Institute of Management Technology
Ghaziabd
Course : Emerging Technology and New Opportunity (ETNO)
EXECUTIVE, Batch: 2013-14, Term – II
Prof. Parijat Upadhyay

Time ; 90 min

Full Marks : 50

Section A(Compulsory)

Internet, 'network of networks' may very well be termed as one ofmankind's finest inventions and 'Internet of Things' (IoT) could be pitted asthe optimal enablement of this invention, owing to its scale and utility. Thescenario outlined earlier will soon be real as the internet is becomingaccessible at one's fingertips and over diverse devices. The ABI Research data states that there are more than10 billion wirelessly connected devices in the market today; with over 30 billion devices expected by 2020. In fact, with millions of devices enabling internet connectivity, this network is not just expanding to reach moreindividuals, but it is likely to bring about a 360 degree change in the way we communicate and operate. Asper Internet and Mobile Association of India (IAMAI) statistics, there are more than 205 million peopleconnected to the internet in India.

Internet is visibly making every object or machine around us smarter, right from connected toothbrush, sportsgear with embedded sensors and smart refrigerators. We will soon live in an ecosystem where these 'dumbdevices' would acquire intelligence through an inbuilt OS enabling the devices to get connected with otherpaired/authorised devices. For example, consider a power controller at home enabled to communicate withthe GPS device of a user's car. In the world of 'Internet of Things,' the GPS device triggers the powercontroller at home, to switch on lights and other important appliances whenever the car reaches a stipulatedgeological radius. Again, the power controller triggers devices at home which are connected to the internet, toschedule tasks as per triggers received. While the ecosystem is being enhanced for all the good reasons, thesecurity aspect is getting immensely threatened because if the object is connected to the internet, hackers willfind it, and if it has an OS they can hack it.

The dynamism of the IoT is one of its most challenging features as most of us in our day-to-day lives mightcome across many of these smart devices, yet be unaware of the consequences that might pop-up if they arenot secured appropriately. More the connected devices, greater is the range of 'significant' security challengesacross data privacy and physical security that have the potential to disrupt functionality of consumers andbusinesses in new ways.

The benefits as well as associated risks around Internet of Things will affect organisations and governments toa great extent. For example, in today's BYOD enabled enterprises, while the device-to-device communicationhas become easier, the apps and services that the devices possess, have a potent security risk. Morechallenging perhaps is the potential for data aggregation across smart devices, internet-based services andexisting data pools.

According to a recent whitepaper by Symantec, targeted attacks against the energy companies are increasingevery year, with the intent of stealing intellectual property of new technologies created for this space. It wasobserved that modern energy systems are becoming more complex as the supervisory control and dataacquisition or industrial control systems sit outside of traditional security walls. And as smart grid technologycontinues to gain momentum, more new energy systems will be connected to the Internet of Things, which .opens up new security vulnerabilities related to having countless connected devices.

Lessening the risks

Security risks in the world of connected devices have already been demonstrated against smart televisions,medical equipment, security cameras, routers, trash-cans, baby monitors and traffic systems. Yet most of ussitting in our living rooms, roaming in a market place, enjoying vacation might not realise the bane. Essentially there needs to be a two- step approach to mitigate the security risks posed through connecteddevices. First, an embedded security software for in-device security can enable devices to filter and preventproliferation of threats. Second, from a manufacturer's perspective,

major software vendors should figure outhow to notify customers and provide patches for vulnerabilities.

Question(20 marks)

1.Internet of Things(IoT) will have a snowballing effect in the way technology is used in day-to-day business enabling digital lifestyle and, at the same time, expanding fertile grounds for cyber-attacks. What in your view are the various ways in which business enterprises are getting impacted? Also suggest a structured approach to counter the threats and protect the data and information assets for a business enterprise.

Section B (Attempt ANY 5 @ 6 marks each. All questions carry equal marks)

1. Enterprise systems are becoming a necessity for doing business for business organisations of any size. What in your view should be a proper approach for small and medium scale enterprises to implement such system in their organisation?

2. There has been lot of technology convergence happening in all forms of business. What can possibly be some of the critical issues which can affect business in such a scenario?

3. Discuss the approaches of few companies where IT has a strategic role in their business model.

4. Discuss the business requirements of information at various levels in an organisation hierarchy along with the characteristics of decision making process.

5. Discuss the role of social media analytics for a business enterprise.

6. Distinguish between predictive and prescriptive analytics with appropriate example.

7. Distinguish between OLAP and OLTP systems. Explain the following concepts in context to Data Warehousing : Roll-Up, Roll-Down, Dice and Slice. Give relevant example to illustrate the concepts.