International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-340
VOL. 2(2),2015

THE INTERNET OF THINGS – A CASE STUDY

Payal Sachdeva[1],
Akshay Chaudhary[2]

ABSTRACT

The lines between our physical and digital worlds are indistinct. Our daily experiences are—and will continue to be--affected by the number of Internet-connected devices and anytime, anywhere access to information. And there is no sign of things slacking down. Each year will see increasing amount of growth in devices connected to the Internet.

These "things" will come in all shapes and sizes, from four-ton cars to clothing and even our whole home. The world of smart devices talking to each other--and to us--is happening now. But collecting the business rewards will depend on the ability to design and build a networking infrastructure that successfully manages the flood of data that comes from this new Internet, the Internet of Things (IoT).

The Internet of Things is not a single technology but an idea with embedded sensors driving the trend, real-time support and learning having a social impact and it allows businesses to make situational decisions based on the sensor's information. It is really about the services and applications that enable them. The aim of this paper is to describe the various applications of IOT in daily life and its impact on our society.

Keywords: Information, Infrastructure, Internet, sensors and society.

1. Assistant Professor, Department of Civil Engineering CGC Technical Campus, Jhanjeri.
2. Assistant Professor, Department of Civil Engineering CGC Technical Campus, Jhanjeri.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-340
VOL. 2(2),2015

INTRODUCTION

The lines between our physical and digital worlds are indistinct. Our daily experiences are—and will continue to be--affected by the number of Internet-connected devices and anytime, anywhere access to information. And there is no sign of things slacking down. Each year will see increasing amount of growth in devices connected to the Internet.

The IoT does not come without its challenges. Threats to data security, physical security, security of devices, regulations, privacy, encryption, authentication and a host of other issues all need to be addressed before the IoT can really become commonplace. These themes sound eerily similar to the ones surrounding the cloud only a couple of years ago. Now, consumer devices are the focus, and service providers will work to find new ways of driving greater operational efficiency and better management of infrastructure—for themselves and their customers. The challenge in harnessing this powerful force isn't limited to managing the sheer volume of data created. It's also making sense of that data to prioritize traffic and optimizing the application architecture itself [1].

The Internet of Things refers to the set of systems and devices that interconnect real-world sensors and actuators to the Internet. This includes many different types of systems, such as:

- Mobile devices and its applications based on the version of operating systems.
- Smart meters and objects
- Wearable devices including clothing, health care implants, smart watches, and fitness devices
- Internet-connected automobiles
- Home automation systems, including thermostats, home theater, lighting, and home security
- Sensors for weather, traffic, ocean tides, road signals, and more .

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-340
VOL. 2(2),2015

These systems connect to the Internet or gateway in a variety of ways, such as long-range WiFi/Ethernet using IP protocols (TCP/UDP, including cellular); shortrange Bluetooth low energy; short-range Near Field Communication; and other types of medium-range radio networks. Point-to-point radio links and serial lines are also used. Some devices/sensors connect directly to the Internet via an IP protocol and others with specific IoT protocols such as Message Queue Telemetry Transport (MQTT), Constrained Application Protocol, and others.

MQTT is a "subscribe and publish" messaging protocol designed for lightweight machine-to-machine communications. Originally developed by IBM, it is now an open standard. It needs a gateway or receiver (broker) to communicate. However, its primary purpose is to allow a device to send a very short message to an MQ broker and to receive commands from that broker. Every message is published to a location, called a topic. Clients (the sensors) subscribe to various topics and when a message is published to the topic, the client/sensor gets it [2].

EFFECTS OF IOT ON APPLICATIONS

Many of today's traditional architectures will buckle under the increasing demand of all the connected devices. According to IDC, the rate at which applications double in the enterprise is once every four years. This time frame is likely to be cut in half as more IoT devices need applications supporting them and service providers need to
be ready for the increased demand [3].

As more applications are needed to run"things," traditional infrastructure concerns such as scale and reliability are becoming most important. Added/more challenges with identity and access, improving the end-user or subscriber experience, and the need for faster provisioning of services could overwhelm IT departments. A strong, large, and intelligent infrastructure will be necessary to handle the massive traffic growth.

Clearly, security must also be present since the IoT has the potential to weave vulnerabilities throughout the system—the ubiquity of connected devices presents a gold mine for attackers. Outpacing attackers in our current threat landscape will require more resources in order to minimize risk. Service providers will need to continue to harden their own infrastructures and look to cloud services like DDoS mitigation to lessen the effects of attacks.

To secure security, intelligent routing, and analytics, networking layers will need to be smooth in

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-340
VOL. 2(2),2015

the language that devices use. Understanding these rules of conduct within the network will allow traffic to be safe, prioritized, and routed accordingly. Recognizing and arranging these messages will enable better scalability and manageability for the onslaught of device traffic and data. Intelligence will also be needed to categorize what data needs attention (like a health monitor alert) and what doesn't (like temperature is good) [4].

CLOUD – THE IOT ENABLER

The cloud has become one of the primary enablers for IoT. Within the next five years, more than 90 percent of all IoT data will be hosted on service provider platforms. That's because cloud computing reduces the complexity of supporting IoT "Data Blending."

In order to achieve or even maintain continuous IoT application availability and keep up with the pace of new IoT application rollouts, service providers must explore expanding their data center options. Having access to cloud resources provides service providers with the agility and flexibility to quickly provision IoT services. The cloud offers organizations a way to manage IoT services, rather than boxes along with just-in-time provisioning. Cloud enables IT as a Service, just as IoT is a service, along with the flexibility to scale when needed.

The connectivity between a data center and the cloud is generally referred to as a cloud bridge. The cloud bridge connects the two data center worlds securely and provides a network compatibility layer that bridges the two networks. This provides a transparency that allows resources in either environment to communicate without concern

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-340
VOL. 2(2),2015

for the underlying network topology. Once a connection is established and network bridging capabilities are in place, resources provisioned in the cloud can be non-disruptively added to the data center–hosted pools.

By integrating the enterprise data center with external clouds, the cloud becomes a secure extension of the enterprise's IoT network. This enterprise-to-cloud network connection is encrypted and optimized for performance and bandwidth, thereby reducing the risks and lowering the effort involved in migrating IoT workloads to the cloud [5].

The services fabric model enables consolidation of services onto a common platform that can be deployed on hardware, on software, or in the cloud. This reduces operational overhead by standardizing management as well as enabling deployment processes that support continuous delivery efforts. By sharing service resources and leveraging fine-grained multi-tenancy, the cost of individual services is dramatically reduced, enabling all IoT applications— regardless of size - to take advantage of services that are beneficial to their security, reliability, and performance.

CONCLUSION

Connected devices are here to stay—forcing us to move forward into this brave new world where almost everything generates data traffic. While there's much to consider, primitively addressing these challenges and adopting new approaches for enabling an IoT–ready network will help service providers chart a clearer course toward success.

An IoT–ready environment can enable service providers to begin taking advantage of this communal shift without a wholesale rip-and-replace of existing technology. It also provides the breathing room needed to ensure that the coming rush of connected devices does not cripple the network infrastructure. This process ensures benefits will be realized without compromising on the operational governance required to ensure availability and security of the IoT network, data, and application resources. It also means service providers can manage IoT services instead of boxes.

However an IoT–ready infrastructure is constructed, it is a transformational journey. It is not something that should be taken lightly or without a long-term strategy in place.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-340
VOL. 2(2),2015

REFERENCES

1. http://www.gartner.com/newsroom/id/2905717
2. http://eclipse.org/community/eclipse_newsletter/2014/february/article2.php.
3. IDC Directions, "Battle for the Future of the Datacenter: The Role of Disaggregated Systems," Mar 2014.
4. http://searchsecurity.techtarget.com/tip/Internet-of-Things-IOT-Seven-enterprise-risks-toconsider.
5. IDC FutureScape Internet of Things: http://www.machinetomachinemagazine.com/2014/12/04/idc-report-worldwide iotpredictions- for-2015/