security framework enables solution framework security. A rule based access control to the system can be enforced by well-defined rules and policy via policy management component. Various privacy constraints and consideration can also be enforced via policy management module by defining associate rules and policy.

Scalability, high availability, and reliability of application framework is very critical in supporting the IoT solution model. The proposed solution framework is expected to be implemented in a cloud environment and applications can be hosted in a distributed computing environment, which provides high availability and thus ensures reliability. The cloud based implementation also supports the required scalability. IoT devices are expected to grow exponentially over the years, thus the solution framework based on cloud computing paradigm can support moderate to large number of smart devices as needed.

6. CONCLUSIONS

IoT will evolve over time with ever increasing advances and capability of smart devices such as sensor, actuators, robust communication and harvesting knowledge and intelligence from arrays of vast amount of data moving from an information age to intelligence age. This will change our current mode of lifestyle and work habits in a significant and perhaps in a disruptive way.
There are several efforts in different standard organizations such asETSI, Open Mobile Alliance, OneM2M, IEEE, ITU-T and forums are focused on various standard activities and architectural aspects supporting IoT. It is expected that work in many of the overlapping areas could converge in near future.

In this paper we focused on overall need of an IoT ecosystem and solution framework to support it. In our future work, we expect to focus on the area of analytics, since it is the heart of providing intelligent and high value add for IoT ecosystem.

ACKNOWLEDGEMENTS

This research was supported in part by NSF Grant # 1614845.

REFERENCES

[1] Dave Evans, "Internet of Things – How the Next Evolution of the Internet is Changing Everything", White Paper - Cisco Internet Business Solution Group, April 2011. http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] V. Bradshaw. "The Building Environment: Active and Passive Control Systems", John Wiley & Sons, Inc., River Street, NJ, USA, 2006

[3] Khalil M. Yousef, Jaml N. Al-Karaki, and AlimShatnawi, "Intelligent Traffic Flow Control System using Wireless Sensor Network", Journal of Information Science and Engineering, Page 753-768, 2010.

[4] A Liu, and D. Salvucci, "Modeling and Prediction of Human Driver Behavior", Intl. Conference on HCI, 2001.

[5] L Da Xu, W He, and S Li, "Internet of Things in Industries: A Survey", IEEE Transactions on Industrial Informatics, Vo. 10, Issue 4, 2014

[6] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities", IEEE 7th International Conference on Service-Oriented Computing and Applications , 2014

[7] Jiang Du, and ShiWei Chao, "A study of information security for M2M of IOT", 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE) , 2010

[8] Jorge Granjal, Edmundo Monteiro ; Jorge Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Surveys & Tutorials, 2015

[9] Chonggang Wang, Mahmoud Daneshmand ; Mischa Dohler ; Xufei Mao ; Rose Qingyang Hu ; Honggang Wang, "Internet of Things (IoT): Architecture, Protocols and Services", IEEE Sensors Journal, 2013

[10] Adnan Aijaz, A. Hamid Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective", IEEE Internet of Things Journal, 2015

[11] Andrea Zanella, Nicola Bui ; Angelo Castellani ; Lorenzo Vangelista ; Michele Zorzi, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, 2014.

[12] S. M. Riazul Islam, DaehanKwak , MD. HumaunKabir, Mahmud Hossain, Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey" , IEEE Access, 2015

[13] ETSI TS 102 690 v2.1.1, Machine-to-Machine Communications (M2M); Functional Architecture, 2013.

[14] Rajive Joshi, Paul Didier, Jaime Jimenez, and Timothy Carey, "The Industrial Internet of Things – Volume G5 Connectivity", IIC:PUB:G5:V0.9:FD:20161028, 2016.

[15] Datta, S.K., and Bonnet, C., "A lightweight framework for efficient M2M device management in oneM2M architecture," International Conference on Recent Advances in Internet of Things (RIoT), April 2015.

[16] Perumal, T., Sulaiman, M.N., Mustapha, N., Shahi, A., and Thinaharan, R., "Proactive architecture for Internet of Things (IoTs) management in smart homes," IEEE 3rd Global Conference on Consumer Electronics (GCCE), Oct. 2014.

[17] Al-Sakib Khan Pathan, Hyung-Woo Lee, and ChoongSeon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", 8th International Conference Advanced Communication Technology, 2006.

[18] Chen Qiang, Guang-riQuan, Bai Yu, and Liu Yang, "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking Vol.6, No.6, pp.1-10, 2013.

[19] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper Resistance Mechanisms for Secure, Embedded Systems", Proc. of 17th International Conference on VLSI Design, 2004.

[20] Ravi S. Sandhu and PierangelaSamarati, "Access Control: Principle and Practice", IEEE Coomunications Magazine, 1994.

[21] Cisco, "Addressing the Full Attack Continuum: Before, during, and after an Attack It's Time for a New Security Model", White Paper, http://www.cisco.com/c/dam/en_us/training-events/le21/le34/assets/events/i/gartner_BDA_Whitepaper.pdf, 2014.
[22] Open Mobile Alliance, "Device Management requirement v1.3 – OMA-RD-DM-V1_3-20160524-A", 2016
[23] Open Mobile Alliance (OMA), Diagnostics and Monitoring Function Specification (OMA-TS-DiagMon_Functions-V1_2-20131008-A), October 2013. http://technical.openmobilealliance.org/Technical/Release_Program/docs/DiagMon/V1_2-20131008-A/OMA-TS-DiagMon_Functions-V1_2-20131008-A.pdf
[24] H. Howie Huang, and Hang Liu, "Big data machine learning and graph analytics: Current state and future challenges" IEEE International Conference on Big Data, Washington DC, 2014.
[25] Daniel E. O'Leary, "Artificial Intelligence and Big Data", IEEE Intelligent Systems , 2013
[26] ITU-T, "Security in Telecommunication and Information Technology - An overview of issues and deployment of existing ITU-T Recommendation for secure telecommunications", 2003, http://www.itu.int/itudoc/itu-t/85097.pdf
[27] Telcordia, "GR-815-CORE Generic requirements for Network Element/Network System (NE/NS) Security," Issue 2, March 2002.
[28] Richardson, Leonard; Mike Amundsen, "RESTful web API", O'Reilly Media, ISBN 978-1-449-35806-8, 2013
[29] RajkumarBuyya and KarthikSukumar, "Platform for Building and Deploying Applications for Cloud Computing", CSI Communications, May 2011
[30] T. Vengattaraman, P. Dhavachelvan, and R. Baskaran, "A Model of Cloud Based Application Environment for Software Testing", International Journal of Computer Science and Information Security, Vo. 7, No. 3, 2010.

Authors

Sukant K. Mohapatracurrently works as a CTO in Ericsson, USA. He has a Ph.D.degree in Computer Science with specialization in Telecommunications from Stevens Institute of Technology, New Jersey. His work and research interest includes: Next Generation Fixed and Mobile Network Architecture, Network Planning, Design, Optimization, and Network Management,Network Virtualization, Cloud Computing, and Internet of Things (IoT).He is recipient of DMTS award at Bell Laboratories and a senior member of IEEE. He is the founder chairman of National Institute of Science and Technology (NIST), India.

Jay N. Bhuyan is a professor in the Department of Computer Science at Tuskegee University. His research and teaching interests include Telecom Software Architecture and Development, Software and Network Security, Big Data Analytics, and Parallel & Distributed Computing. He received a Ph.D. in Computer Science from the University of Louisiana at Lafayette. He has over 25 years of full-time and part-time teaching experience as well as over 15 years of research and development experience in the Telecom industry. He is a member of IEEE and IEEE Computer, IEEE Communications Societies.

Pankaj Asundi brings 30 years of systems and technology experience to Ericsson in his position as Vice President Sales for IOT, Cloud and Media solutions. His key responsibilities are to develop and manage new business. Before joining Ericsson, Pankaj was a Software Development Manager for First Consulting Group. He holds a Master of Science in Industrial Engineering from University of Oklahoma.

Anand Singh is currently working in CenturyLink as Vice President – Architecture. He has over twenty-seven years of telecom industry experience with technological, transformational and strategic leadership in Network, OSS/BSS, and emerging technologies/services. In past he has worked as DMTS, technology leader and executive director at AT&T and Bell laboratories. He has PhD degree in Physics from Banaras Hindu University, India, and worked as Research Scientist in Carnegie-Mellon University, University of California Berkeley, and Naval Research Laboratories WashingtonDC.